Next-Generation Endpoint Security Market Sizing and Forecast 2016–2020

By David Monahan
An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) End-User Research Report
February 2016
Table of Contents

Executive Summary .................................................................................................................. 1
Background and Scope ............................................................................................................. 2
Definitions of Qualifications .................................................................................................... 2
  Qualifications for Consideration ....................................................................................... 2
  Functionality Definitions ...................................................................................................... 3
The Market and Maturity ......................................................................................................... 4
Research Participants ............................................................................................................. 6
  Participants .......................................................................................................................... 6
  Declined to Participate ........................................................................................................ 6
Market Share .......................................................................................................................... 6
  Largest Single Deployment ................................................................................................ 7
  Market Share by Customer Licenses .................................................................................. 8
  Market Share by Revenue ................................................................................................... 10
  Aggregate Ranking .......................................................................................................... 12
Market Size and Forecasts ...................................................................................................... 13
  Total Revenue and Growth Rate ........................................................................................ 13
EMA Perspective .................................................................................................................... 14
  Pivotal Change in the Market ............................................................................................ 14
  Taking the Next Step ......................................................................................................... 14
  Educating Auditors and Regulators .................................................................................. 15
  Differentiation .................................................................................................................... 15
  New Entrants, Acquisition, and Market Consolidation ...................................................... 15
    Tanium ............................................................................................................................. 16
  Expanding into the Consumer Segment ............................................................................ 16
  Comments on Current Market Leaders ............................................................................. 16
Vendor Profiles (Listed in alphabetical order) ........................................................................ 17
  Analyst Notes ..................................................................................................................... 17
  Invited but No Response .................................................................................................... 17
  Vendor Changes ................................................................................................................ 18
Participating Vendor Profiles ................................................................................................. 19
  Avecto ............................................................................................................................... 19
  Bromium ............................................................................................................................. 20
  Carbon Black (Formerly Bit9+Carbon Black) ..................................................................... 21
  Cisco Systems ..................................................................................................................... 22
  Comodo .............................................................................................................................. 23
  CounterTack ....................................................................................................................... 24
  CrowdStrike ......................................................................................................................... 25
  Cybereason ........................................................................................................................ 26
# Table of Contents

<table>
<thead>
<tr>
<th>Company</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cylance</td>
<td>27</td>
</tr>
<tr>
<td>Deep Instinct</td>
<td>28</td>
</tr>
<tr>
<td>Fidelis Cybersecurity</td>
<td>29</td>
</tr>
<tr>
<td>FireEye HX</td>
<td>30</td>
</tr>
<tr>
<td>Hexis Cyber Solutions</td>
<td>31</td>
</tr>
<tr>
<td>IBM Apex</td>
<td>32</td>
</tr>
<tr>
<td>Invincia</td>
<td>33</td>
</tr>
<tr>
<td>LightCyber</td>
<td>34</td>
</tr>
<tr>
<td>Malwarebytes</td>
<td>35</td>
</tr>
<tr>
<td>Outlier</td>
<td>36</td>
</tr>
<tr>
<td>Promisec</td>
<td>37</td>
</tr>
<tr>
<td>RSA ECAT</td>
<td>38</td>
</tr>
<tr>
<td>SentinelOne</td>
<td>39</td>
</tr>
<tr>
<td>Sophos</td>
<td>40</td>
</tr>
<tr>
<td>Tanium</td>
<td>41</td>
</tr>
<tr>
<td>Triumfant</td>
<td>42</td>
</tr>
<tr>
<td>Ziften</td>
<td>43</td>
</tr>
</tbody>
</table>
Executive Summary

This vendor-related research focuses on solution providers that are providing proactive next-generation endpoint security services covering prevention, detection, and response. EMA provided all identified participants the opportunity to participate in both a vendor-answered questionnaire and interviews. EMA then combined that information with research efforts external to the providers to create company profiles and assess each on their applicability to the space as well as their market share by revenue and license volumes. Most of the vendors competing in this space have emerged or refocused in the last few years, with only a few having competed in the market for more than five years.

As with any study, this study is only as good as its data inputs. This research identified 34 solution-provider candidates as participants. Of those companies, nine vendors elected not to respond or share data. Within the remaining 25, some were unable to provide complete data due to company policy.

The Next-Generation Endpoint Security (NGES) market is most similar to the Endpoint Threat Detection and Response (EDR) market identified by Gartner, but also overlaps the Specialized Threat Analysis and Protection (STAP) market identified by IDC. It is contained within the broader endpoint software security market, which includes traditional antivirus, also identified by IDC, and the even larger endpoint security market identified by “MarketsandMarkets,” which includes all of the previous functionalities plus firewall, endpoint device control, and more. There is not a more comprehensive report in the market today discussing endpoint security.

The NGES market is highly competitive. With a 2013–2014 annual growth rate over 100% and 2014–2015 shaping up similarly, NGES is pushing a five-year compounded annual growth rate (CAGR) of over 50%.
Background and Scope

Vendors providing “next-generation endpoint security” are focused on endpoint protection via prevention and/or detection and response. However, their approaches to this are highly variant. One key aspect is they do not rely solely or primarily on signature-based or hash-based prevention as their means of defense. In fact, in this area, only four of the vendors use signatures/file hashes for detecting nuisance malware at all. Those that do employ the functionality use it for a “quick hit” prior to leveraging their advanced capabilities.

How vendors achieve these advanced results is highly variant as well. Non-signature-based approaches include adaptive/dynamic application control, containers (Docker-like), virtualization, system correlation between endpoint and network detection, deep learning (cutting-edge adaptive algorithms similar in concept to machine learning), and a few other proprietary methods. All but one of these methods use various algorithmic implementations of unsupervised adaptive machine learning for anomaly and behavioral detection. It is important to note that three of those vendors use a totally agentless solution, two vendors use virtualization, one uses Docker-like containers, and one uses a combined network and endpoint inspection in a single solution, though many have integrations and partnerships with network protection vendors.

Of the nine vendors that elected not to participate, five are market leaders in the traditional antivirus space. Three are newcomers or relative newcomers to the next-generation endpoint security market, and one has changed its business focus from endpoint protection to threat-actor hunting.

The report focuses on enterprise-capable solution providers. The minimum qualifications for an enterprise class solution are listed in the “Definitions of Qualifications” below. The research was open to all enterprise-focused vendors; none of the invited vendors paid to participate in the research.

Though significant time was put into locating vendors, there are probably a few that were not identified. EMA believes, however, that it reached the point of diminishing returns and that any remaining vendors are small enough that their inclusion would not have significantly affected the outcome of the analysis.

It was disappointing that some vendors chose to not participate. A significant driver of this report was to provide vendors with an opportunity to demonstrate next-generation protection capabilities and, especially for the traditional antivirus players, to break out of their perceived molds.

Definitions of Qualifications

In order to qualify as a next-generation endpoint security player, vendor solutions must meet the following criteria.

Qualifications for Consideration

1. Non-reliant on signature/pattern-based enforcement or detection - This is one of the most significant entrance requirements. It is clear that signature- and pattern-based solutions have passed their peak. First, it is clear that enterprises are less tolerant of the signature approach because it leaves them vulnerable to early attacks prior to signature creation. For the organization that is one of the early targets, this can easily equate to millions of dollars in losses. Second, with more threat actors creating code and a proliferation of code recombinating tools, signature writers can’t keep up with the variants and users won’t put up with broad signatures that cause excessive false positives.
2. **Proactive** - Users of these solutions depend on the solutions’ ability to proactively identify and alert/notify administrators of incidents they detect. The solutions may not prevent or detect all issues, but when they do, they let someone know.

3. **Centrally Manageable and Scalable** - To qualify as an enterprise-class system, the solution must have the capacity to be installed across thousands of endpoints and be centrally managed; it should require only a few administrators to install and maintain it. The central management console is preferably created and supported by the solution provider, but that is not a hard-and-fast requirement. If the solution cannot be centrally managed, then no business will seriously consider it because they will not be able to meet the administration needs in any sizeable environment.

4. **Granular policy-based control** - Regardless of how each of the solutions accomplishes its task, the requirements for operation, enforcement, alerting and access must be controlled by a policy (or rules) engine. Existence of this engine is table stakes for consideration in any business environment, as companies require consistent policy alignment within the environment and usually have limited personnel resources for management.

**Functionality Definitions**

1. **Prevention solutions** must stop the execution of malware. Depending upon the solution, the means of prevention and the place in the kill-chain at which the prevention activates will vary considerably. Some solutions stop executables from activating while others use behavioral monitoring of the program during its lifecycle and stop it if it attempts to perform actions that are outside the realm of normal operations. These activities can include writing to system memory space, process injection, opening network connections, and many others.

2. **Detection solutions** do not attempt to stop execution, but rather rely on their ability to identify activities and changes that the advanced persistent threat (APT) makes to the operating system, configuration and/or data files, processes, memory, etc. Other patterns can also include new/unknown files including data accumulation for exfiltration and endpoint-initiated communications/connections that can indicate command and control.

All solutions in this space have a response capability. At a bare minimum, response capabilities include common alerting of incidents to a log management, security incident and event management (SIEM), or similar solution. However, more advanced detection solutions provide mitigation and/or remediation capabilities. While many in the market are still building their confidence around these new remediation capabilities and mitigation techniques while continuing to reimagine machines, some are taking full advantage of the capabilities to initiate surgical strikes against malware on the infected system, leveraging the automation and accuracy to save significant time and money, both for the IT teams and for the affected individual. On average, the time savings of this technique over rebuilding a system is three hours of IT time per infected system plus the end-user time to re-customize the desktop, apps, and other systems settings, as well as reloading data.

Some solutions provide both prevention and detection. A layered security approach is a hallmark of a mature security program, making this the best strategy for vendor and consumer alike. Given that persistent and skilled attackers may find a way past prevention, having detection on the system as well is a winning play. The best option is a single-vendor solution to avoid possible solution conflicts, but there are also a number of solution partnerships that are well-tested to provide strong protection while minimizing potential impacts.
The Market and Maturity

As is a common problem with reports, no two seem to cover the same exact scope. This report overlaps with IDC’s definition of “Specialized Threat Analysis and Protection” (STAP) but does not entirely match up from a vendor-identification perspective, making the estimate outcomes significantly different. From IDC, “Endpoint STAP products use behavioral analysis of memory and application operations. It primarily consists of an agent or sensor on devices that monitor system processes and files for signs of anomalous behavior or attempt to prevent suspicious files from executing.”\(^1\)

Though antivirus and endpoint protection have been around for over 20 years, the next-generation endpoint security market is very young, but accelerating very quickly along the growth curve. According to EMA’s report “Data-Driven Security Reloaded: A Look into Data and Tools Used for Prevention Detection and Response,” next-generation endpoint security solutions have about a 32% market penetration. Given the overall market attention paid to the endpoint and that level of penetration, EMA estimates the market to be just at “The Chasm” point of the market curve. Sitting between the emerging and growth segments, “The Chasm” is the point at which the technologies are known well enough and have enough proof in the marketplace that the growth curve of market adoption accelerates more steeply. In this area, the market still sees innovation, but it also sees consolidation with the older, more cash-rich organizations acquiring the much smaller innovators. (See Figure 3)

![Figure 3: Market Evolution Curve and “The Chasm”](image)

Other facts that support this estimate of the market stage include the following:

1. There is a yearly increase in the number of vendors supplying next-generation endpoint security.
2. There are at least 25 active vendors, all with large-to-extraordinary growth over the last several years.
3. Of the 25 identified vendors, most are five years old or less.

\(^1\) IDC 2015 STAP Market Sizing Report
Focus on the endpoint for the protection market began to dip in 2007, just after the initial (and very successful) marketing campaign of one of the leading network threat detection vendors. However, attention began to return to the endpoint market around 2010, with significant resurgence starting in 2012. Figure 5 clearly shows acceleration of market entrants at that point due to increased focus and product demand.
Research Participants

Participants

<table>
<thead>
<tr>
<th>Participating Vendors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avecto</td>
</tr>
<tr>
<td>CounterTack</td>
</tr>
<tr>
<td>Fidelis Cybersecurity</td>
</tr>
<tr>
<td>LightCyber</td>
</tr>
<tr>
<td>SentinelOne</td>
</tr>
<tr>
<td>Carbon Black</td>
</tr>
<tr>
<td>CrowdStrike</td>
</tr>
<tr>
<td>FireEye HX</td>
</tr>
<tr>
<td>Malwarebytes</td>
</tr>
<tr>
<td>Sophos</td>
</tr>
<tr>
<td>Bromium</td>
</tr>
<tr>
<td>Cybereason</td>
</tr>
<tr>
<td>Hexis Cyber Solutions</td>
</tr>
<tr>
<td>Outlier</td>
</tr>
<tr>
<td>Tanium*</td>
</tr>
<tr>
<td>Cisco</td>
</tr>
<tr>
<td>Cylance</td>
</tr>
<tr>
<td>IBM Apex</td>
</tr>
<tr>
<td>Promisec</td>
</tr>
<tr>
<td>Triumfant</td>
</tr>
<tr>
<td>Comodo</td>
</tr>
<tr>
<td>Deep Instinct</td>
</tr>
<tr>
<td>Invincea</td>
</tr>
<tr>
<td>RSA ECAT</td>
</tr>
<tr>
<td>Ziften</td>
</tr>
</tbody>
</table>

Table 1: Next-Generation Endpoint Security Providers Participating in Research

Declined to Participate

<table>
<thead>
<tr>
<th>Non-Participating Vendors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avast</td>
</tr>
<tr>
<td>Intel Security</td>
</tr>
<tr>
<td>Symantec</td>
</tr>
<tr>
<td>Confer</td>
</tr>
<tr>
<td>Kaspersky</td>
</tr>
<tr>
<td>Trend Micro</td>
</tr>
<tr>
<td>Endgame*</td>
</tr>
<tr>
<td>Palo Alto Networks</td>
</tr>
<tr>
<td>Webroot</td>
</tr>
</tbody>
</table>

Table 2: Next-Generation Endpoint Security Providers Not Participating in Research

Market Share

With the array of competitors in the space, market shares are fairly small. Interestingly, the market has observed major players emerging from the following three key areas:

1. Staple players in terms of longevity in maintaining and growing market share. (Carbon Black, Comodo, Malwarebytes, and Sophos)
2. Key disruptors acquiring endpoint protection technology, adding it to their portfolio and successfully leveraging their brand to acquire market share. (Cisco, Fidelis Cybersecurity, and FireEye)
3. New brands with highly innovative technology and aggressive marketing able to gobble market share with their new technology. (Bromium, CrowdStrike, Cylance, Invincea, [and Tanium])

EMA evaluated market share and market stature using three different variables. Each variable speaks to a core aspect of the market and how consumers perceive it:

1. **Largest single deployment** – This variable speaks to scalability of the product from the enterprise perspective. All of the participants had single deployments in the tens of thousands, and many had single deployments in the hundreds of thousands.
2. **Customer licenses** – This variable speaks to the overall penetration of the solution provider in the marketspace.
3. **Revenue** – This variable speaks to the financial viability of the solution provider.

As readers compare the rankings by revenue and licensing, they should note some ranking alignments and some disparities. These features demonstrate the differences in promotional and “strategic” pricing as well as early beta customer license incentives, the latter of which is a significant issue with so many of the companies being very young.

---

*a* See discussion on Tanium in “New Entrants, Acquisition and Market Consolidation” and “Vendor Profiles”

*b* Endgame is the vendor that has shifted focus to threat hunting
**Largest Single Deployment**

For largest deployment, vendors tied if their deployments were within 10,000 licenses of each other.  
*(Within the tied levels, vendors are listed in alphabetical order.)*

<table>
<thead>
<tr>
<th>Company Name</th>
<th>Rank by Largest Deployment (Ties within 10K)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avecto</td>
<td>1</td>
</tr>
<tr>
<td>Fidelis Cybersecurity</td>
<td>2</td>
</tr>
<tr>
<td>Bromium</td>
<td>3</td>
</tr>
<tr>
<td>Invincea</td>
<td>4</td>
</tr>
<tr>
<td>Malwarebytes</td>
<td>4</td>
</tr>
<tr>
<td>Carbon Black</td>
<td>5</td>
</tr>
<tr>
<td>Cisco</td>
<td>5</td>
</tr>
<tr>
<td>Cyrence</td>
<td>5</td>
</tr>
<tr>
<td>CrowdStrike</td>
<td>6</td>
</tr>
<tr>
<td>Cybereason</td>
<td>6</td>
</tr>
<tr>
<td>IBM Apex</td>
<td>7&lt;sup&gt;c&lt;/sup&gt;</td>
</tr>
<tr>
<td>Promisec</td>
<td>7</td>
</tr>
<tr>
<td>RSA ECAT</td>
<td>7</td>
</tr>
<tr>
<td>Ziften</td>
<td>7</td>
</tr>
<tr>
<td>Hexis Cyber Solutions</td>
<td>9</td>
</tr>
<tr>
<td>Triumfant</td>
<td>9</td>
</tr>
<tr>
<td>Outlier</td>
<td>10</td>
</tr>
<tr>
<td>CounterTack</td>
<td>11</td>
</tr>
<tr>
<td>Light Cyber</td>
<td>12</td>
</tr>
<tr>
<td>SentinelOne</td>
<td>12</td>
</tr>
<tr>
<td>Comodo</td>
<td>13</td>
</tr>
<tr>
<td>Deep Instinct</td>
<td>No Data&lt;sup&gt;d&lt;/sup&gt;</td>
</tr>
<tr>
<td>FireEye HX</td>
<td>No Data&lt;sup&gt;e&lt;/sup&gt;</td>
</tr>
<tr>
<td>Sophos</td>
<td>No Data&lt;sup&gt;f&lt;/sup&gt;</td>
</tr>
</tbody>
</table>

Table 3: Next-Generation Endpoint Security Providers Ranked by Largest Single Deployment

All vendors ranked through number eight have at least 100,000 endpoints being deployed and managed at a single customer, demonstrating significant ability to scale. Even the vendors ranked from nine to the end of the list have reported single deployments in the multiple tens of thousands, indicating that scale is not an issue for them either.

<sup>c</sup> IBM ranking is estimated to be at least 100,000 based upon its target market/relationships and other research factors.

<sup>d</sup> Deep Instinct did not provide this information

<sup>e</sup> FireEye has a new next-generation endpoint security solution. FireEye did not release data on its largest deployment. Given the newness of the service, there is not enough data to make an estimate.

<sup>f</sup> Sophos has a new next-generation endpoint security solution. Sophos did not release data on its largest deployment. Given the newness of the service, there is not enough data to make an estimate.
A top item in this category is the agentless solution, of which there are three: LightCyber, Outlier and Promisec. With an agentless installation, they have the advantage of deploying in far less time than agent-based solutions. Though there are trade-offs that must be considered based upon requirements, these solutions can deploy in several days, or even in as little as a few hours, depending upon overall environment size, without the need to make changes on the endpoints themselves. The trade-off is that prevention is not possible. These solutions allow only detection and response. Also, the technology implementation and the interval between polling cycles may affect successful attack dwell time.

**Market Share by Customer Licenses**

Market share by licenses is significant because, aside from there only being so many seats to fill, it demonstrates overall penetration of the vendor in the marketplace. The volume of licenses may be a more accurate indication of the overall size of the company than revenue due to the fact that you can't give away a poor product at any scale, especially in a commercial environment where people's reputations and livelihood are at stake.
For easy reference, Table 4 contains the ranking (market share ranking tied within a percentage point).

*(Within the tied levels, vendors are listed in alphabetical order.)*

<table>
<thead>
<tr>
<th>Company Name</th>
<th>Rank by Licenses Sold (Ties within 1%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Carbon Black</td>
<td>1</td>
</tr>
<tr>
<td>Cisco</td>
<td>2</td>
</tr>
<tr>
<td>Fidelis Cybersecurity</td>
<td>2</td>
</tr>
<tr>
<td>Avecto</td>
<td>3</td>
</tr>
<tr>
<td>Cylance</td>
<td>3</td>
</tr>
<tr>
<td>Invincea</td>
<td>4</td>
</tr>
<tr>
<td>Malwarebytes</td>
<td>4</td>
</tr>
<tr>
<td>Cybereason</td>
<td>5</td>
</tr>
<tr>
<td>Promisec</td>
<td>6</td>
</tr>
<tr>
<td>RSA ECAT</td>
<td>6</td>
</tr>
<tr>
<td>Bromium</td>
<td>7</td>
</tr>
<tr>
<td>IBM Apex</td>
<td>7</td>
</tr>
<tr>
<td>Sophos</td>
<td>7</td>
</tr>
<tr>
<td>CounterTack</td>
<td>8</td>
</tr>
<tr>
<td>CrowdStrike</td>
<td>8</td>
</tr>
<tr>
<td>SentinelOne</td>
<td>8</td>
</tr>
<tr>
<td>Ziften</td>
<td>8</td>
</tr>
<tr>
<td>Comodo</td>
<td>9</td>
</tr>
<tr>
<td>Deep Instinct</td>
<td>9</td>
</tr>
<tr>
<td>FireEye HX</td>
<td>9</td>
</tr>
<tr>
<td>Hexis Cyber Solutions</td>
<td>9</td>
</tr>
<tr>
<td>Light Cyber</td>
<td>9</td>
</tr>
<tr>
<td>Outlier</td>
<td>9</td>
</tr>
<tr>
<td>Triumfant</td>
<td>9</td>
</tr>
</tbody>
</table>

Table 4: Next-Generation Endpoint Security Providers Ranked by Licenses Sold
Market Share by Revenue

Market share by revenue is the age-old standard and a very relevant measure. The issue with revenue is that, despite the list price, there is no common price. As larger companies, prospects considered “strategic,” and tougher/timelier negotiators may get better pricing, revenue is all over the place. The percentage cost of support for perpetual licensing also varies because of the same factors. However, money is king in business, and revenue shows how viable/solvent a company is and thus how likely it is to weather economic downturns and other financial crises.

![Figure 7: Top 5 Ranked Vendors’ Market Share Market Share by Revenue](image-url)
For easy reference, Table 5 contains the rankings (market share ranking tied within a percentage point).

*Within the tied levels, vendors are listed in alphabetical order.*

<table>
<thead>
<tr>
<th>Company Name</th>
<th>Rank by Market Share (Ties within 1%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Carbon Black</td>
<td>1</td>
</tr>
<tr>
<td>Cisco</td>
<td>2</td>
</tr>
<tr>
<td>Bromium</td>
<td>3</td>
</tr>
<tr>
<td>Malwarebytes</td>
<td>3</td>
</tr>
<tr>
<td>CrowdStrike</td>
<td>4</td>
</tr>
<tr>
<td>Invincea</td>
<td>5</td>
</tr>
<tr>
<td>Avecto</td>
<td>6</td>
</tr>
<tr>
<td>Comodo</td>
<td>6</td>
</tr>
<tr>
<td>Sophos</td>
<td>6</td>
</tr>
<tr>
<td>IBM Apex</td>
<td>7</td>
</tr>
<tr>
<td>Countertack</td>
<td>8</td>
</tr>
<tr>
<td>Fidelis Cybersecurity</td>
<td>8</td>
</tr>
<tr>
<td>FireEye HX</td>
<td>8</td>
</tr>
<tr>
<td>Cybereason</td>
<td>8</td>
</tr>
<tr>
<td>Hexis Cyber Solutions</td>
<td>8</td>
</tr>
<tr>
<td>SentinelOne</td>
<td>8</td>
</tr>
<tr>
<td>Promisec</td>
<td>9</td>
</tr>
<tr>
<td>RSA ECAT</td>
<td>9</td>
</tr>
<tr>
<td>Ziften</td>
<td>9</td>
</tr>
<tr>
<td>Light Cyber</td>
<td>9</td>
</tr>
<tr>
<td>Triumfant</td>
<td>9</td>
</tr>
<tr>
<td>Outlier</td>
<td>9</td>
</tr>
<tr>
<td>Deep Instinct</td>
<td>9</td>
</tr>
</tbody>
</table>

Table 5: Next-Generation Endpoint Security Providers Ranked by Revenue
Aggregate Ranking

The number that may tell the best story is the average of license and revenue rankings. If a vendor keeps a relatively level pricing structure, then their rankings by revenue and by licenses should be consistent. On the other hand, the organizations that are giving away large numbers of licenses, though they are getting market saturation, will have a significantly lower ranking by revenue, regardless of how much they are making, unless the average price is significantly higher than average.

(Within the tied levels, vendors are listed in alphabetical order.)

<table>
<thead>
<tr>
<th>Company Name</th>
<th>Aggregate Ranking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Carbon Black</td>
<td>1.0</td>
</tr>
<tr>
<td>Cisco</td>
<td>2.0</td>
</tr>
<tr>
<td>Malwarebytes</td>
<td>3.5</td>
</tr>
<tr>
<td>Avecto</td>
<td>4.5</td>
</tr>
<tr>
<td>Fidelis Cybersecurity</td>
<td>4.5</td>
</tr>
<tr>
<td>Invincea</td>
<td>4.5</td>
</tr>
<tr>
<td>Bromium</td>
<td>5.0</td>
</tr>
<tr>
<td>CrowdStrike</td>
<td>6.0</td>
</tr>
<tr>
<td>Cybereason</td>
<td>6.0</td>
</tr>
<tr>
<td>IBM Apex</td>
<td>6.5</td>
</tr>
<tr>
<td>Sophos</td>
<td>6.5</td>
</tr>
<tr>
<td>Promisec</td>
<td>7.0</td>
</tr>
<tr>
<td>RSA ECAT</td>
<td>7.0</td>
</tr>
<tr>
<td>Comodo</td>
<td>7.5</td>
</tr>
<tr>
<td>Countertack</td>
<td>7.5</td>
</tr>
<tr>
<td>SentinelOne</td>
<td>7.5</td>
</tr>
<tr>
<td>FireEye HX</td>
<td>8.0</td>
</tr>
<tr>
<td>Hexis Cyber Solutions</td>
<td>8.0</td>
</tr>
<tr>
<td>Ziften</td>
<td>8.0</td>
</tr>
<tr>
<td>Deep Instinct</td>
<td>8.5</td>
</tr>
<tr>
<td>Light Cyber</td>
<td>8.5</td>
</tr>
<tr>
<td>Outlier</td>
<td>8.5</td>
</tr>
<tr>
<td>Triumfant</td>
<td>8.5</td>
</tr>
</tbody>
</table>

Table 6: Next-Generation Endpoint Security Providers Ranked by Aggregate of Licenses and Revenue
Market Size and Forecasts

The next-generation endpoint security market is part of both the larger Endpoint Software Security Market, identified by IDC, which is currently over $9 billion and includes traditional antivirus as the majority of its revenue, and the even more expansive Endpoint Security market, identified by “MarketsandMarkets,” which is cast at over $11 billion and includes all of the previous plus Antispyware/Antimalware, Firewall, Endpoint Device Control, Intrusion Prevention, and Endpoint Application Control. Both of those markets include commercial and consumer purchases.

The vendors included align most closely with the Specialized Threat Analysis and Protection (STAP), though that definition included perimeter protection solutions and endpoint protection solutions. This report required an endpoint focus and seemed to include more vendors than the IDC marketspace, though the exact alignment is difficult since the IDC report had some vendors lumped together without delineating which were included. This particular endpoint market also has negligible consumer market at this time.

Total Revenue and Growth Rate

Total market revenue, including allowances for other smaller vendors is listed in Table 7.

<table>
<thead>
<tr>
<th>Est Value 2015</th>
<th>Low-Range NGES Market Value</th>
<th>Mid-Range NGES Market Value</th>
<th>High-Range NGES Market Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$314,775,000</td>
<td>$426,462,500</td>
<td>$538,150,000</td>
</tr>
</tbody>
</table>

Table 7: Next-Generation Endpoint Security Market Revenue 2015

Though most of the vendors are on a calendar year for financial reporting, not all follow this standard. The vendors that were able to provide revenue information have reported similar growth rates between 2014 and 2015 as they reported in 2013 to 2014.

The larger endpoint security and endpoint software markets are projected to experience compounded annual growth rates (CAGR) between 5% and 10% over the next five years. This is far below the current average in the next-generation endpoint security market, which is 124%; in multiple cases vendors exceeded a 250% annual growth rate. However, this type of growth rate from the market is unsustainable over the long haul, though it is entirely possible that both the smaller companies and the market leaders will continue to see very strong double- and even triple-digit growth over the next few years, which is why the five-year CAGR for this market is projected at 67%. Table 8 depicts the details of the projected revenue and CAGR.

<table>
<thead>
<tr>
<th>Conservative</th>
<th>Low NGES Market Value</th>
<th>Mid NGES Market Value</th>
<th>High NGES Market Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Est Value 2016</td>
<td>$535,117,500</td>
<td>$724,986,250</td>
<td>$914,855,000</td>
</tr>
<tr>
<td>Est Value 2017</td>
<td>$829,432,125</td>
<td>$1,123,728,688</td>
<td>$1,418,025,250</td>
</tr>
<tr>
<td>Est Value 2018</td>
<td>$1,202,676,581</td>
<td>$1,629,406,597</td>
<td>$2,056,136,613</td>
</tr>
<tr>
<td>Est Value 2019</td>
<td>$1,623,613,385</td>
<td>$2,199,698,906</td>
<td>$2,775,784,427</td>
</tr>
<tr>
<td>Est Value 2020</td>
<td>$2,029,516,731</td>
<td>$2,749,623,632</td>
<td>$3,469,730,534</td>
</tr>
</tbody>
</table>

Table 8: Next-Generation Endpoint Security Market Growth Estimates (Conservative)
EMA Perspective

Pivotal Change in the Market

A crucial factor in the growth of the next-generation endpoint security market will be whether vendors and consumers of the technology can convince auditors and regulators that this technology is sound and can replace antivirus. Most of the vendors currently market their solutions as complementary to antivirus because most auditors and regulators can’t get past the letter of the law (or regulations), most of which contain the word antivirus. Additionally, they may not be educated enough about the advantages of the new cutting-edge solutions. Few auditors are willing to put their names on the lines for having sanctioned an alternate product if the company using it is breached. Vendors also market their solutions as complementary when they could in many cases actually replace antivirus because the vendors don’t want prospects to think that implementing their solution will cause a rip-and-replace scenario for tens of thousands to hundreds of thousands of endpoints.

The aggressive model below indicates that the market could increase by over half a billion dollars if the shift in acceptance takes place. If the shift in acceptance takes place, much of the aggressive model depends upon when the shift takes place. At the current estimate, the shift could add a billion dollars to the revenue pool.

<table>
<thead>
<tr>
<th></th>
<th>Low NGES Market Value</th>
<th>Mid NGES Market Value</th>
<th>High NGES Market Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Est Value 2016</td>
<td>$629,550,000</td>
<td>$852,925,000</td>
<td>$1,076,300,000</td>
</tr>
<tr>
<td>Est Value 2017</td>
<td>$1,070,235,000</td>
<td>$1,449,972,500</td>
<td>$1,829,710,000</td>
</tr>
<tr>
<td>Est Value 2018</td>
<td>$1,805,352,500</td>
<td>$2,174,958,750</td>
<td>$2,744,565,000</td>
</tr>
<tr>
<td>Est Value 2019</td>
<td>$2,167,225,875</td>
<td>$2,936,194,313</td>
<td>$3,705,162,750</td>
</tr>
<tr>
<td>Est Value 2020</td>
<td>$2,709,032,344</td>
<td>$3,670,242,891</td>
<td>$4,631,453,438</td>
</tr>
</tbody>
</table>

Table 9: Next-Generation Endpoint Security Market Growth Estimates (Aggressive)

Taking the Next Step

Two vendors, Carbon Black and SentinelOne have taken the extra step to have their solutions certified as antivirus replacements. This was not a trivial exercise, but it offers an additional payoff for those companies. If either of these companies gains proportionately more market share over the next year, other vendors may decide to make the investment in certification as well, but both will still have a head start of more than a year.

If widespread certification happens, the cash cow the traditional vendors are still experiencing will be in jeopardy, and the relative size of the market could expand a hundredfold, even at the high estimate.

Speaking about no vendor in particular but about the group as a whole, these types of solutions show they are more effective than traditional antivirus. If they weren’t, the market would not be experiencing such high growth. These solutions should be evaluated by the appropriate regulators to fill the antivirus role.
**Educating Auditors and Regulators**

To open the market up for the next level of competition, the next-generation security organizations will need to influence auditors and regulators to expand their definitions and mentality to allow for the adaptation of technology. It is well known that regulators and legislators lag behind technology, so it will be up to the market participants to work in “coopetition” for their greater good.

The current openness of the market leads EMA to believe that this type of mass effort will not occur anytime soon. But when the companies hit the glass ceiling, it will be an option on the table. It would be smarter for companies to be proactive on this point so they can maintain their momentum, but ultimately it comes down to the cost and time of resources involved in accomplishing the task. Since changing policy takes time, it would be better to start early and slow than to wait.

**Differentiation**

In a market with more than 25 participants, creating and maintaining product differentiation is difficult, maybe even impossible. As EMA has seen time and time again, as soon as a thought-leading marketer is able to create a new concept and differentiate his company or product and gain attention, other less-imaginative marketers latch on to the concept and create their own campaigns based on the original.

Though imitation is the sincerest form of compliment, it is frustrating not only for the company but also for the consumers. Every year we see similar messaging come out from competitors of every cyber security player. It is up to the marketers to keep their messages simple and focus on the components that are most unique to their solutions.

Since most vendors have machine learning capabilities, those sharing that capability need to help prospects see how their intellectual property in the space makes them different. Why are one vendor’s algorithms or approach better?

Some vendors use cloud for off-system threat analysis; others use it for threat data augmentation. Some require the cloud portion to operate; others do not. What differentiates that implementation and integration from the others?

Prospects in the market must devise and prioritize a list of requirements and use cases that best fit their businesses and use those criteria to differentiate among the available solutions.

**New Entrants, Acquisition, and Market Consolidation**

Just as Cisco, Palo Alto Networks, FireEye, Carbon Black, Fidelis Cybersecurity, IBM, and RSA have already leveraged acquisition as a means to enter the market, others are likely to do so over the next few years. Each of the players has significant intellectual property, and as the smaller companies prove themselves, they will be ripe for the picking. Acquisition could come from a number of sources including the following:

- Other mainstay providers in the antivirus space seeking to augment their existing technology and market appeal
- Vendors that want to augment their current network threat detection portfolios
- Mergers of technologies to maintain market strength against leaders

However, if the growth rates continue as expected, each company will ripen for the picking over the next three years, and we are guaranteed to see some changes.
Tanium
Another interesting situation is Tanium (company profile included below). Tanium has been taking the endpoint operations business by storm. They have announced partnerships and integrations and have had numerous of large deals close. Tanium has a lot of potential in the security market and as such, deserves mention in this report. The company already delivers facets of endpoint security very effectively. The primary reason Tanium is not included in the rankings in the report is because of its lack of proactive capability. Tanium’s technology is based upon querying and response. They do not have a proactive capability, which is a foundational requirement for next generation endpoint security. In fact, that particular characteristic has been a foundational characteristic of all endpoint security technologies since the start of antivirus.

If Tanium adds a policy-based, proactive alerting and notification capability to their solution, they will have to be considered a serious player not only in the NGES market but any of the endpoint security markets.

Expanding into the Consumer Segment
The option of expanding into the consumer segment is less likely in the near future as the resources involved are quite significant. However, as providers evolve their solutions, including a partnership with an ISP as a perk could help market penetration. Going retail would be another way to accomplish the same thing. Aside from the resources involved in moving in this direction, the endpoint and policy management aspects of these solutions are currently too complex for most end users. To meet the consumer market, not only would the vendors need more resources to staff call/support centers, but management aspects of the applications would have to be simplified to enable setting policies with a few checkboxes to avoid overtaxing the average consumer. Only the largest players could consider this move at the current time, and with the commercial market growing as quickly as it is, there doesn’t seem to be much incentive to move in that costly direction.

Comments on Current Market Leaders
Of the top four market leaders by aggregate, Carbon Black was the clear leader in terms of both market share and revenue of its solution. It should be noted that Cisco had higher gross revenues, but that revenue included income from more than just their endpoint security. Every reasonable attempt was made to segment out the revenues fairly based on an apples-to-apples comparison.

From a licensing perspective, a similar issue arises with Carbon Black and Malwarebytes. Malwarebytes would have had significantly more licenses if its consumer solutions, which make up the majority of the company’s revenue at this point, were included. These variances must be taken into account to make the most accurate disclosure possible.

Cisco, Bromium, and Malwarebytes are each maneuvering as viable competitors for the top spot, while Carbon Black pushes forward doing all in its power to maintain its position. Competition will be fierce over the next few years; the playing field is currently wide open, so it is anyone’s game.
Vendor Profiles (Listed in alphabetical order)

Analyst Notes

1. Some organizations chose not to fully respond to the questionnaire based upon company policies or other current situations; a few chose not to participate; several vendors failed to respond at all to numerous requests. Non-responsive vendors are identified in their profile. However, reasonable efforts were made to research these vendors externally and use that data where it was available.

2. EMA recognizes that some smaller vendors have not been included in the report. Based on time boundaries for report delivery and those vendors’ small impact on the market from an overall revenue perspective, the decision was made to move ahead without them. The forecasts made attempt to accommodate for these vendors in the range estimates made.

3. An invitation to participate in the research project included the major antivirus companies serving the commercial markets that also claim some form of next generation endpoint security to try to understand how their solutions qualify for next-generation endpoint security. These vendors include (in alphabetical order) Avast, Comodo, Intel Security (Formerly McAfee), Symantec, Kaspersky, Sophos, and Trend Micro. Each of the traditional antivirus vendors claim next-generation endpoint security capabilities but despite multiple requests for response, only two, Sophos and Comodo, responded to the information request. Because of lack of response, EMA was unable to render a positive decision on these vendors’ ability to deliver on next-generation endpoint protection, so they were therefore excluded. This stance is also in line with the general commercial consumer market for these vendors and their perception of the efficacy of those solutions in defending endpoints against APT’s. As these traditional vendors continue to move into next-generation capabilities, it is highly possible that their market dollars will increase and associated market shares will change.

Invited but No Response

A number of vendors were invited to participate but in the research but did not respond to requests for either the written questionnaire or a phone briefing:

**Avast, Intel Security, Kaspersky, Symantec and Trend Micro** are all mainstays of the traditional antivirus market. They also have marketing around solutions to indicate they have next-generation endpoint security capabilities either built into their traditional antivirus platforms or have additional service offerings.

**Palo Alto Networks** is a broad provider of security solutions including perimeter, network, mobile, web threat prevention, and endpoint security, which it gained through its Cyvera acquisition in 2014. Cyvera was a small Israeli startup launched in 2011 which EMA briefed with shortly before the acquisition.

**Webroot** is a long-time player in the web threat protection market and has in the last six years expanded its portfolio to include other solutions and services including next-generation endpoint protection

**Confer** is a small next-generation endpoint security vendor providing advanced threat prevention and incident response for endpoints, servers and cloud workloads. Confer’s patented technology uses enterprise-wide telemetry and data science to analyze, adapt and eliminate manual processes, and facilitates an intelligent and efficient approach to securing the enterprise.

EMA has no information as to why these vendors did not participate in the research but hopes that they will be able to participate when EMA updates the study.
Vendor Changes

Endgame began developing its technology platform and agent technology for use within US Federal Government agencies. After significant success in that space, the company decided to expand into the commercial next-generation endpoint security space. Though its technology won multiple proof-of-concept tests and the resulting contracts, Endgame has since determined that its true forte is threat hunting and has refocused on that specific segment of the market. Endgame is still a minor player in the commercial sector, so the company’s impact on the market sizing is negligible. As Endgame grows, it could impact the dollar spend on other vendors in the sector, not as a replacement solution, but as an augmentation to other vendors’ capabilities.
Avecto

Description:

Avecto DefendPoint provides a three-pronged approach using privilege management, application control and application sandboxing across Windows environments. Privilege management dramatically reduces the attack surface of the Windows endpoint, mitigating as much as 97% of the Windows’ critical vulnerabilities identified in 2014.

Avecto’s privilege management allows granular elevation of user and application administrative privilege, as the user logs on with a safer and more secure standard Windows account. This allows the workforce to be empowered without having to give either full administrative control, granting users the tools they need to remain productive while simultaneously allowing the organization to achieve compliance, control, and oversight of their activities.

Application control builds on the least privilege environment, allowing organizations to take a pragmatic but effective approach to application whitelisting. This control allows only known good applications to run, providing protection against both known and unknown threats by denying any unknown applications the ability to execute.

The third layer is the sandboxing module, which allows Avecto to isolate applications interacting with untrusted content. Sandbox technology isolates their actions, denying access to the user’s environment and corporate data. The sandbox also provides an additional context (environment), distinct from the context in which the user operates, allowing additional application policies to be applied, further restricting the known good applications which run within the sandbox, while allowing users to remain free and productive in their environments.

Analyst Notes:

Avecto previously competed in the privileged management space but its technology development path has allowed it to expand into competing in the next-generation endpoint space. The added benefit is they have built layered interlocking capabilities that can provide a strong defensive position for their customers.
**Bromium**

**Description:**
Bromium is one of only two major players in the next-generation endpoint space that approaches prevention through system virtualization. However, Bromium is the only solution using CPU-enforced isolation implemented outside of the operating system making it highly resistant to even kernel-level exploits. The Bromium Advanced Endpoint Security solution deploys virtual machine technology termed “micro-VMs” to provide hardware-based isolation of tasks such as navigating to a Web site, opening an Office document or Adobe PDF file, and so on. The system is divided into trust zones so only tasks and data within the same trust zone can freely interact. The micro-VMs contain all activity within that trust zone. If one of the processes should try to contact another process or resource outside of the micro-VM it is unable to do so, thus preventing malware from spreading or attacking other parts of the system or network. Data collected from within a micro-VM is labeled by its trust zone so if it has embedded malware that attempts to activate at any time after download or access, that malware is still contained in an isolated environment. This functionality prevents attacks including kernel-based malware. Bromium not only isolates less trusted processes, but in response to a violation, Bromium automatically shuts down and destroys the micro-VM upon completion of the task.

As of February 10th, 2016, Bromium has expanded its portfolio. Bromium Advanced Endpoint Security includes a new host monitoring capability in addition to its flagship micro-virtual machine-based protection capabilities. The Bromium Endpoint Monitoring module addresses two primary use cases. The first addresses systems that were compromised pre-installation of the core Bromium Advanced Endpoint Security product. The second deals with older systems that cannot run the micro-VM technology due to system configuration and performance limitations. The product monitors the host OS using behavioral analysis to identify malicious activity in real-time. Post-detection, it notifies the user/administrator of the attack and its characteristics.

Both Bromium products communicate with the Bromium central management solution called Bromium Threat Analysis. Threat Analysis is a centralized security application that works in conjunction with the Bromium Endpoint Protection and Bromium Endpoint Monitoring modules, which are installed on endpoints in the organization. Bromium Threat Analysis offers visualization to deliver immediate, actionable intelligence on attacks and easy search for IOCs across the endpoint base, enabling security teams to quickly analyze and respond to threats. The Bromium Threat Analysis module runs on the Bromium Enterprise Controller (BEC).
Carbon Black (Formerly Bit9 + Carbon Black)

Description: Carbon Black enables organizations to arm their endpoints by combining continuous, real-time visibility into every computer in their environments; real-time signature-less threat detection; incident response that combines a recorded history with live remediation; and prevention that is proactive and customizable.

Customizable prevention is primarily provided through the Carbon Black Enterprise Protection product (formerly Bit9 Security Platform) which dramatically reduces an organization’s attack surface while providing administrators with the flexibility they need to ensure the right balance between protection and access. It offers three primary prevention strategies which customers can deploy in any mix they want to match the needs of their business:

Default-Deny is Carbon Black’s advanced application whitelisting capability and the heart of its proactive prevention capabilities. This proven approach to policy-driven and trust-based application control has been optimized to make it easy to ensure that only software trusted by administrators can run in the environment. This approach allows Carbon Black to adapt to new versions of trusted applications without user or administrator intervention.

Detect-and-Deny uses advanced threat indicators from Carbon Black Threat Intel (formerly Bit9 + Carbon Black Threat Intelligence Cloud) as a signature-less approach to prevention. This strategy automatically identifies and bans malicious files either on a single-machine or across the deployed environment.

Detonate-Deny leverages a next-generation sandboxing service that detonates and evaluates endpoint files. If a file is found to be suspicious, Carbon Black can either automatically ban the file or submit it for IT review and approval.

Carbon Black’s Enterprise Response solution (formerly Carbon Black) provides insights into the history/progression of attacks by continuously recording all endpoint activity and centralizing and correlating that data with unified intelligence sources. It reveals a complete kill chain that pinpoints the attacks’ root cause and then provides live threat containment, banning and remediation capabilities. Built entirely on open APIs, Carbon Black Enterprise Response pushes and pulls data through the security infrastructure to automate and enhance adaptive threat response processes.

Carbon Black is also the only solution independently certified to perform as endpoint protection in a PCI-DSS regulated environment and one of only two that is certified as a replacement for antivirus.
Cisco Systems

Description:
Based on the Immunet engine acquired through SourceFire, Cisco AMP for Endpoints has been advanced to provide prevention and detection of malware threats using global threat intelligence, file hash disposition, and numerous threat hunting capabilities; detection and blocking of known malicious files based on file signatures (file reputation), fuzzy fingerprinting capabilities; numerous detection engines (such as ClamAV, SPERO and ETHOS); and malware analysis (static, dynamic, sandboxing, forensic, MBR, etc.). Many of these services are offered for deployment both on-premises or within hosted or cloud services. AMP also provides detection and aids response using retrospective security. AMP can record the activity of files already on a customer’s endpoints, regardless of the file’s disposition and alert security teams to any malicious behavior that it identifies.

Since the acquisition, Cisco has been integrating AMP into its network ecosystem architecture with other Cisco products, thus creating a much broader solution than AMP had in both its Sourcefire and Immunet days. AMP functionality has been extended beyond the endpoint agent into other Cisco solutions such as Web Security (appliance and cloud), Cyber Threat Defense, Cisco ASA and ISR, and Firepower NGIPS.

Analyst Notes:
Much to Cisco’s credit, AMP has seen much better development since being acquired than many of Cisco’s past technology acquisitions. This integration, combined with other acquisitions such as Lancope and OpenDNS, could move Cisco into a key role over the next few years. Cisco’s acquisition of ThreadGrid is also playing a part in Cisco’s overall strategy for integrating endpoint security with their network components.

Category: Prevention, Detection and Response for Windows, MAC, Linux, and Android systems

Started: 2008/2011/2013 – While Cisco Systems has been a mainstay of the network world for many years, it is only recently they have ventured into the world of endpoint protection. The three dates listed are, in reverse order: the date Cisco acquired Sourcefire, the date Sourcefire acquired Immunet Corporation and the date that Immunet was started. It is important for readers to note that Cisco’s foundation was built through acquisition of a solution that has had its roots in the industry since 2008.

Funding: Not Applicable

Rank by largest single deployment: 5
Market share by licenses sold: 11.6%
Rank by licenses sold: 2
Market share by revenue: 16.2%
Rank by revenue: 2
2015 revenue growth: 15%–35%
Comodo

Description:
Comodo Advanced Endpoint Protection (AEP) provides a Default Deny Platform that relies on a layered approach to prevent, detect, and respond to malware threats. Using the intelligence gained from over 85 million consumer endpoints and the largest certificate authority in the world, Comodo’s default-deny platform efficiently identifies known good files (whitelist) and ensures it can identify known bad files (blacklist). All unknown files are automatically run in containment until an accelerated verdict is reached.

Using patent-pending automatic containment technology similar more in design to Docker than to virtual-machining, Comodo’s technology protects systems by containing suspect processes or executables, leveraging numerous advanced features including CPU/memory, API, service, and privilege “jailing.” The product’s automated containment employs file system, registry and object virtualization so any attempts to modify or compromise the endpoint have no effect on the underlying system. Comodo’s endpoint behavior and action based analysis engine, VirusScope, analyzes the unknown executable to determine a verdict of “good” or “bad.”

The Comodo Client is managed with Comodo IT and Security Manager (ITSM) which unifies both IT and security management into a single console ITSM allows for the configuration of security policies and visibility into the health of the endpoint, Mobile Device Management, Inventory Management, full device monitoring and even takeover, allowing for the remote provisioning, and device configuration and control. ITSM has cross-platform policies, so customers can perform tasks like restricting what a user can do on a corporate owned mobile phone, determine which applications are running in containment, remote wipe a device, and identify the geographic location of a device. With Comodo ITSM, System Administrators can get an enterprise view of all unknown files running in automated containment and even execute an enterprise-wide malware scan.

Comodo Advanced Endpoint Protection is bundled with Host Firewall, AV, HIPS, File Reputation, Web URL filtering, and more at no additional charge, which should help with those trying to transition to a more modern, advanced endpoint security approach while simultaneously trying to reduce cost or replace the “AV” budget line item. Comodo is a company that should looked at when an organization is looking for an advanced endpoint protection solution.

Category: Prevention, Detection and Response for Windows, iOS, and Android devices

Started: 1998/2013/2014 – Comodo started delivering traditional consumer antivirus since 1998. In 2013, Comodo delivered its first next generation engine for consumers but has only entered the enterprise market in the last year.

Funding: No information available

Rank by largest single deployment: 13

Market share by licenses sold: <1%

Rank by licenses sold: 9

Market share by revenue: 3.2%

Rank by revenue: 6

2015 revenue growth: 35%–55%
**CounterTack**

**Description:**
CounterTack is a provider of endpoint detection and response technology for the enterprise. Through its Sentinel solution, CounterTack uses a big data analytics foundation to provide real-time high visibility and context around operating system and binary behaviors to detect zero-days attacks, rootkits, targeted malware and advanced persistent threats, thus improving enterprise-wide advanced threat detection.

CounterTack's on Big Data architecture allows Sentinel to counter endpoint threats at-scale leveraging tamper-resistant collection at the endpoint for advanced behavioral identification of endpoint threats including laptops, servers, workstations, and mobile devices. CounterTack detection reduces the dwell time of advanced threats. Using it in conjunction with the company's other solutions, Responder Pro and Active Defense, provides enterprise class APT/ATA malware detection and analysis both on disk and in memory. Responder Pro also supports malware reverse engineering, providing operations and response teams the ability to defend the enterprise across the entire cyber kill chain.

CounterTack methodology is comprised of five key areas: (source: CounterTack)

- **Integrity** - Restoring integrity to enterprise endpoints is critical to understanding the broader threat surface and managing them effectively. Sentinel helps teams establish endpoint integrity through data collection that's tamper-resistant and transparent to users and attackers.

- **Visibility** - Every security and incident response team needs more context and visibility into behavior that's impacting workstation and server endpoints. Through continuous, real-time data collection and monitoring, Sentinel delivers the capability of continuous response to teams so they can reduce the impact of threats detected.

- **Context** - Understanding the context of threats through full attack lifecycle visibility is critical to mitigating attacks. Sentinel's automatic threat detection capability removes the guesswork of teams to understand exactly how to respond to and manage known and unknown threats.

- **Control** - Through rapid detection of advanced threats and with the context for how those threats correlate across the enterprise, Sentinel enables teams to respond, remediate and resist threats to isolate malicious behavior and eliminate threats entirely.

- **Scale** - The ability to monitor endpoints at scale is essential in order to effectively defend systems from persistent attacks across a company's endpoint environment. Sentinel leverages on-premises, big data analytics so organizations can monitor endpoints across the enterprise without impacting performance.
CrowdStrike

Description:
CrowdStrikes’ Falcon Host solution utilizes a combination of endpoint agent and cloud services to provide endpoints with a multi-layered approach for endpoint protection to prevent both malware and non-malware based threats. Included in the capabilities are hash-based application whitelisting and blacklisting, malware and exploit blocking, and cloud analysis.

Falcon Host also uses various Indicators of Attack (IOA) to provide prevention of non-malware attacks such as privilege escalation and Windows login bypass based attacks. Falcon Host’s use of IOAs to identify threats based on behavioral patterns removes reliance on signature-only protection. Falcon Host records all significant endpoint events and uses the cloud to analyze them to reduce overhead on the endpoint while delivering threat alerting in real-time. Falcon Host integrates with the CrowdStrike Falcon Host Platform to create a unique combination of technology and human expertise integrated via a 100% cloud based Security as a Service offering. (The human aspect is part of CrowdStrikes’ Managed Hunting Services.)

Because analysis is cloud–based, there is no on-premises equipment to update.

Category: Prevention, Detection and Response for Windows Linux, and MAC systems

Started: 2011

Funding: $156M in private equity funding between 2012 and 2015

Rank by largest single deployment: 6
Market share by licenses sold: 1.7%
Rank by licenses sold: 8
Market share by revenue: 8.1%
Rank by revenue: 4
2015 revenue growth: 60%–80%
Cybereason

Description:

Cybereason leverages a proprietary user space endpoint sensor (agent) technology platform to automate detection of and response to malicious operations (Malops™). The platform reconstructs the attack from both known (signature) and unknown (behavioral) elements, thus removing superfluous events from the attack chain to create a clear image of a cyberattack in context. This functionality enables enterprises to discover and respond, minimizing attack dwell time of even sophisticated targeted threats at a very early stage. Early detection and disruption significantly reduce the costs and damages caused by such attacks.

Cybereason connects individual pieces of evidence to form a complete picture of a malicious operation or “Malop.” A Malop is a collection of related suspicious activities that are highly likely to indicate a security incident, and are defined in a way that minimizes the likelihood of analysts spending time investigating benign activities. Cybereason’s Incident Investigation Console illustrates the attack story, revealing the timeline, communication, and affected endpoints and users, providing a clear blueprint for containment and remediation thus empowering action oriented decision making.

One of Cybereason’s goals is to act as a force multiplier for staff. By centralizing all of the threat indicators in a streamlined, centralized view, personnel with less experience are provided with enough decision making information to act at a higher tier, and higher tier individuals are freed from hunting to spend time on more proactive concerns.

Category: Detection and Response for Windows and MAC systems

Started: 2014

Funding: $88.6M in equity funding between 2014 and 2015

Rank by largest single deployment: 6

Market share by licenses sold: 4.2%

Rank by licenses sold: 5

Market share by revenue: 1.3%

Rank by revenue: 8

2015 revenue growth: >250%
Cylance

Description:
Cylance, Inc.’s CylancePROTECT uses artificial intelligence to proactively prevent advanced persistent threats and malware. The product’s technological approach involves small-footprint mathematical agents that work autonomously on the endpoints, using algorithmic techniques to identify abnormal and anomalous features to quickly and accurately recognize threats and predictively determine the malicious or safe intention of code prior to run time. CylancePROTECT also captures a forensics profile about the found malware for use after the item has been blocked. Thus, for systems that have CylancePROTECT, a responder will have all the requisite insight and context to seek the malware on those systems.

CylancePROTECT’s architecture consists of a small footprint agent that integrates with existing software management systems or Cylance’s own cloud console. The endpoint detects and prevents malware through the use of tested mathematical models on the host, independent of a cloud or signatures. The cloud component is the administration portal for administration and reporting. Analysis and blocking is performed on the end device. Because detection and file analysis is based on algorithmic models, there is no need for any signature updates.

Analyst Notes:
Cylance has grown significantly over the past year due to several very large strategic wins. In addition, its recent technology partnership with Dell to deliver PROTECT in Dells’ Endpoint Security Suite will also have a large, lasting, positive effect on revenues. Though Cylance asked EMA not to break out their financial information in the report at this time, their revenue was taken into account in the market models. Also, given the available information, Cylance is and will continue to be a major disruptor in the NGES market and hopes to be able to participate more fully in the next report.
Deep Instinct

Description: Deep Instinct’s product release brings deep learning to information security for the first time. Deep learning has previously been applied most often to language translation, voice and image recognition and other cognitive fields.

Because it is the first company to apply deep learning to cybersecurity, Deep Instinct brings a completely new approach to cybersecurity that is proactive and predictive. Deep learning technology is inspired by the brain’s ability to learn/adapt and the next advanced step towards artificial intelligence. Once a brain learns to identify an object, its identification becomes second nature. Similarly, as Deep Instinct’s artificial brain learns to detect any type of cyber threat, its prediction capabilities become instinctive. As a result, zero-day and APT attacks are detected and prevented in real-time with unmatched accuracy. While deep learning only claims the equivalent of 100 million synapses, as compared to a human brain’s billions, that is enough to do the job more effectively than traditional anti-malware solutions. Deep Instinct provides comprehensive defense that is designed to protect against the most evasive unknown malware in real-time, across an organization’s endpoints, servers, and mobile devices. Deep learning’s capability of identifying malware from any data source results in comprehensive protection on any device, platform or operating system.

Though on the surface Deep Instinct appears to be much like the machine learning that is the current tech buzz, according to experts in the field, the product’s underlying structure makes it much more adaptable so it can render more accurate decisions 20 to 30 percentage points higher than current machine learning solutions. Deep Instinct has trained is artificial “brain” by using massive structured and unstructured datasets that include both malicious and non-malicious files which, just like real brains, teach it the difference between the two. Similarly to a real brain, the more training it gets the better decisions it makes.

Category: Detection, and Response for Windows, Linux, MAC, Android, iOS systems

Started: 2015

Funding: Deep Instinct has received and undisclosed level and type of funding from Blumberg Capital and UST Global

Rank by largest single deployment: No information provided

Market share by licenses sold: <1%

Rank by licenses sold: 8

Market share by revenue: <1%

Rank by revenue: 9

2015 revenue growth: Deep Instinct has only emerged from stealth mode as of November 2015. Given this newness, the company does not have a revenue growth track record at this time. However, given the uniqueness of its engine, its small size, and the overall growth in the market, Deep Instinct’s growth this year should be very large.
**Fidelis Cybersecurity**

Description: 

Fidelis Endpoint is an automated endpoint threat detection and response solution that provides deep detection, visibility, and rapid response to security incidents. The solution is built on a platform ecosystem designed to leverage not only the endpoint information delivered via its agent, but also integration of other intelligence tools and threat data that the customer already has in its environment.

While the agent provides endpoint detection, threat hunting, response, forensics, and remediation, the platform has APIs and partnerships to ingest and convey commercial threat intelligence, integrate with network-based threat detection vendors, malware analysis vendors and SIEM solutions. The platform detects threats by using various methods (manual and automatic) based on industry standard formats such as OpenIOC (full multi term), STIX, YARA, and various forms of behavior-based detection. Continuous monitoring capabilities occur either on the agent or through the use of a centralized system with query capability, which enables the security analyst to take remediation action against a compromised endpoint.

**Category:** Detection and Response for Windows, MAC, Linux, Android, and iOS devices. Not all features are available in all OS platforms

**Started:** 1987/2001/2012/2014/2015 – Fidelis Cybersecurity was formed in 2001 but their next generation endpoint protection solution has a bit more history. Resolution1 Security was acquired by Fidelis Cybersecurity in 2015 following its spin out from AccessData in 2014. AccessData was founded in 1987 as an e-discovery and forensics company and started to sell Resolution1 as one of the first endpoint, detection and response solutions starting in 2012.

**Funding:** $28.4M in equity investments between 2005 and 2010. However, it should be noted that Resolution1 acquired an undisclosed debt from assets and operating costs as a result of its spin out from AccessData. Fidelis was acquired by Marlin Equity Partners in April of 2015 from General Dynamics and Fidelis acquired Resolution1 Security in May, 2015.

**Rank by largest single deployment:** 2

**Market share by licenses sold:** 11.6%

**Rank by licenses sold:** 2

**Market share by revenue:** 2

**Rank by revenue:** 8

**2015 revenue growth:** 30%–50%
**FireEye HX**

Description:
FireEye is the dominant player in the network-based threat prevention market and has made a number of acquisitions in the past few years to expand its portfolio. The key acquisition relevant to this discussion is the Mandiant acquisition in 2014, from which the FireEye MIR solution came. The MIR toolset was a foundational step in getting to HX endpoint security. MIR was difficult to productize and was therefore slow to get into market. Ultimately, HX was developed to be the platform that coalesces data from all of the FireEye systems, thus providing intelligence for analysts and hunters from across the entirety of the monitored environment. The Malware Protection System builds a 360-degree, stage-by-stage analysis of an advanced attack, from system exploitation to data exfiltration, in order to most effectively stop would-be APT attackers.

The HX solution is an appliance and an endpoint agent. HX is used to monitor endpoints for threats in cooperation with the agent that is based on the MIR technology acquired from Mandiant. HX uses threat intelligence to determine if there are corresponding indicators of compromises (IOC) when FireEye detects an attack anywhere in a network. Compromised endpoints can be isolated with a single click while security teams use the Enterprise Security Search feature to identify known or unknown threats on other endpoints. Security teams can also use the Data Acquisition feature, which allows analysts to inspect any endpoint, whether compromised or not, and to analyze all gathered information to create custom IOCs as well as to address previously unknown threats. As a result of the depth of visibility HX provides, security teams can quickly gain deeper insights into attacker behavior and tools via detailed information on the vulnerabilities and risks of a company’s on- and off-premise endpoints.

With FireEye Endpoint Security (HX series), organizations can proactively inspect, analyze, and contain known and unknown threats at any endpoint, connected or not. Endpoint Security helps security teams hunt down and stop advanced threats with an array of features that enable analysis capabilities, such as Triage Viewer to view known IOCs, Enterprise Security Search to rapidly conduct wide ranging searches and contain threats or suspicious activities, then using Data Acquisition for in-depth endpoint inspection and analysis of current and past endpoint activities.

Analyst notes:
The revenue rank is an estimate that may be somewhat high at this time. However, due to FireEye’s overall presence in the market it is easily foreseeable that their revenue growth curve for the 2016 year with steepen. This increase would have to be very significant to change their market share in 2016.
**Hexis Cyber Solutions**

Description: **Hexis Cyber Solutions’** Hawkeye G is a multifaceted solution for endpoint protection. Hawkeye G endpoint agents use behavior-based detection (heuristics) and perform real-time alerting of endpoint activity. Endpoint capabilities are complemented by a network sensor that detects outbound communications from infected endpoints. HawkEye G incorporates additional detection indicators including threat intelligence feeds, a community-based malware verification service, and signatures. Currently, HawkEye G also ingests third-party threat indicators from FireEye and Palo Alto Networks. HawkEye G detection indicators are sent to the HawkEye G Manager appliance where threat analytics are applied via ThreatSync™ capability. ThreatSync fuses together multiple indicators into a dynamic, real-time threat score used as the basis for policy-based threat responses that can be deployed in automated or automatic mode (in which the user clicks to initiate response).

In every deployment in which HawkEye G is installed, the system detects currently-infected machines and, in automated mode, infections can be remediated automatically or with a few mouse clicks. Post-event, HawkEye G updates its knowledge baseline with the learned behaviors to improve future protection.

Hexis Cyber is a wholly owned subsidiary of The KEYW Holding Corporation.

**Analyst Notes:**

Though it offers manual intervention for remediation, Hexis Cyber has the most advanced automated and automatic remediation mechanism built into its solution discovered during the course of this research. The difference between “automated” and “automatic” is the level of human interaction in the resolution. Automated indicates that the system diagnoses the remediation needs and then contacts an analyst to walk through the steps. In an automatic remediation, the analysts trust the systems to engage and remediate the problem then notify them of the outcome. This separation is policy driven, so operators can pick and choose the path they are most comfortable with.

Remediation can be accomplished directly by the system or through integrations/partnerships with other protection mechanisms including Palo Alto NGFW and WildFire, and FireEye NX.
**IBM Apex**

Description:  
**IBM Security Trusteer Apex (Apex)**  Advanced Malware Protection prevents unknown/zero-day threats and advanced malware. Trusteer Apex combines a multi-layered defense with dynamic intelligence, strengthening the overall defense and optimizing the ability to prevent successful endpoint compromise.

Apex protects endpoints throughout the threat lifecycle by applying an integrated, multilayered defense that breaks the attack chain and preempts infection. It does this through:

- **Credential protection** from cyber attackers who use phishing schemes or breached third-party databases to manipulate users.
- **Exploit chain disruption** to help prevent stealthy infection of user applications.
- **Advanced malware detection and prevention** to prevent mass-distributed malware infections and detect legacy threats.
- **Lockdown for Java** to enable the safe use of Java applications while preventing untrusted Java applications from executing high-risk actions.
- **Malicious communication blocking** that prevents untrusted files from executing operations and establishing connection channels between malware and the attacker.

Apex also uses application fingerprinting to control process execution for known good processes; it also allows processes that are unknown, but not performing “risky” or “sensitive” execution. This decision is made by Trusteer Apex at runtime and does not require any external intervention or support.

**Category:** Prevention, Detection, and Response for Windows systems.

**Started:** 2010/2013 – Apex was originally developed by Trusteer in 2010. Trusteer was acquired by IBM in 2013

**Funding:** IBM is a public company

**Rank by largest single deployment:** 7

Though IBM did not disclose this information, given Trusteer’s and IBM’s relationships with large financial institutions and other factors from investigation, EMA has estimated that the largest deployment of Apex is in the 100,000 and above range.

**Market share by licenses sold:** 2.3%

**Rank by licenses sold:** 7

**Market share by revenue:** 2.4%

**Rank by revenue:** 7

**2015 revenue growth:** IBM does not release this level of breakout. However, IBM security has seen double digit growth in the last year. Given that data, the attention organizations are paying to endpoint protection, and other factors, EMA estimates APEX growth to have been in the 20%–40% range.
Invincea

Description:
Invincea is a premier provider of advanced malware threat detection, breach prevention, and forensic threat intelligence. It is one of only two major players in the next-generation endpoint space that approaches prevention through system virtualization. Moreover, it has expanded from its historical foundation of virtual container technology into a broader detection and prevention platform.

Invincea uses both container-based protection to stop spear-phishing and machine learning based anti-malware detection to defend against both known and unknown malware. Both internal and external to the container, its machine learning engine performs static code analysis of files to provide rapid detection of threats that evade signature-based antivirus and other controls. Behavioral monitoring within the container also detects and terminates file-less intrusions that use trusted programs to conduct attacks. Invincea allows security administrators to specify which end user applications run within the secure virtual container and which are trusted outside the container. Administrators can also configure whether or not malicious processes within the container are automatically and immediately terminated.

Invincea protects against zero-day attacks including malware-based advanced persistent threats (APT) and advanced targeted attacks (ATA). Within the Invincea console, security administrators can specify the use cases for container-based protection. Post identification of a threat, Invincea provides detailed forensic intelligence about the attack to aid in defense and identification of future similar attacks.

Invincea leverages endpoint sensing, behavioral monitoring/blocking, and cloud-based analytics to protect against a diverse set of malware and file-less intrusions regardless of the delivery method to the endpoint.
LightCyber

Description:
LightCyber Magna Platform, is one of only three solutions that is agentless in design.

LightCyber Magna is a Behavioral Attack Detection platform that provides accurate and efficient security visibility into advanced or targeted attacks, insider threats, and malware that have circumvented traditional security controls. Magna delivers alerts that include automated investigative data with rich user, endpoint, and network context enabling swift triage and resolution. The result is an ability to detect and stop attacks early, without generating hundreds or thousands of alerts for analysts to wade through.

Magna identifies compromised users and entities across the entire attack lifecycle and is the only solution in the research that natively (without partner or separate product integrations) incorporates both network (DPI) and endpoint (agentless) context. Magna does not rely on technical artifacts that produce excessive false positives. Instead, it detects anomalous attacker behaviors that cannot be concealed. The result is highly actionable alerts that include automatically generated investigative data to focus incident response and stop attackers before real damage is done.

Category: Detection and Response.
LightCyber device profiling is active for all IP connected devices. Endpoint interrogation is only currently available for Windows systems.

Started: 2013

Funding: $16.5M in seed and equity funding from 2011 to 2015

Rank by largest single deployment: 12

Market share by licenses sold: <1%

Rank by licenses sold: 9

Market share by revenue: <1%

Rank by revenue: 9

2015 revenue growth: 40%–60%
**Malwarebytes**

**Description:**
Malwarebytes has been a staple in the antimalware business for years. When traditional antivirus fails to detect an infection, IT professionals worldwide download Malwarebytes’ free version to see how it can help. Based upon that legacy, Malwarebytes Endpoint Security enterprise solution has a two-pronged approach with anti-malware and anti-exploit solutions merged into one through a central management console.

Malwarebytes Endpoint Security offers a four-layer defense approach in the Anti-Exploit component of the solution. Layer 0 is application hardening, which generically hardens applications to be less susceptible to vulnerability exploit attacks. Layer 1 is OS bypass isolation, which protects the systems from exploits rendered against the host OS. Layer 2 memory call protection. Layer 3 is application behavior protection, which understands how programs are supposed to operate; if they begin to vary from the norm, the application operation can be stopped. With this combination, anti-exploit protects all major browsers and browser components including Java and Flash, defends the endpoint against drive-by download attacks, shields other vulnerable applications including MS Office, PDF readers, and media players, and ultimately blocks unknown and known exploits from executing.

Malwarebytes’ anti-malware engine provides on-endpoint, anti-malware scanning and malicious website blocking to protect endpoints against zero-day malware. It reports vulnerable endpoints to the management console (or log management tool of the customer’s choice) and allows customizable prevention policies. The anti-malware engine is based on the company’s heuristic and behavioral rules engine.

**Analyst Notes:**
Malwarebytes’ revenue included for the report is only for its enterprise product. The company’s consumer base licensing is over 30M active monthly users and is also still based on its traditional signature and pattern matching engine.
Outlier

Description:
Outlier is one of only three solutions identified that is agentless. Due to its agentless implementation architecture, deploying the solution requires far less effort than agent-based solutions because there is nothing to install and no need for change control windows or agent conflict testing. Lifecycle is much simpler as well, as there are no agents to repair or update. Therefore, Outlier has zero impact on end user computers.

Outlier automatically examines on-network endpoints without relying on signatures. The analysis system collects digital forensics evidence (artifacts) from computers and performs multi-dimensional security analysis to identify attacker activity, rogue user behaviors, malware, and advanced persistent threats. Outlier can assess the attack surface of exploitable vulnerabilities across the enterprise as a whole, providing immediate visibility of endpoints to measure the scope and severity of a company’s enterprise threat profile.

With centralized cloud-based threat intelligence, once the automated analytics system has seen and analyzed an artifact from one customer, it does not need to analyze it again when it is seen in another customer’s network. Outlier in-house analysts see the results of all SaaS customers and work to continually improve the underlying detection mechanisms for the benefit all customers.

By examining the entire enterprise endpoint data set with various data modeling techniques, the system finds anomalies and outliers that end up as being malicious actors or artifacts. When anomalies are found on an endpoint, Outlier reports findings and solutions back to its in-house analysts to provide automated response. A human analyst initiates remediation with a mouse click to automatically remove malicious artifacts and associated registry keys.

Category: Detection, and Response for Windows, Linux and MAC systems
Started: 2014
Funding: No public funding records available
Rank by largest single deployment: 10
Market share by licenses sold: <1%
Rank by licenses sold: 9
Market share by revenue: <1%
Rank by revenue: 9
2015 revenue growth: >250%
**Promisec**

**Description:**
*Promisec Endpoint Manager Platform (PEM)* is one of only three agentless solutions identified in the marketplace. PEM inspects every aspect of endpoints—not just installed applications, patches and running programs. The solution provides a detailed contextual inventory of the systems that is used to detect threats early in the exploitation cycle before they can cause significant problems for the monitored organization.

Once data is gathered, PEM databases each item for comparison with the past inventory and for use in future evaluation. It analyzes the systems and then, by incorporating the organization’s own security policies, PEM can immediately indicate which systems are no longer in compliance with those policies and can clean or quarantine systems either as a manual or automated operation. PEM can also direct execution of any Windows OS-built application on the endpoint from a central command center to aid in remediation. PEM can view all files in a system via explorer view; open a command prompt on the system; remove/kill a process/application; push out a patch/installer; capture memory contents; and see all network traffic and open connections on the endpoint.

PEM can leverage best practice standards such as NIST, CIS Benchmarks, DISA STIGs and Active Directory group policies to gauge overall endpoint risk. Additionally, files and processes that are compromised or are malware are quickly identified with the industry’s first agentless File Integrity Monitoring and Reputation technology. Polling can be determined by the administrator, attaining five-minute detection of active threats, which meets virtually all standards for real-time response. Because it captures all of the data at the host, investigators can review endpoint datasets from as far back as the customer wishes to store them.

PEM has significant strength in its integrations and controls for other tools. Though it does not directly prevent compromise of systems, through its partner integrations it provides proactive protection.

PEM offers completely customizable settings to detect virtually every security agent on the market (AV, Patch, Config management, encryption, etc.). It also offers a tailorable blacklist of over 5000 applications and whitelisting of application, services, processes, startup apps, browser objects, and toolbar shell apps. The application whitelisting capabilities allow for controlling any combination of application installs, services, processes, files, registry settings, startup items, browser objects, etc. Whitelist enforcement can be manual or automatic. PEM also offer out of the box service with VirusTotal and can integrate with many IOC threat intelligence services via its hash match capabilities.

**Category:** Protection, Detection, and Response for Windows, Linux, and MAC systems

**Started:** 2014

**Funding:** Undisclosed – Promisec has received two round of funding, one equity and one venture between 2006 and 2011.

**Rank by largest single deployment:** 7

**Market share by licenses sold:** 3.5%

**Rank by licenses sold:** 6

**Market share by revenue:** <1%

**Rank by revenue:** 9

**2015 revenue growth:** Given the newness of the company, there is not enough information available to make an estimate.
**RSA ECAT**

Description:

RSA ECAT (ECAT) RSA ECAT is a continuous endpoint threat detection and response solution. ECAT’s agent operates in both the kernel space (below the operating system) and in the user space (above the operating system), providing contextual visibility, seeing beyond a single alert to provide incident responders and security analysts a full attack platform to detect and respond in real-time against advanced attacks. ECAT uses signature-less, next generation behavioral analytics to detect even the most stealthy malware and advanced persistent threats (APT).

ECAT can operate as a completely autonomous behavioral analytics solution using machine learning-based analytics to detect security related anomalies. This means ECAT can protect the endpoint in the absence of a feed or static indicator of compromise (IOC). Though it can use intelligence feeds such as RSA Live, as well as those provided by third parties leveraging STIX, to provide more context, it is not reliant upon an external connection/engine to identify, monitor, analyze or respond to observed issues and behaviors.

To improve accuracy ECAT analyzes behaviors in two ways. First, ECAT identifies anomalies at the system or user level. Secondly, it compares findings in one system with all monitored systems in the to direct remediation across all affected systems in the organization. Risk ratings can be further augmented by whistling and blacklisting features that are ingested into ECAT.

ECAT uses both static and dynamic models for determining risk. In the static model a bad action triggers an event. Each variance from the norm adds points to the total risk score. Known attack vectors or indicators have predetermined risk weighting, so they modify the risk score non-uniformly. In the dynamic model the machine learning algorithms tune the weight of an action or threat based on the accumulated real-world data and activities; this hones the weighting factors to the environment making more customized predictors that enable a security analyst to focus first on higher risk incidents.

ECAT is integrated with other RSA products such as RSA Security Analytics (SA), creating a holistic security monitoring solution with visibility at both the network and endpoint levels. Security Analytics uses the data and metadata created by ECAT to enrich its detection, incident forensics and hunting capabilities. Using SA alone, if ECAT is not deployed on a suspicious endpoint, the analyst on SA can create an action to deploy ECAT on the host and trigger an investigation from that point forward.

**Category:** Prevention, Detection and Response for Windows and MAC Systems

**Started:** 1982/1999/2012 – Founded in 1982, RSA is a long time cybersecurity player. Silicium Security, the creator of ECAT endpoint security technology, was founded in 1999. RSA acquired Silicium and ECAT in 2012 and have been developing the technology since then in close conjunction with RSA Security Analytics. Storage giant EMC is RSA’s parent company, having acquired RSA in 2006.

**Funding:** RSA is a wholly owned subsidiary of publicly traded company EMC

**Rank by largest single deployment:** 7

**Market share by licenses sold:** 3.5%

**Rank by licenses sold:** 6

**Market share by revenue:** <1%

**Rank by revenue:** 9

**2015 revenue growth:** RSA has made a significant internal investment to move ECAT forward post the acquisition of Silicium. RSA has also increased marketing for ECAT in the last year. Given these facts and other research, EMA estimates ECAT revenue growth for 2015 to be in the 20%–40% range.
SentinelOne

Description:
The SentinelOne endpoint protection platform (EPP) was founded by a group of Israeli cybersecurity experts who took a fundamentally different approach to endpoint protection. SentinelOne unifies endpoint threat prevention, detection and response in a single platform that is driven not by traditional signature- and pattern-based methods, but by sophisticated machine learning and intelligent automation. With SentinelOne, organizations can predict malicious behavior across multiple vectors, rapidly eliminate threats with fully-automated, integrated response capabilities, and adapt their defenses against the most advanced cyber-attacks.

SentinelOne EPP deploys a lightweight autonomous agent that monitors all activity in both kernel and user space (including files, processes, memory, registry, network, etc.). The Agent is virtually silent and has little-to-no system performance degradation. With its dynamic execution inspection, SentinelOne EPP detects advanced threats, including zero-day attacks to help enterprises augment existing protection of endpoints. It provides automated mitigation, that reverses malware-driven modifications by restoring manipulated files to their last known trusted states and generates real-time forensics.

EPP provides autonomous, silent monitoring of all endpoint activity in real-time; it delivers forensic quality endpoint analysis and investigative capabilities that generate intuitive reports during attacks. It also offers “zero-touch” fully automated remediation protocol that covers all endpoints-- local and remote—allowing for decisive incident response virtually eliminating dwell time.

EPP’s unique attack storyline visualization shows a 360-degree view of an attack, mapping out its point of origin and progression across endpoints and other systems for complete forensic insight. Its robust containment capability immediately stops its lateral spread cold by disconnecting the infected endpoint device from the network, but still maintains the Agent’s connection to the SentinelOne management console.

EPP is the only next generation endpoint security/EDR/ETDR/STAP/Endpoint Threat Detection solution on the market to have gained antivirus replacement certification for its solution. The AV-TEST Institute has certified the SentinelOne EPP as a replacement for antivirus on MAC OS X and Windows.
**Sophos**

Description: *Sophos* has been a major force in the endpoint protection market for many years. Seeing the need for advanced endpoint threat detection and remediation solutions, it has both created a new cloud-based endpoint security solution called Malicious Traffic Detection (MTD) and acquired other advanced endpoint exploit detection technology to maintain its place in the market. Sophos is one of two traditional antivirus vendors that participated in the research.

Malicious Traffic Detection is a cloud-based analysis engine that detects outbound traffic attempting to communicate with known command and control servers using advanced Sophos network technology. MTD monitors outbound traffic across all secure endpoints and blocks advanced threats that may or may not have a payload. Many newer advanced threats tend to be memory based and file-less, or even infect and impersonate legitimate applications, which can evade some traditional security, but MTD can block these zero-day threat attempts. As threats are not limited to malware, MTD will also see threats that are driven by un-authorized applications like a penetration tool, powershell, password cracker, etc.

Sophos’ endpoint technology is integrated with its perimeter protection XG Firewall via a threat sharing technology called “Synchronized Security” that provides faster response to identified threats. Synchronized security provides continuous, real-time information about suspicious behavior or malicious activity between endpoints and the network firewall or UTM. By giving these traditionally independent products the ability to directly share intelligence, Synchronized Security can instantly trigger a response to stop or help control a malware outbreak or data breach. The Sophos XG Firewall uses data provided by Sophos endpoint protection to isolate and restrict access to and from the affected device, and in parallel, the endpoint protection can remediate the attack.

With a growing set of next-generation technologies such as behavior-based analytics and malicious traffic detection, the SurfRight acquisition increases Sophos’ ability to prevent, detect and remediate zero-day and sophisticated attacks by interrupting malware and advanced persistent threat (APT) vectors. This acquisition will further strengthen Sophos’ endpoint protection technology portfolio by adding complementary new defense tactics, delivered either on-premises or in the cloud.
Tanium

Description:
Tanium is something of an oddity in the endpoint security world in that spans both operations and security use cases. Developed as a platform to provide high scalability and fast response to queries within an organization’s endpoint environment, Tanium has recently added modules that provide specific solutions for endpoint security and management use cases such as forensic investigation. With the Tanium architecture, endpoints are directed by the administration console but communicate with each other to make inquiries, collect information, and return results to the administration console.

Tanium’s core tenants are Ask, Know, and Act.

- **Ask** – Using a Google-like natural language query interface, endpoint administrators request information about the systems. Acting as a collective, systems on the network relay the query throughout the environment using a peer-to-peer communications style.

- **Know** – Systems respond to the management station with their information. Because communications happen in parallel in hyper-speed, data for queries is returned in 15 seconds or less, regardless of the number of endpoints. However, network delay can affect round-time response times to remote sites.

- **Act** – Administrators can act upon provided data to update any aspect of the endpoints’ configuration including stopping processes, uninstalling applications, deploying patches or even shutting down systems. Changes are pushed out in the same manner - queries are passed so updates are also done in seconds to minutes.

In the security context Tanium addresses threat detection via adhoc queries and IOC scans, investigation via historical and real-time queries on endpoint activity, compliance and configuration management, vulnerability assessment and incident response, and remediation via the act functionality including patch management.

Analyst Notes
Tanium is present in this report because it has the potential to be a significant player in the endpoint security market. However, the company’s main issue for full participation in endpoint security is its lack of proactive identification, alerting and notification capabilities. All of the other next-generation endpoint solutions proactively identify and alert on incidents they detect. For all of its strengths, Tanium’s weakness is that it is currently reactive in nature. If Tanium develops a policy-based alerting capability that brings it into the proactive realm, the company will significantly change the endpoint security landscape.
Triumfant

Description:
Triumfant’s AtomicEye solution can be deployed in physical or virtual environments and works on a five stage model: Capture, Create models, Detect Anomalies, Classify Anomalies, and Synthesize Responses. The small-footprint agent captures data concerning activities and changes on the endpoint. Using its patented technology, AtomicEye creates behavioral models of those activities and changes; the models are maintained and updated by the system over time. The models are stored in an embedded MySQL database. Active Directory can be used to associate systems together as a community for analysis both individually and by related community, further increasing accuracy of the analysis.

The database on each system is polled by the management station (aggregator), at an administrator-defined interval or based on changes in risk in the system to compare device object states captured by the agent with policies administered by the aggregator. Process behaviors are monitored continually by the agent and compared to the existing local process models to discover anomalous process behaviors.

Anomalies are classified by proprietary “Recognition filters” that assign risk levels, determine responses and generate incidents. If an anomaly identified at the agent or the aggregator breaks policy and/or is considered highly risky, the event will trigger an automated investigation of the endpoint.

If a response is determined as necessary, a surgical response is synthesized by the Triumfant server based on the detected changes and passed to the agent for execution. Remediations can be executed by the system either pre- or post-human authorization. Triumfant’s unique Donor Technology repairs tainted or corrupted files on one computer with cloned good files from another computer. If at any point a remediation is deemed to negatively affect the environment, AtomicEye can undo the remediation.

Triumfant can also aid in prevention by alerting and/or remediating on missing patches, out of compliant security settings, inactive or missing protective software, and detection of unauthorized applications.

The central management console, Triumfant Server, is designed for SOC analysts to quickly see the scope of issues, prioritize activities, and initiate response. It is also the reporting and administration gateway for all managed devices.

Category: Detection and Response for Windows, Linux, and MAC systems

Started: 2003/2006/2010 – Triumfant was originally founded in 2003 as a help desk management tool, but after making several discoveries and filing for patents on them, in 2006 the company decided to re-architect its solution and focus on endpoint security. After several years and numerous augmentations, the current design was released in 2010.

Funding: $29M in equity financing between 2006 and 2015

Rank by largest single deployment: 9
Market share by licenses sold: <1%

Rank by licenses sold: 9
Market share by revenue: <1%

Rank by revenue: 9
2015 revenue growth: 95%–115%
**Ziften**

**Description:**
Ziften provides continuous endpoint visibility for exceptional insight into the endpoint and its interaction with the network, enabling organizations to efficiently prevent security exposures and detect and respond to advanced threats that are attacking endpoints. Ziften's features include:

- **Collaboration** – Ziften uses blacklists to stop known bad or undesirable applications. It can also kill processes and modify affected registry keys. Through its integration partnerships, the product enhances security discovery and analysis of existing workflows to reduce time to resolve incidents and uses key performance indicators (KPIs) that quantify the attack surface of each endpoint, and as an aggregate risk surface across all endpoints. Ziften enriches data in major SIEM vendors like Splunk, QRadar, and ArcSight using CEF formatted alerting.

- **Fast Deployment** – Ziften deploys in most environments in minutes to hours using standard software distribution tools such as Microsoft SCCM, Altiris, Casper, etc.

- **Scalable** – Ziften can manage 100,000+ endpoints with a physical or virtual infrastructure.

- **On-Premises or Hosted** – Ziften offers a hosted option for deployment, further reducing the need for internal management infrastructure.

- **Lightweight** – Ziften’s agent consumes less than 1% of system resources

- **Extensible** – Through a vast array of partnerships, Ziften consumes third-party data sources (notably Blue Coat, ReversingLabs, AlienVault, and iSIGHT Partners) to improve context and invoke additional Ziften functionality as customer needs change.

Ziften’s value increases for customers who leverage its ZFlow technology, which combines the abilities of an endpoint agent with the insight of a NetFlow capture tool. This powerful capability provides comprehensive intelligence of activities on the endpoint with the associated network telemetry so analysts can forensically observe compromised endpoints to gain insight of the attackers’ methods, tools, and tactics. This functionality provides several benefits. First, where either no network telemetry is captured external to the host or where it is only captured at the core or WAN and Internet layers, ZFlow closes the security blind spots by providing visibility into the LAN-to-LAN, local broadcast, and intra data center application communications, also called “East-West” traffic. Second, ZFlow improves context and thus reduces false positive alerts. ZFlow accomplishes this in a highly reliable and repeatable manner because of its ability to correlate system processes with the network activity they generate, which NetFlow is incapable of doing. To do this, ZFlow provides traditional OSI layer 3-4 data such as source and destination IP addresses and ports, but also provides additional valuable Layer 4-7 information.
About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMAs clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook or LinkedIn.

This report in whole or in part may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Enterprise Management Associates, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice. Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. “EMA” and “Enterprise Management Associates” are trademarks of Enterprise Management Associates, Inc. in the United States and other countries.

©2016 Enterprise Management Associates, Inc. All Rights Reserved. EMA™, ENTERPRISE MANAGEMENT ASSOCIATES®, and the mobius symbol are registered trademarks or common-law trademarks of Enterprise Management Associates, Inc.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com