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 9
  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
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Training</td>
<td>14</td>
</tr>
<tr>
<td>Data Classification, Data Handling and Data Retention Policies</td>
<td>14</td>
</tr>
<tr>
<td>Incident Response Plans and Exercises</td>
<td>14</td>
</tr>
<tr>
<td>Business Continuity Management</td>
<td>15</td>
</tr>
<tr>
<td>Service Continuity</td>
<td>15</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>15</td>
</tr>
<tr>
<td><strong>Privacy &amp; Compliance</strong></td>
<td>15</td>
</tr>
<tr>
<td>Privacy</td>
<td>16</td>
</tr>
<tr>
<td>Privacy in the European Union</td>
<td>16</td>
</tr>
<tr>
<td>Regulatory Compliance</td>
<td>16</td>
</tr>
<tr>
<td>Carbon Black’s compliance requirements</td>
<td>16</td>
</tr>
<tr>
<td>Your compliance requirements and Carbon Black</td>
<td>17</td>
</tr>
</tbody>
</table>
Welcome

This guide is an overview of the people, processes, and technology that Carbon Black Inc. and its subsidiaries (“Carbon Black” or “us”, “our”) uses to develop, test, and deploy our cloud products.

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

- "security of the cloud" - security measures the cloud service that the 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.

Carbon Black uses Amazon Web Services™ (AWS) as our cloud hosting 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

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(s), 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 to reset forgotten passwords. You should also review your internal data classifications and have a good understanding of what types of (regulated) data might be within your environment and processed by Carbon Black.

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 that they focus on technical controls instead of on financial controls. It is an industry standard that is used to validate the security controls 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 that are 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 that are delivered via the cloud (referred to as “Cloud Services”).

Secure Data

In the world of the cloud, “data security” has different definitions for different people. This section covers data security from the following 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 networks have access to your data.

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

- **Products that are hosted on the CB Predictive Security Cloud** (other than CB ThreatSight): Northern Virginia (AWS US-East region), Frankfurt, Germany (AWS EU-Central region) and Tokyo, Japan (AWS AP-NorthEast region).
- **CB ThreatSight**: Northern Virginia (AWS US-East region).
- **CB Response Cloud**: Northern Virginia (AWS US-East region), Frankfurt, Germany (AWS EU-Central region), or Singapore (AWS Asia Pacific region). Threat intelligence data that is collected by the CB Response Cloud is stored in the United States.

During provisioning, CB Predictive Security Cloud and CB Response Cloud allow you to choose the AWS region that hosts your service.

Physical Security

AWS Cloud Hosting

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 these physical controls is included in AWS ISO 27001 audit, the PCI assessment, ITAR audit, and FedRAMP testing programs. See the [AWS Risk and Compliance Whitepaper](#) for information about AWS physical security.

---

1 Products hosted on the CB Predictive Security Cloud include CB Defense, CB ThreatHunter, CB LiveOps and CB ThreatSight.
Private Datacenter in Boston, MA

Resources in Carbon Black’s private datacenter in Boston, MA 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 visitor access management procedures.

The datacenter has environmental controls that include climate control, redundant A/B condition power supplies to each cage, and 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

Neither AWS nor Carbon Black will disclose your data unless required by law, regardless of the applied source or type of political pressure. Both AWS and Carbon Black policy will 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 AWS data privacy policies.

In providing Cloud Services, Carbon Black can engage other third party services providers. Before engaging such providers, Carbon Black conducts review of service provider’s security, privacy and confidentiality practices, and contractually imposes Carbon Black’s standard security and privacy requirement as required by applicable laws. A current list of third party service providers and their data processing locations is posted on our Policies Portal (https://www.carbonblack.com/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. 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 that processes the data or the Carbon Black application.

Only Carbon Black authorized personnel have access to production systems where customer data is stored. All access is supplied 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

The data from your endpoint(s) to the cloud instance is encrypted in transit by using Transport Layer Security (TLS). Carbon Black closely monitors industry best practices for TLS configurations and makes sure that our products enforce appropriate protocols and ciphers. Any data transmission via unsecured transports is not supported and is strictly prohibited.

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

Data segmentation & destruction

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

CB Predictive Security Cloud

Customer data is logically segmented from other customer data with Role Based Access Controls. When your license ends, your logins are disabled and Endpoint data stored in your console is purged within 90 days after termination of business relationship. The destruction delay is a safeguard against miscommunication and coordination.

CB Response Cloud

Customer data is physically and logically segmented from other customer data. When your CB Response Cloud license ends, the server is shutdown and the console is inaccessible. Any remaining sensors are automatically uninstalled seven days after the license ends. The server is deleted 14 days after expiration. All backups are deleted 30 days after expiration.

Reference individual product “Data Collection Guide” documents” for more details.

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 authorized user behavior on assets. These logs are transmitted in real-time to a central logging system and are 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’s Cloud Services is centrally logged. Scripts, pattern analysis and threat intelligence sources are applied to the data to highlight suspicious activity. A team of security analysts actively review activity across all environments for suspicious activity.

Third-Party Penetration Tests

All of Carbon Black’s Cloud Services undergo regular network penetration tests and intrusion exercises by a third-party security firm. The network penetration tests validate our configuration management procedures, and 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

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

Operating system configurations are tightly controlled and hardened. In addition to unnecessary services, they consume resources. They present a stability risk to the availability and performance of systems that are running on cloud systems. We carefully limit operating system services to those services that are critical to the function of the operating system and our application.

Each cloud service team follows patch management procedures to make sure that software packages are at current patch levels, and all required security patches are applied. Patches are applied regularly as part of the routine operations and updates to the systems; exception procedures are in place for critical patches that require immediate application to maintain optimal security.

Vulnerability Scans

All of Carbon Black’s 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’s cloud services.

**Backups and availability**

Data backups and disaster recovery preparations adhere to each service’s defined recovery point objective (RPO) and recovery time objective (RTO). Each cloud service maintains procedures that are required for the specific technology that is used.

**CB Predictive Security Cloud**

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

CB Predictive Security Cloud 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 services as part of each upgrade: the same as if there were complete loss of a datacenter.

In the unlikely event that the service is unavailable, CB sensors cache recorded data until the server becomes available. Service downtime does not result in data loss unless the volume of data exceeds the 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 selected region. AWS datacenters are highly-available in their design: network, power and other critical resources are redundant to mitigate the risk of wide datacenter outages.

In the event of a hardware failure in the physical computer that hosts a virtual machine, the virtual machine is migrated to a new machine with no data loss and minimal downtime.

Snapshots of data volumes are taken hourly and are retained for twenty-four hours. In the event of data corruption or lost data, your data is restored to the most recent valid backup. Backup restoration procedures are tested at least semi-annually.

Virtual machine images and data backups are replicated to a second AWS datacenter in 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 that is used on your live volumes using AES-256. Encryption keys are unique for each customer.

If the server is unavailable, sensors cache recorded data until the server is available. The local cache size is configurable; the default is 2GB, which is enough for approximately thirty 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, which includes automated testing and other checks that are used as a conditional acceptance before 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 that is used to develop our applications (more information on the Carbon Black Product Security Program is available in the Secure Development section). As a result, all changes to production infrastructure:

- Are saved as a clearly-defined changeset in a source code repository with metadata that includes who made the change, when, why, and a reference to a ticket that is 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 additional engineer who has 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 is 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 personnel will actively work with AWS staff to develop countermeasures specific to the attack profile. This can be simple IP filtering, specialized proxy servers in front of the server, deep packet inspection, or any combination of these measures.

**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 in which we are investing to further reduce risks.
- **Secure Development Lifecycle**: Activities during software development that are required to make sure that 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 that are 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 are 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 services is covered by the Carbon Black Information Security Program, administered by the Office of the Chief Information Security Officer (CISO) as well as the Product Security Program, is administered by the Engineering Product Security Team, and 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 and cloud-specific security operations policies and procedures.

Governance of the Carbon Black Information Security Program is managed through the Security Steering Committee and Security Governance Council. This includes, but is not limited to, the Carbon Black Chief Executive Officer, Chief Financial Officer, Chief Information Officer, Chief Product Officer, Chief Information Security Officer, VP of Operations & Engineering, and Governance Council.

Personnel Security

Background checks

Every Carbon Black employee and contractor undergoes a 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
- Widescreen Plus National Criminal Search
- Social security validation

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 customer/confidential data. Any raw or attributable data from our customers is considered Customer Data and is subject to usage that is described in the applicable license agreement. Any agreements with third-party service providers also include confidentiality clauses.

Acceptable Use and Code of Conduct

All Carbon Black employees are bound by the Carbon Black Code of Business Conduct and Ethics that describes the behaviors that our culture demands. It also describes an Acceptable Use policy (also applicable to contractors) that describes appropriate use of our information and 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 and contractors are required to review and acknowledge the security policies annually.

Security Training

Every Carbon Black employee undergoes security training both 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 that 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 maintains separate policies specific to classification, handling, and data retention. These policies provide 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 other policies, the incident response plan is reviewed and updated annually to make sure that 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.

**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 preceding backup section, service architecture follows modern cloud application practices to use resources at multiple physical datacenters in separate geographic locations, to make sure that the service remains available.

Additionally, each cloud service is an independent administrative domain that is 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 does not impact your service. Similarly, a failure in CB Defense does not impact CB Response cloud clients. Internally, each service is architected to further isolate failure domains and limit the impact of failure as much as is 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 service. 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 technical systems and 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’s Cloud Services undergo an annual risk assessment process that catalogs and quantifies risk to the security and availability of Carbon Black’s Cloud Services. Any high risk item is considered for additional investment to reduce the risk.

**Privacy & Compliance**

Each cloud service has a ‘Data Collection Guide’ document that details the collected information. These documents are available upon request.
Privacy

Carbon Black’s cloud services collect data in two classes:

- **Device attributes**: At initial registration and at each check-in, attributes such as computer name and operating system are collected and stored for computer management, context, and 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. As a result, device activity is either process-based (every time a process is launched and takes an action), or are binary-based (every time a new executable executes). Carbon Black products monitor the processes and executable files as they access resources and collect a subset of activities for analysis.

The data can include user or device IDs, IP addresses, executable files, file paths, file names, email addresses, binary data and other. Some of these attributes can constitute ‘personal data’ under applicable privacy laws such as the General Data Protection Regulation (“GDPR”). Carbon Black has done an extensive review of all data elements that each Cloud Service collects and processes. 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.

Carbon Black Privacy Program

Carbon Black respects and is committed to protecting personal data. Our data protection and privacy program reflects current global principles, legal frameworks and standards on processing personal data. Carbon Black is EU-U.S. and Swiss-U.S. Privacy Shield certified.

To read Carbon Black’s full privacy statement, see: [https://www.carbonblack.com/privacy-policy/](https://www.carbonblack.com/privacy-policy/)

Regulatory Compliance

General Data Protection Regulation (GDPR)

Processing personal data to ensure endpoint security is broadly recognized as a “legitimate interest” under the GDPR. Recital 49 of the GDPR says that every data controller has a legitimate interest in

> "the processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity and confidentiality of stored or transmitted personal data. And the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by"
Carbon Black’s cloud services are aimed at preventing unauthorized malware, malicious code or other attach distribution and damage to computer systems. Please consult your privacy advisor for proper classification of the legal basis under the GDPR before deploying Carbon Black’s cloud services.

Although Carbon Black’s cloud services are not a compliance tool, certain cloud services are often used by our customers to detect, contain and response to a data breach. For example, CB Response Cloud or CB ThreatHunter empowers security operations teams and/or incident response teams to proactively hunt for threats, uncover suspicious behavior, disrupt active attacks, and address gaps in defenses.

Other compliance requirements and Carbon Black

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