THIS COVER SHEET IS TO BE DELETED PRIOR TO CONTRACT SIGNATURE AND DOES NOT FORM PART OF THE AGREEMENT, WHETHER OR NOT ATTACHED TO THE AGREEMENT AT THE TIME OF SIGNATURE.

Thank you for reviewing Carbon Black’s End User Agreement or Master Terms and Conditions agreement (each referred to in this Cover Sheet as the “Agreement”) that govern Carbon Black products and services (together “Carbon Black Products”). We recognize that sometimes attorneys, contract professionals, and procurement specialists are asked to review an agreement without being given an explanation of what is being purchased as well as how the vendor’s contracts process work. We hope that this Cover Sheet will be useful as you review the Agreement.

This Cover Sheet is provided for reference purposes only and does not create any warranties or obligations on the part of either party.

What products and services does Carbon Black provide?
Carbon Black offers endpoint security cloud services and on-premises software applications, depending on our customers’ needs. An ‘endpoint’ is a computing device(s) that may include laptops, desktops, tablets, point of sale devices and servers.

• Cloud services. Carbon Black’s cloud services use a cloud delivery model whereby data is collected via proprietary software sensors installed on customer endpoints and sent to Carbon Black’s servers for analysis. Customer’s administrators access Carbon Black’s cloud services console running in Carbon Black’s cloud environment. Carbon Black manages and updates the cloud services console. All customers are on the current version of Carbon Black cloud services console at all times.

• On-premises software. Carbon Black’s on-premises software is provided for installation and configuration by customer in its own computing environment. Carbon Black’s proprietary sensor software is installed on customer endpoints and automatically collects data for analysis. But, instead of being sent to Carbon Black’s cloud servers, the data remains in customer’s computing environment, where it is analyzed by Carbon Black’s on-premises software. Using software settings, customers may opt-in to share some data with Carbon Black for limited purposes (such as troubleshooting or diagnostics) at which point such data will be stored Carbon Black’s servers. The customer is responsible for managing the on-premises software and the data stored in own computing environment.

Can I customize Carbon Black’s cloud services?
Carbon Black offers cloud services utilize a “one-to-many” cloud architecture, whereby the system resources may be shared simultaneously by multiple customers. In this way, customers avoid costly and disruptive upgrades as well as the expense of building and operating their own computing environment.

What data will Carbon Black Products collect?
Carbon Black Products collect technical data relating to an endpoint or activity at, and traffic through, an endpoint. At a high level, this includes data elements relating to process and file executions, network connections, file modifications, registry modifications, cross-process events, unique binaries, API calls, etc. Depending on the specific Carbon Black Product and configuration selected by the customer, some examples of these elements could include things such as IP address, device ID, file name, binaries and associated metadata, command name, endpoint connections including date and time stamp, or other technical data.

Importantly, Carbon Black Products are not intended to function as a storage/repository system for customer’s data. This means that unlike many other cloud services, where customers transfer their data to the provider’s systems for long-term storage and processing, Carbon Black’s proprietary sensor software is design to capture only the information necessary for Carbon Black Product(s) to function.

What is ‘threat intelligence data’?
Certain Carbon Black Products collect metadata relating to malicious or potentially malicious code, attacks, and activities on monitored customer endpoints (called “Threat Intelligence Data”). The Threat Intelligence Data is collected and analyzed to identify and alert you to threats in your environment, and to improve the security efficacy of the Carbon Black Products. Threat Intelligence Data may be included in Carbon Black’s threat intelligence data feed (which is one of numerous threat data feeds available to customers through the Carbon Black Products that allow a customer to identify attacks more quickly and effectively.) Prior to inclusion in the threat intelligence data feed, all Threat Intelligence Data is reduced to a unique file hash or to queries or general behavioral descriptions that can be used to identify the same or similar malicious or potentially malicious code in customer systems. All data included in the Threat Intelligence Data feed is aggregated, and not attributable to any individual customer.
How does Carbon Black protect customer data?
Protecting the security and privacy of our customers’ data is a priority for Carbon Black. Carbon Black regards all Customer Data as confidential, and, to the extent it includes personal data, Carbon Black complies with GDPR and other data privacy laws applicable to it. Carbon Black has adopted appropriate technical and organizational security measures designed to protect all customer data under its control. Carbon Black's formal and comprehensive security program is detailed in its independent third party SOC-2 Type 2 audit report, our Information Security Policy, Security and Privacy Guide, and Privacy Policy, all of which can be found on the Carbon Black Policies Page as referenced in the Agreement. This comprehensive security program is provided across our product infrastructure, development, and corporate environments. The Agreement has additional provisions that further detail Carbon Black’s security obligations and our protection of Customer Data.

Unfortunately, Carbon Black is not able to agree to individual customer security policies or requirements, as it is not practical given our unique single back-end security program, and the shared cloud operations and support model applicable to all customers.

Does Carbon Black use third party service provider(s) to provide Carbon Black Products?
Yes. Carbon Black’s Products may incorporate certain elements provided by third party service providers. Carbon Black reviews security, privacy and confidentiality practices of its service providers and contractually requires them to apply security and privacy requirements equivalent to those in our Agreement. A current list of such providers is at all times posted on our Policies Page (https://www.carbonblack.com/policies).

Will I be able to access and/or retrieve my data from the Carbon Black Products?
As is detailed in the Agreement, Carbon Black’s customers own their data at all times. Customers can access and download copies of their data stored in the Carbon Black Products.

How does the Agreement work?
The Agreement contains the general legal terms and conditions governing the use of Carbon Black Products under either delivery model. Once the Agreement is accepted, a customer can purchase any Carbon Black Products pursuant to the Agreement terms. If agreed with Carbon Black, the Agreement can also be used for product evaluations.

I am buying Carbon Black through a Carbon Black reseller; what paperwork do I need?
Most Carbon Black customers purchase through an authorized Carbon Black reseller. Once you enter into the Agreement with Carbon Black you will provide an order (usually via a purchase order) to the authorized Carbon Black reseller. The reseller will then place your order directly with Carbon Black.

Do you have a GDPR-compliant data processing agreement (DPA)?
Yes. Our Agreement automatically incorporates a GDPR Policy. The GDPR Policy includes all GDPR Article 28 requirements. The Agreement also has provisions designed to address the security and confidentiality of Customer Data that are specifically tailored to the kinds of data collection and processing performed by Carbon Black and the Carbon Black Products. When required, we also have a stand-alone DPA that can be executed between the customer and Carbon Black.

Does Carbon Black offer a service level agreement?
Yes. Carbon Black provides what we believe to be a best-in-class service level agreement for our cloud services, with specified service availability levels and credits. This Cloud Services SLA applies for all cloud services customers. Since Carbon Black has the same operational business model for our entire customer base, the SLA cannot be modified on an individual customer by customer basis.

Does Carbon Black offer a termination for convenience?
Carbon Black does not agree to “termination for convenience.” Since Carbon Black incurs significant expenses in advance relating to the provision of Carbon Black Products, Carbon Black cannot allow early termination for convenience of customer subscription. As a public company, termination for convenience could also adversely impact our ability to recognize revenue and report financial results.

Does Carbon Black offer an acceptance test period?
Carbon Black's Products are COTS (Commercial-Off-The-Shelf) products, not created for or customized for individual customers. As such, the functionality of our products and services has already been demonstrated by the thousands of existing customers who run their businesses on the same products and services. Thus, acceptance testing does not comport with Carbon Black's business model, especially since many of our customers undertake proof-of-concept evaluations in advance of purchase.
Will Carbon Black permit customers to audit Carbon Black?
In order to maintain the security of Carbon Black’s services and facilities, except as required by law Carbon Black cannot allow facility audits. In order to provide Customers with objective evidence that Carbon Black is adequately maintaining its security controls, Carbon Black engages qualified third parties to produce an annual SOC-2 audit report and to perform vulnerability scanning and penetration testing, as applicable. (Please note that Carbon Black’s GDPR Policy allows for customer audits in limited circumstances).

Does Carbon Black offer unlimited liability for security breaches?
Carbon Black takes its security obligations very seriously, and continues to evaluate and improve its privacy and security measures and controls as new technologies and methodologies are created. However, despite Carbon Black’s efforts, Carbon Black does not control our customers’ internal environment or user activities, or elements of the end-to-end internet infrastructure, all of which may be subject to or the cause of unauthorized intrusion. In addition, as Carbon Black does not limit the types of data our customers may possess, or the value of such data, it is impossible for us to evaluate the risks associated with data held by our customers. As such, Carbon Black cannot become an "insurance provider" for our customers' data, and must include a liability limitation relating to security obligations.

Are other types of damages subject to a limitation of liability?
A fundamental principle of Carbon Black's cloud business model is that any damages and any other breaches of the Agreement are subject to a limitation of liability. This limitation of liability also serves to protect our customers by limiting their liability to Carbon Black.

Can we negotiate the Agreement and/or attach our own security/privacy exhibits?
Carbon Black’s ability to provide a consistently high level of service at a reasonable price relies on being able to standardize the delivery model for Carbon Black Products and associated security and data privacy methodologies. As a result, Carbon Black cannot agree to contract documents that do not accurately reflect those elements.

Will Carbon Black ever make changes to the Carbon Black cloud services?
Carbon Black is constantly working to improve our cloud services, whether by adding new or improved functionality or addressing suggestions from our customers. As such Carbon Black regularly makes updates to the cloud services. Such updates are applied by Carbon Black across the entire cloud services platform at the same time, with no effort or assistance required from our customers. This is one major advantage of purchasing Carbon Black cloud services, as our customers are always on the most current version of the cloud services without having to perform time-consuming and costly upgrades on their own infrastructure. Carbon Black commits that any such updates are not designed to degrade the cloud services or create additional obligations for our customers. Please see the specific language in the Agreement for details.

Will Carbon Black ever make changes to its policies?
As detailed in the Agreement, all applicable Carbon Black policies are available on the Policies Page of our website. From time to time, Carbon Black updates its policies or introduces new policies to comply with new legal requirements and regulations, or in response to market demands. The efficiency and manageability of Carbon Black’s operational model requires that the same policies apply to all Carbon Black customers. As a result, we are not able to exempt individual customers from modifications that we make to our policies. As with updates to the cloud services, however, we do commit that any changes are not designed to degrade the policies or create additional obligations for our customers. Please see the specific language in the Agreement for details.