Carbon Black.

Security & Privacy Guide

May 2018

Carbon Black, Inc.
1100 Winter St,, Waltham, MA 02451 USA
Tel: 617.393.7400 Fax: 617.393.7499
E-mail: support@carbonblack.com
Web: http://www.carbonblack.com

Table of Contents

Welcome 4

Service Overview 6

Secure Data 6

Physical Security 6

Cb Response Cloud and Cb Defense 6

Predictive Security Cloud 7

Political & Legal 7

Logical 7

Access controls 7

Encryption 8

Data segmentation & destruction 8

Cb Response Cloud 8

Cb Defense 8

Secure Operations 8

Audit Logging & Retention 8

Security Monitoring 8

Threat Hunting 9

Third Party Penetration Tests 9

Secure Network, Operating System Configurations and Patch Management 9

Vulnerability Scans 9

Backups and availability 10

Cb Defense and Predictive Security Cloud 10

Cb Response Cloud 10

Denial of Service 12

Secure Development 12

Secure Organization Policies and Procedures 12

Responsibility 13

Personnel Security 13

Background checks 13

Confidentiality Agreements 13

Acceptable Use and Employee Code of Conduct 14

Security Policies 14

Security Training 14

Data Classification, Data Handling and Data Retention Policies 14

Incident Response Plans and Exercises 14

Business Continuity Management 15
Service Continuity 15
Risk Assessment 15
Privacy & Compliance 15
Privacy 15
Privacy in the European Union 16
Regulatory Compliance 16
Carbon Black’s compliance requirements 16
Your compliance requirements and Carbon Black 17

Welcome

This guide is an overview of the people, process and technology Carbon Black uses to develop, test, and deploy our products.

When evaluating the security of a cloud solution, it is important to distinguish between:

- **"security of the cloud"** - security measures the cloud service provider implements and operates
- **"security in the cloud"** - security measures the cloud user implements and operates, related to the security of applications using AWS services

Cb uses Amazon Web Services™ (AWS) as our primary Cloud Service provider. AWS shares responsibility with Carbon Black for the security of cloud operations. AWS provides "security of the cloud" while Carbon Black provides "security in the cloud." AWS publishes substantial documentation on their security best practices.

This guide describes Carbon Black's security procedures in five areas:

- how we protect your data
- our operational security procedures
- our secure development practices
- our organizational security program and policies
- privacy and compliance considerations with Carbon Black

Security does not end with Carbon Black. Your team also shares responsibility for security. AWS is responsible for the security of their infrastructure, Carbon Black is responsible for the security of the Carbon Black® application, and you are responsible for the security of your accounts. Your team should choose strong passwords, enable two-factor authentication for all users and carefully protect email accounts used to reset forgotten passwords.

Carbon Black's Cloud Services are covered by a SSAE-16 SOC2 Type 1 report ("SOC 2"). SOC 2 reports are developed and governed by the American Institute of Certified Public Accountants. The reports are similar in structure to financial audit reports, except they focus on technical controls instead of financial controls. It is an industry standard used to validate the security controls in place to manage the confidentiality, integrity and availability of cloud infrastructure and customer data. Our services have an AICPA SSAE-16 SOC 2 Type 1 Report, as described by Attestation Standards Section 801. This report is available upon request.

If you have questions not covered in this guide, contact your Carbon Black representative or email us at support@carbonblack.com. Due to the evolving nature of threats and business needs, Carbon Black reserves the right to modify our practices.

Service Overview

The security controls, processes and procedures in this guide apply to all Carbon Black products and services delivered via the cloud (referred to as “Cloud Services”) :

Secure Data

In the world of the cloud, “data security” has different definitions to different people. This section covers data security from four perspectives:

- **Physical** - where your data is physically located
- **Political** - the political environment where your data and data-controlling entities reside
- **Legal** - the legal entities that control or process your data
- **Logical** - which people and which networks have access to your data

Carbon Black’s Cloud Services are hosted in the following locations:

- **Cb Defense**: Northern Virginia (Amazon’s US-East region) or Frankfurt, Germany (Amazon’s EU-Central region)
- **ThreatSight:** Northern Virginia (Amazon’s US-East region)
- **Cb Response Cloud**: Northern Virginia (Amazon’s US-East region) or Frankfurt, Germany (Amazon’s EU-Central region), Singapore, (Amazon’s Asia Pacific region)
- **Predictive Security Cloud**: Boston, MA (a private datacenter) or Northern Virginia (Amazon’s US-East region)

Cb Defense and Cb Response Cloud allow you to choose the AWS region hosting your service at the time of provisioning.

Physical Security

Cb Response Cloud and Cb Defense

AWS datacenters are staffed 24x7 by trained security guards. Datacenter access is authorized strictly on a least privilege basis. AWS customers are not authorized physical access to any AWS datacenter. Physical controls in AWS datacenters are validated by auditors as part of AWS’s SSAE-16 SOC 2 Type II report. Independent reviews of those physical controls is also included in AWS’s ISO 27001 audit, the PCI assessment, ITAR audit and FedRAMP testing programs. See the AWS Risk and Compliance Whitepaper for information regarding AWS’s physical security.

Predictive Security Cloud

The Predictive Security Cloud™ product (PSC) provides threat intelligence services to Cb Response™, Cb Response Cloud™, Cb Defense™ and Cb Protection™ products. Data transmitted to or processed by the PSC is anonymized and aggregated unless explicitly opted-in via in-product configuration controls.

Resources in the Boston datacenter are physically isolated in a dedicated cage and restricted to authorized personnel. Physical controls include 24x7 staffing by trained security guards, surveillance cameras, biometric access controls and strict facility visitor access management procedures.

The datacenter has environmental controls including climate control, redundant A/B condition power supplies to each cage, multiple emergency generated and gas fire suppression systems.

These controls are annually reviewed and validated by the hosting facility's SSAE-16 SOC2 Type II report. Copies of the SSAE-16 SOC2 Type II report for this datacenter are available upon request.

Political & Legal

Cb Cloud Services are hosted in either the United States or Germany. Cb Defense and Cb Response Cloud allow you to choose the country hosting your service at the time of service provisioning.

Neither Amazon nor Carbon Black will disclose your data unless required by law, regardless the source or type of political pressure applied. Both Amazon and Carbon Black policy is to notify customers before disclosing their data, unless we are legally prevented from doing so.

See Amazon Web Services Data Privacy FAQ for more information on Amazon's data privacy policies.

Logical

Each Cloud Service is an independent security and administrative domain. Administrator access to one Cloud Service does not mean access to another. Similarly, if one Cloud Service is compromised, it does not enable lateral movement into another Cloud Service. Additionally, each Cloud Service is further segmented, based on the service requirements and the principle of least privilege.

Access controls

Access to data requires access to the systems on which it is processed. Access is permitted via the operating system of the machine processing the data or the Carbon Black application.

Only Cb Product Operations or Cb Security Operations personnel have access to the systems.   All access is via remote desktop or secure shell, authenticated per-user and requires a username, password, SSH public/private keys, and a two factor authentication token. Role based access controls, audit logging and the policy of least privilege are used to provide logical segmentation and tracking of user behavior on assets in which each user is permitted. Network access to systems is restricted via comprehensive network controls.

Encryption

Your data is encrypted in transit with TLS. Carbon Black closely monitors industry best practices for TLS configurations and ensures our products enforce appropriate protocols and ciphers. Any data transmission via unsecured transports is not supported and strictly prohibited.

Reference individual product “Data Collection Guide documents” for specifics.

Data segmentation & destruction

Your data is segmented from data of other Carbon Black clients.

Cb Response Cloud

When your Cb Response Cloud license ends, any remaining sensors are issued an uninstall command, all daily backups are deleted, a final backup is taken and your server is powered off.   Any server that remains powered off for 14 days is destroyed.   Final backups are destroyed after 60 days.   The destruction delay is a safeguard against miscommunication and coordination.

Cb Defense

When your Cb Defense license ends, your logins are disabled, your devices are deregistered and information is no longer collected from your devices. Information previously collected is purged within 60 days after termination of business relationship. The destruction delay is a safeguard against miscommunication and coordination.

Secure Operations

Audit Logging & Retention

Role based access controls, audit logging and the policy of least privilege are used to provide logical segmentation and tracking of user behavior on assets in which each user is authorized. These logs are transmitted in real-time to a central logging system and retained for 12 months.

Security Monitoring

Carbon Black staffs a 24x7x365 Cloud Network Operations Center with analysts to investigate any unusual activity. These analysts receive security alerts and respond as needed.   Any abnormal activity is escalated to Tier II responders for deeper investigation and response.

Threat Hunting

Activity from all Carbon Black Cloud Services is centrally logged. Scripts, pattern analysis and threat intelligence sources are applied to the data to highlight suspicious activity and a team of Security Analysts actively review activity across all environments for suspicious activity.

Third Party Penetration Tests

All Carbon Black Cloud Services undergo regular network penetration tests and intrusion exercises by an third party security firm. The network penetration tests validate our configuration management procedures, while the intrusion exercises validate our detection and response procedures. To maintain the security and stability of our service, we do not allow clients to perform their own penetration tests against any Carbon Black Cloud Service.

Secure Network, Operating System Configurations and Patch Management

Since each Cloud Service is an independent security and administrative domain, the network configurations are tightly segmented. Public services are limited to tcp/80 and tcp/443 (HTTP and HTTPS) and HTTP simply redirects to HTTPS. Management access for administration is limited to the small number of Cloud Operations staff directly responsible for managing the service's infrastructure.

Operating system configurations are similarly tightly controlled and hardened. In addition to the security risks of unnecessary services, they also consume resources and present a stability risk to the availability and performance of systems running on cloud systems. Since we're fanatics about efficiency and availability, we carefully limit operating system services to those critical to the function of the operating system and our application.

Each Cloud Service team follows patch management procedures to ensure software packages are at current patch levels with all required security patches applied. Patches are applied regularly as part of the routine operations and updates to the systems; exception procedures are in place for critical patches requiring immediate application to maintain optimal security.

Vulnerability Scans

All Carbon Black Cloud Services use a variety of vulnerability scanning/management platforms to monitor systems for unexpected configuration changes and vulnerable software packages. These platforms run at least monthly. Many are in constant use and proactively deliver alerts to the Cloud Network Operations Center in near real time. Like penetration tests, we do not allow clients to perform their own vulnerability scans against any Carbon Black Cloud Service.

Backups and availability

Data backups and disaster recovery preparations are in place to adhere to each service's defined recovery point objective (RPO) and recovery time objective (RTO). Each Cloud Service maintains procedures required for the specific technology used.

Cb Defense and Predictive Security Cloud

Cb Defense and Predictive Security Cloud systems are architected for highly available service: all services use resources in at least two datacenters within your chosen region. Data is replicated in real time between datacenters, with seamless failover between services datacenters. Loss of a system or disk will not result in service interruption or data loss. Loss of an entire datacenter will not result in service interruption or data loss.

Cb Defense and Predictive Security Cloud both test failover and restore procedures as a part of day to day operations. For example, Cb Defense services are highly available and are designed to distribute load between two datacenters in the same region. Upgrade procedures failover service as part of each upgrade, the same as if there were complete loss of a datacenter.

In the unlikely event the service is completely unavailable, Cb Defense sensors cache recorded data until the server is available. Service downtime does not result in data loss unless the volume of data exceeds local cache configuration.

Cb Response Cloud

Cb Response Cloud is hosted on a virtual machine and data stored on a network SAN in an AWS datacenter in your chosen region. AWS datacenters are highly-available in their design: network, power and other critical resources are redundant to mitigate the risk of datacenter wide outages.

In the event of a hardware failure in the physical computer hosting your virtual machine, your virtual machine will be migrated to a new machine with no data loss and minimal downtime.

Data volumes are snapshotted hourly and retained for 24 hours. In the event of data corruption or lost data, your data will be restored to the most recent valid backup. Backup restoration procedures are tested at least semi-annually.

Your virtual machine images and data backups are replicated to a second AWS datacenter within the same region. In the event of a complete datacenter-wide outage, your service can be restored to the alternate datacenter from the most recent backup with minimal data loss.

Local and off-site backups are encrypted at rest with the same encryption key used on your live volumes using AES-256. Encryption keys are unique per customer.

If the server is unavailable, sensors cache recorded data until the server is available.   The size of the local cache is configurable, the default is 2GB - enough for about 30 days of storage on a typical system. Server downtime does not result in data loss unless the volume of data exceeds local cache configuration.

Change Control

Carbon Black's Product Operations Teams follow "Infrastructure as Code" development principles.

When infrastructure is code, it is checked into a source code repository. Proposed changes are tracked on a per commit basis, and each commit includes a brief message with context, including a link to a ticket. Each change goes through a manual code review process, including automated testing and other checks used as a conditional acceptance prior to review by other members of the team.

These procedures mirror those of the traditional software development processes, allowing consistent procedures and practices between application development and infrastructure management within the team. These practices are a core tenant of "DevOps."

Carbon Black's Product Operations Teams follow the same Product Security Program, including the Secure Development Lifecycle, used to develop our applications. (More information on the Carbon Black Product Security Program is available in the Secure Development section below) As a result, all changes to production infrastructure:

- Are saved as a clearly-defined changeset in a source code repository with metadata including: who made the change, when, why and a reference to a ticket used to coordinate the change.
- Each proposed change undergoes automated acceptance testing, including QA tests and security-specific tests, static and dynamic code analysis
- All proposed changes that pass acceptance testing must pass code review by at least one other engineer with sufficient knowledge of the system
- Any security-sensitive changes must pass code review by the team's designated security engineer
- Both regular and security engineers have escalation procedures to senior members of the architecture and security teams to escalate change reviews as needed

These change control procedures are backed up by vulnerability scanners and configuration monitors that alert on unexpected or unsafe changes to critical configurations. If an unsafe change passes each of these controls and still makes it to production, it triggers a root cause analysis of the control efficacy.   The review team makes recommendations for control updates to mitigate the risk of that change happening again such as training, education, new automated tests or architectural update.

Denial of Service

Every Denial of Service (DoS) attack is unique and the solution will be tailored to the attack.

AWS uses proprietary techniques to mitigate the risk and reduce the impact of many off-the-shelf Distributed Denial of Service (DDoS) attacks. In the event of an attack, Carbon Black staff will actively work with AWS staff to develop countermeasures specific to the attack profile. This may be simple IP filtering, specialized proxy servers in front of your server, deep packet inspection or any combination of these.

Secure Development

A secure product starts with secure development. The security of our products is critical for our customers and we are committed to doing our part to secure our products.

Security procedures in our product development teams are governed by the Carbon Black Product Security Program. It includes three primary components:

- **Product Risk Management Plan**: a bottom up evaluation of the risks to product security, the mitigations in place to reduce risks and the areas we are investing to further reduce risks within our products.
- **Secure Development Lifecycle**: activities during software development required to ensure security is deliberately considered during planning, development and release testing.
- **Security Response Center**: monitoring for and responding to vulnerabilities in our products post-release.

A complete description is available on carbonblack.com and in this technical whitepaper, including an overview of these components and the activities contained within.

Secure Organization Policies and Procedures

Carbon Black maintains a large library of policies and procedures related to information security and privacy. These policies are reviewed and refreshed at least annually as required. They are provided to employees during the hiring process as part of initial training and always available to employees via a web portal.

Carbon Black does not distribute these policies. As part of our SSAE-16 SOC2 assessment, our auditors have reviewed these policies to ensure their suitability. Summaries of the SOC2 reports are available upon request.

Responsibility

Carbon Black takes a blended approach to information security policies and procedures. The security of cloud systems is covered by both the Carbon Black Information Security Program, administered by the Office of the Chief Information Security Officer (CISO), as well as the Product Security Program, administered by Engineering's Product Security Team, chaired by Engineering's Director of Product Security.

The CISO's program sets the policies and frameworks for the company and our personnel. The Engineering Product Security Team manages the day to day execution of the Secure Development Lifecycle as well as cloud-specific security operations policies and procedures.

Governance of the Carbon Black Information Security Program is managed through the Security Steering Committee, which includes the Carbon Black Chief Executive Officer, Chief Financial Officer, Chief Information Officer, Chief Product Officer, Chief Information Security Officer, and VP of Operations & Engineering.

Personnel Security

Background checks

Every Carbon Black employee, contractor and subcontractor undergoes a complete background screening during the hiring process. Background checks for US personnel include:

- 7-Year Criminal History Search at Federal, State and County levels (county availability is state-dependent)
- Social Security Trace
- Consent Based Social Security Number Verification (CBSV)
- National Criminal Record Locator
- Office of Foreign Assets Controls (OFAC) checks

The background screening must be completed with no material findings before an employee's start date or contract start.

Confidentiality Agreements

Every Carbon Black employee's employment agreement includes confidentiality clauses that explicitly describes and legally protects confidential data. Any raw or attributable data from our customers is considered confidential, subject only to usage described in the Data Use provisions of the license agreement.   Any agreements with contractors and subcontractors also include confidentiality clauses.

Acceptable Use and Employee Code of Conduct

All Carbon Black employees, contractors and subcontractors are bound by an Employee Code of Conduct that describes the behaviors our culture demands as well as an Acceptable Use policy that describes appropriate use of our information systems.

Security Policies

In addition to the Acceptable Use policy, Carbon Black maintains detailed security policies that describe appropriate use of our information systems, specific to security concerns. Employees, contractors and subcontractors are required to review and acknowledge the security policies annually.

Security Training

Every Carbon Black employee also undergoes security training at the time of hiring and annually. Training content is refreshed each year to reflect current threats and trends in the security industry. Employees are required to acknowledge they understand their responsibilities in the security of our systems.

Data Classification, Data Handling and Data Retention Policies

In addition to the Personnel Security policies that provide guidelines to our employees, Carbon Black also maintains separate policies specific to classification, handling and retention of data. These policies provide very clear guidelines to ensure consistency across the entire company in the classification, handling and retention of all data, including customer data.

Incident Response Plans and Exercises

Carbon Black maintains a detailed incident response plan to prepare for the technical and administrative aspects of handling a potential breach.   Like the other policies, the incident response plan is reviewed and updated annually to ensure it remains consistent and complete.

Each year, the company runs an incident response exercise, where the key participants in incident response from Security Operations, IT, legal and communications react to potential response scenarios.

Carbon Black staffs a 24x7x365 team of responders that monitor our Cloud services for suspicious activity, using a variety of data sources and methods. In the event of an actual breach, we commit to notifying any customer whose data has been compromised as soon as possible.

In the event of a breach, we commit to notifying any customer whose data was affected as soon as practical.

Business Continuity Management

Service Continuity

Carbon Black’s Cloud Services are architected to be highly available and minimize or eliminate single points of failure. As described in detail in the backup section above, service architecture following modern cloud application practices to use resources at multiple physical datacenters in separate geographic locations to ensure the service remains available.

Additionally, each Cloud Service is an independent administrative domain, logically isolated from each other as well as Carbon Black's internal office automation and IT systems. For example, failure of Carbon Black's email server or a Domain Controller will not impact your service. Similarly, a failure in Cb Defense will not impact Response Cloud clients. Internally, each service is architected to further isolate failure domains and limit the impact of failure as much as practical.

All services test backup, failover and restore procedures as a part of day to day operations. For example, Cb Defense and Cb Response Cloud's portal are both highly available: services are hosted by resources in two datacenters and requests are distributed between each. Normal software upgrades failover service as part of the upgrade process, in the same manner as would occur if there were complete loss of a datacenter hosting service.

Carbon Black's Corporate IT services for critical business processes are similarly architected to eliminate or reduce single points of failure in both technical systems as well as personnel. Even in the event of a catastrophic outage that affects Carbon Black's Waltham headquarters, critical support operations are seamlessly transferred to personnel in other regions until service is restored.

Risk Assessment

All Carbon Black Cloud Services undergo an annual risk assessment process that catalogs and quantifies risk to the security and availability of Carbon Black Cloud Services. Any high risk items is considered for additional investment to reduce the risk.

Privacy & Compliance

Cb Response Cloud and Cb Defense each have a *Product Deep Dive document* that details exactly the information they collect. These documents are available upon request; please refer to them for more information.

Privacy

Carbon Black products collects data in two classes:

- **Device attributes:** at initial registration and each checkin, attributes such as computer name and operating system are collected and stored for computer management, context & event correlation.
- **Device activity:** In every device, a process is the primary abstraction of computation. Each process is backed by an executable file on disk. Carbon Black products monitor the processes and executable files as they access resources and collects a subset of potentially interesting activity of the processes.

Privacy concerns are typically raised when personal data or other sensitive content is collected and processed. Carbon Black products do not collect sensitive ***content***, but ***attributes of access*** to content. Carbon Black has done an extensive review of all data elements that our products and Cloud Services collect, and process. Please see the individual "Data Collection Guides" for a more detailed breakdown of what data elements are collected. These are available upon request after an NDA has been signed.

Privacy in the European Union

The European Union (EU) data protection law regulates the transfer of EU customer personal data to countries outside the European Economic Area (EEA). The EU Model Clauses are standardized contractual clauses used in agreements between service providers and their customers to ensure that any personal data leaving the EEA will be transferred in compliance with EU data-protection law and meet the requirements of the EU Data Protection Directive 95/46/EC. Carbon Black complies with the EU data protection laws and utilizes the EU Model Clauses with its customers and service providers. In addition Carbon Black has certified under the US-EU and US-Swiss Privacy Shield Framework.

Regulatory Compliance

Carbon Black's compliance requirements

Carbon Black products are not classified as Service Providers and thus are not subject to the regulatory compliance guidelines including, but not limited to, PCI-DSS, HIPAA, GLBA, SOX, FISMA or FERC.

In general, these regulations are concerned with protection of sensitive content. As described above, Carbon Black products do not collect content, but attributes of access to content.

As described in the introduction, Cloud Services are covered by a SSAE-16 SOC2 Type 1 report, completed by an independent 3d party audit firm. SSAE-16 SOC2 reports are similar in structure to financial audit reports, except they focus on technical controls instead of financial controls. It is an industry standard used by many organizations to validate the security controls in place to manage the confidentiality, integrity and availability of cloud infrastructure and client data.

General Data Protection Regulation (GDPR)

Carbon Black's products never collect data with the intention of attribution. Meaning that the majority of data elements are not considered personal data because the contents cannot be tied directly to an individual without additional information being provided outside of the product. Data elements such as IP address may be considered as personal data, so Carbon Black has taken precautions and completed an in-depth review of all data elements collected for each Cloud Service. The specifics are outlined in our “Data Collection Guides” which are available upon request after an NDA has been signed.

Your compliance requirements and Carbon Black

Carbon Black Cloud Services can help you meet your compliance requirements. Please see our regulatory compliance matrix and related links for details.