verizon

Verizon Risk Report +

1. GENERAL

1.1 **Service Definition.** Verizon Risk Report service provides an automated assessment of Customer's cybersecurity posture that identifies and evaluates Customer's current security capabilities and security gaps, weaknesses, and associated risks. Verizon Risk Report ~~Level 1 helps Customer to quantify their current exposure to cyber related risks using BitSight's risk scoring~~consists of three service ~~combined with deep web and dark web information from Recorded Future for external assessments, and further enhanced with insights from the Verizon Data Breach Investigation Report (DBIR). Verizon Risk Report Level 2 combines this~~levels: Level 1 – Outside-In ~~Security Posture Score with an internal analysis, of Customer's systems using Tanium and Cylance software agents deployed on Customer endpoints~~view, Level 2 – Inside- Out view, and Level 3 – Culture and Process. The three levels can be stacked to provide ~~an external and internal risk profile, which can be updated on a monthly, weekly or daily basis. Verizon Risk Report Level 3 combines the external and internal assessments with the Verizon Cyber Risk Program, to add a culture and process assessment, on a monthly or quarterly basis, providing~~ a 360 degree assessment of Customer's cybersecurity posture. Each Level provides additional data and insight to quantify risk posture which can help improve security through preventative measures. Each Verizon Risk Report Level provides specific recommendations, based on the ~~risk report~~available data, to aid Customer in addressing vulnerabilities, prepare for potential threats, and improve its risk management position.

1.2 **Service Implementation**. Verizon ~~Risk Report Level 1~~ will ~~provide~~send automated communications to ~~the identified Customer point of contact~~ Customer's personnel authorized by Customer to access the Customer portal and to interact with Verizon for the Service (Authorized ~~Contact~~Contacts) to establish ~~the Service~~, access ~~and~~, administer ~~adding other Authorized Contacts to~~ , and utilize the Service. ~~Verizon Risk Report Level 2 and/or 3 are implemented to provide the required Services. Upon Service Activation,~~ Verizon will assign a ~~Project Manager~~project manager to ~~Customer who will schedule a kick off meeting to introduce the Verizon service delivery team, identify the Authorized Contacts, discuss the scope of the Verizon Risk Report Level service and its business impacts, and obtain any required~~

verizon

~~information from~~assist Customer in operationalizing the Service, including ~~appropriate configuration/specification. Upon receipt of all customer required information, the Verizon service delivery team will provide a schedule for implementation. Configuration of Verizon Risk Report Level 1 will include BitSight MyOrg with Forensics features. Configuration of Verizon Risk Report Level 2 will include~~ configuration and deployment ~~of Tanium and Cylance Agents within the Customer Environment to retrieve endpoint device data used to create the Level 2 Risk Vectors and configuration of the appropriate network/security devices so that the Verizon provided Tanium and Cylance Agents can communicate externally. If Customer already has Tanium and/or Cylance deployed, then the Customer will provide data from those solutions for Verizon to process into risk vectors.~~ Service Implementation requires Customer to be authorized to obtain and provide endpoint data to Verizon and authorizes Verizon to process and display the endpoint data within the Verizon Risk Report.

~~1.3 **Service Features.** Verizon Risk Report consists of three service levels which can be stacked to provide a 360 degree view of Customer's cybersecurity posture. Each level provides additional data and insight to quantify measurements which can help improve security through preventative measures against cyber related threats.~~

~~1.3.1~~1.3 **Verizon Risk Report Level 1 – Outside-In View**

~~1.3.1.1 **Overview.**~~ The Level 1 external risk score is an "outside-in" assessment of Customer's security posture based on: (1) BitSight report and External Risk Vectors; (2) Recorded Future deep web and dark web data; and, (3) Verizon Data Breach Investigations Report Incident Classification Patterns.

1.3.1 ~~the BitSight report which~~ **External Risk Vectors.** The BitSight report collects data points accessible and visible from the public internet to determine a risk rating ranging from 250 to 900 and is refreshed every 24 hours. The BitSight rating is calculated ~~by evaluating compromised systems, diligence information, user behavior~~on 21 External Risk Vectors which includes 4 categories: Compromised Systems, Diligence, User Behavior and Others, such as publicly ~~reported~~disclosed data breaches ~~based on 21 External Risk Vectors from BitSight.~~involving data loss or data theft. The BitSight rating, rating range, and External Risk Vectors are set at the sole discretion of BitSight and subject to change from time to time. ~~Currently, the risk rating range determines Customer's BitSight Score and categorized as Basic, Intermediate, and Advanced as follows:~~

~~Basic~~	~~Intermediate~~	~~Advanced~~
~~250 – 639~~	~~640 – 739~~	~~740 – 900~~
~~Bottom 20% of companies~~	~~Middle 40% of companies~~	~~Top 40% of companies~~

~~Customers may also purchase third party monitoring reports for their partners, suppliers, vendors, and/or potential acquisitions (Vendor Monitoring).~~

1.3.~~1.~~2 **External ~~Risk Vectors.~~** ~~The BitSight External Risk Vectors include 4 categories: Compromised Systems, Diligence, User Behavior and Other.~~

- ~~Compromised Systems include: botnet infections, spam propagation, malware servers, unsolicited communication, and potentially exploited (system vulnerability to adware, spyware, and remote access tools).~~
- ~~Diligence includes: open ports, TLS/SSL certificates, TLS/SSL configuration, web application headers, sender policy framework (SPF) domains, Domain Keys Identified Mail (DKIM), patching cadence, server software, desktop software, mobile software, insecure systems, DNSSEC Records, and domain squatting.~~
- ~~User Behaviors include: file sharing and disclosed credentials.~~
- ~~Other includes publicly disclosed data breaches involving data loss or data theft.~~

verizon

1.3.1.3 **External Threat Intelligence**. The external assessment also includes Recorded Future's Deep Webdeep web and Dark Webdark web data that highlight potential threats and global trends, including company brand mentions and company credentials over the past two years, on a quarterly basis.

1.3.1.43 **Verizon Data Breach Investigation Report (DBIR).** The external assessment also provides incident classification patterns based on BitSight External Risk Vectors. In addition, the DBIR attack vectors, attack varieties, motives, industries, geographies, and customer size are used to prioritize thesethe BitSight External Risk Vectors. DBIR Incident Classification Patterns include the following:

- : Crimeware: All instances involving malware that did not fit into a more specific pattern. The majority of incidents that comprise this pattern are opportunistic in nature and are financially motivated. This pattern will often affect customers and is where "typical" malware infections are placed.
- , Denial of Service: Any attack intended to compromise the availability of networks and systems. Includes both network and application attacks designed to overwhelm systems, resulting in performance degradation or interruption of service.
- , Physical Theft & Loss: Any incident where an information asset went missing, whether through misplacement or malice.
- , Payment Card Skimmers: All incidents in which a skimming device was physically implanted (tampering) on an asset that reads magnetic stripe data from a payment card (e.g. ATMs, gas pumps, POS terminals, etc.)
- , Insider **and Privileged**Privilege Misuse: All incidents tagged with the action category of Misuse—any unapproved or malicious use of organizational resources—falls within this pattern. This is mainly insider-only misuse, but outsiders (due to collusion) and partners (because they are granted privileges) show up as well.
- , Cyber-Espionage: Incidents in this pattern include unauthorized network or system access linked to state-affiliated actors and/or exhibiting the motive of espionage.
- , Point of Sale Intrusions: Remote attacks against the environments where card-present retail transactions are conducted. POS terminals and POS controllers are the targeted assets. Physical tampering of PIN entry device (PED) pads or swapping out devices is covered in the Payment Card Skimmers section.
- , Web Application Attacks: Any incident in which a web application was the vector of attack. This includes exploits of code-level vulnerabilities in the application as well as thwarting authentication mechanisms.
- , Miscellaneous Errors: Incidents in which unintentional actions directly compromised an attribute of a security asset. This does not include lost devices, which are grouped with theft.
- , and Everything Else: Any incident that did not classify as one of the nine patterns (Phishing, Footprinting, Pretexting, Use of Stolen Cards, Brute Force, Back Door, etc.).

1.3.4 **Vendor Monitoring**. Customers may also purchase BitSight's third party monitoring reports for their partners, suppliers, vendors, and/or potential acquisitions.

1.3.25 **Excluded Services**. BitSight may offer additional services to the Customer. Any BitSight services not incorporated in the Service are handled directly between the Customer and BitSight under a separate agreement.

1.4 **Verizon Risk Report Level 2 – Inside-Out View**

1.3.2.1 **Overview.** . The internal risk score is an "inside-out" assessment which focuses on two groups of internal risk vectors: Infrastructure that is, measured using Tanium technology, and Endpoint Threat Management that is, measured using Cylance technology, and both are combined with Verizon Risk Report Level 1. for a fuller view of Customer's cyber security posture. This internal security posture is analyzed through the deployment of both Tanium and Cylance agents to Customer endpoints to gather

data used to calculate the grades ranging from A (the highest score) to F (is the lowest score) for each internal risk vector across both groups.

1.~~3.2.2~~4.1 **Infrastructure Internal Risk Vectors.** The Infrastructure group is analyzed using Tanium technology and its internal risk vectors, ~~as follows~~including: unexpected running services, uncommon port usage, end of life software in use, vulnerable firmware versions, systems in poor health, endpoint visible wireless networks, endpoint visible wireless networks, identify dual homed devices, identify unusual connections, identify anomalies/misconfigured password & audit policies, identify user misbehavior, identify SSL certificate issues, network segmentation, identify unapproved established connections, identify operating system risks, identify application risks, and identify anomalies that could indicate compromise. These risk vectors can change over time.

1.~~3~~4.2.~~3~~ **Endpoint Threat Management**. The Endpoint Threat Management group uses Cylance technology to assess internal risks posed by malware, potentially unwanted programs (PUPs), and dual use tools.

- ~~Malware category analyzes endpoints containing: malware, ransomware, fake security software, backdoors, viruses, downloaders, rootkits, infostealers, remnants, worms, exploit based malware, droppers, bots, and generic malware.~~
- ~~Potentially unwanted programs category analyzes endpoints containing: adware, games, keygens, toolbars, scripting tools, remote access tools, corrupted PUPs, hacking tools, portable applications, generic PUPs, and other PUPs.~~
- ~~Dual use tools category analyzes endpoints containing: remote access tools, password crackers, cracking software, monitoring tools and general dual use detections.~~
- ~~These risk vectors can change over time.~~

1.~~3.3~~5 **Verizon Risk Report Level 3 – Culture and Process View**

~~1.3.3.1 **Overview.**~~ The Culture and Process score provides a 360 degree security risk assessment of Customer's overall culture and processes when combined with Verizon Risk Report Level 1 and Level 2~~ involving all the elements that are required to meet the most rigorous security framework methodologies within the industry.~~. Verizon will deploy automated tools and human intelligence to generate ~~comprehensive assessments~~an assessment of ~~the customer~~Customer's culture and process risk vector data to calculate the grades ranging from A (highest score) to F (lowest score) for each culture and process risk vector across the organization, resulting in Customer's overall security posture and threat level scores. Verizon will provide an Executive Report of Culture and Process Assessment ~~Report~~ with recommendations for improvements to Customer's security posture.

1.~~3.3.2~~5.1 **Culture and Process Risk Vectors**. Verizon uses 12 categories to assess Customer's culture and process risk vectors. These risk vector assessments can change over time. Customer can purchase additional units to be assessed at the then current rate. The 12 categories include the following assessments: External Vulnerability (100 IPs); IP Reputational (100 IPs); NetFlow (100 IPs); Web Application (3 web applications); Internal Vulnerability (3,300 IP addresses); E-Mail Filter Check (2 email gateways); Firewall (3 firewall); Endpoint System (500 IPs); Phishing (600 email addresses); Wireless; Physical Inspection (1 floor, 1 building); and, Policy, Process, and Procedure.

~~**External Vulnerability Assessment**: Verizon will scan specific Customer IP (CIP) addresses or a range of Customer IP addresses (as provided in Exhibit A attached hereto) to discover active devices, identify operating systems, find open network ports and determine which services are running with those ports, and uncover vulnerabilities, leveraging Level~~

- ~~1 data. The results from the external risk assessment will be used to calculate a portion of the Risk score and will be detailed in the quarterly Level 3 –~~.5.2 **Executive Report of Culture and Process** ~~View report. Verizon will report Customer's External Vulnerability Assessment Score, Trend, and Recommendations to reduce vulnerabilities and unexpected services. This assessment includes 100 IP addresses and Customer may purchase additional IP addresses at the then current rate.~~

- **IP Reputational Assessment**: Verizon will analyze specific Customer IP address and/or ranges, and Customer domain names within an internet based cyber analytic platform. The analysis will be based on a set of evolving use cases derived from emerging threat conditions, such as registered fraud domains, disclosed incidents, watchlist hits, spam, and phishing activities. Verizon will leverage Level 1 external risk vectors and Recorded Future company specific brand and credentials with industry specific information for enhanced output. The results from the IP reputational assessment will be used to calculate a portion of the Risk score and will be detailed in the quarterly Level 3 - Culture and Process View report. Verizon will report Customer's IP Reputational Assessment Score, Trend, and Recommendations to help decrease the likelihood of incident disclosures and negative domain mentions. This assessment includes 100 IP addresses and Customer may purchase additional IP addresses at the then current rate.
- **NetFlow Assessment**: Verizon will conduct a search to correlate Customer IP Addresses with NetFlow data (IP network traffic as it enters or exists a router interface) for a period of at least 15 days. The NetFlow assessment will capture routing and source/destination CIP information to help protect Customer from potential abuses of services or unauthorized access to its information, systems and applications. The results from the NetFlow assessment will be used to calculate a portion of the Risk score and will be detailed in the quarterly Level 3 - Culture and Process View report. Verizon will report Customer's NetFlow Assessment Score, Trend, Recommendations to help decrease the volume of suspicious internet communications. This assessment includes 100 IP addresses and Customer may purchase additional IP addresses at the then current rate.
- **Web Application Assessment:** Verizon will scan specific Customer IP Addresses or range of IP Addresses, and/or specific URLs to discover web application vulnerabilities and associated weaknesses, leveraging both Level 1 external risk vectors and Level 2 internal risk vectors data. The results from the Web Application assessment will be used to calculate a portion of the Risk score and will be detailed in the quarterly Level 3 - Culture and Process View report. Verizon will report Customer's Web Application Assessment Score, Trend Recommendations to help remove application vulnerabilities. This assessment includes 3 external web applications and Customer may purchase additional web applications at the then current rate.
- **Internal Vulnerability Assessment**: Verizon will scan specific Customer IP Addresses and/or range of IP Addresses to discover active devices, identify operating systems, and uncover vulnerabilities, leveraging Level 1 internal risk vectors data. Internal scanning includes provision of a various Appliances, including some hosted on Customer's internal network and Virtual Appliance which is deployed onto a Customer-provided virtualization platform (e.g., VMware) to bring security and compliance assessment capabilities to the Customer network without the need to deploy dedicated hardware. The results from the Internal Vulnerability assessment will be used to calculate a portion of the Risk score and will be detailed in the quarterly Level 3 - Culture and Process View report. Verizon will report Customer's Internal Vulnerability Assessment Score, Trend and Recommendations to help reduce vulnerabilities and unexpected services. This assessment includes 3,300 IP addresses and Customer may purchase additional IP addresses at the then current rate.
- **E-Mail Filter Check Assessment**: Verizon will evaluate the effectiveness of Customer's e-mail gateway content filtering and endpoint filtering controls. A series of e-mails with attachments will be sent to a Customer e-mail address with attachments. The e-mails are not invasive and/or dangerous to the Customer. Customer will evaluate that the recipient(s) follow appropriate verification instructions and record the results. Customer will ensure that the Verizon analyst has an email account on the Customer's network and the analyst will record the actions taken by the Customer's network to defend against the simulated threat scenarios. Customer may opt to be responsible for recording the actions taken by the Customer's network to defend against the simulated threat scenarios and providing this to the Verizon analyst. The results from the E-Mail Filter Check assessment will be used to calculate a portion of the Risk score and will be detailed in the quarterly Level 3 - Culture and Process View report. Verizon will report Customer's E-Mail Filter Assessment Score, Trend and Recommendation to reduce hostile inbound attachments to which organizations are susceptible. This assessment includes 2 Email

gateways addresses and Customer may purchase additional email gateways at the then current rate.

- **Firewall Assessment**: Verizon will review select Customer firewall configurations (as provided by Customer) remotely for the presence of strong firewall configurations and/or necessary boundary protections that can detect, prevent, and correct the flow of data transferring networks, leveraging Level 1 internal risk vectors data. The results from the Firewall assessment will be used to calculate a portion of the Risk score and will be detailed in the quarterly Level 3 - Culture and Process View report. Verizon will report Customer's Firewall Assessment Score, Trend and Recommendations to reduce redundant rules, unexpected rules, and outdated rules. This assessment includes 3 firewall and Customer may purchase additional firewalls at the then current rate.
- **Endpoint System Assessment**: Verizon will analyze Customer provided endpoint devices remotely, assessing the security baseline for the presence of improper anti-virus, screen saver passwords, default configurations, industry best practice build standards, and secure configurations, leveraging Level 2 internal risk vectors data. The results from the Endpoint System assessment will be used to calculate a portion of the Risk score and will be detailed in the quarterly Level 3 - Culture and Process View report. Verizon will report Customer's End-Point System Assessment Score, Trend and Recommendations to help ensure that endpoint configurations align with the Customer's baseline. This assessment includes 500 IP addresses from the Level 2 – Inside-Out endpoint nodes and Customer may purchase additional IP addresses at the then current rate.
- **Phishing Assessment**: Verizon will conduct e-mail campaigns that evaluate employee knowledge, and organizational areas of susceptibility. The phishing assessment will offer a scenario-based template that gauges employees' behavior and their understanding of cyber security for Verizon to provide metrics on security awareness and behavior patterns, as well as reinforce effectiveness of training programs. The results from the Phishing assessment will be used to calculate a portion of the Risk score and will be detailed in the quarterly Level 3 - Culture and Process View report. Verizon will report Customer's Phishing Assessment Score, Trend and Recommendations to help reduce employee susceptibility and increase training program effectiveness. This assessment includes 600 email addresses and Customer may purchase additional email addresses at the then current rate.
- **Wireless Assessment**: Verizon will evaluate the effectiveness and security of Customers wireless network implementation. The onsite survey reviews corporate wireless policy, procedures, and network architectures. A wireless analyzer is used to detect wireless devices, and their configurations are analyzed to provide key reporting information, leveraging Level 2 internal risk vectors data. The assessment measures the risk of unauthorized or rogue wireless devices and indicate how well the wireless security defenses are deployed. The wireless assessment will identify Wireless attributable networks, Ad-hoc wireless networks, Wireless printers, Guest wireless networks, Wireless infrastructure vulnerabilities, and Bluetooth technologies. The results from the Wireless assessment will be used to calculate a portion of the Risk score and will be detailed in the quarterly Level 3 - Culture and Process View report. Verizon will report Customer's Wireless Assessment Score, Trend and Recommendations to help reduce wireless and Bluetooth vulnerabilities. This assessment includes 1 floor of 1 building and Customer may purchase additional floors/buildings at the then current rate.
- **Physical Inspection Assessment**: Verizon validates physical controls that focus on the security posture of the physical environment surrounding the critical network infrastructure. The activity is conducted by the Verizon Cyber Security analyst via onsite inspections and demonstrations on a semi-annual basis in the contract year. The Verizon analyst will conduct—but is not limited to—the following activities when inspecting the facilities: Review door security: biometric security, key card, access control, etc.; Review policies for physical security; Review convergence of physical security and information security; Review security awareness training related to physical security; Review Incident response policies for physical security events; and, Review business continuity and disaster recovery processes. The results from the Physical Inspection assessment will be used to calculate a portion of the Risk score and will be detailed

in the semi-annually Level 3 - Culture and Process View report. Verizon will report Customer's Physical Inspection Assessment Score based on an evaluation of employee knowledge and organizational areas of susceptibility. This assessment includes 1 building within a facility and Customer may purchase additional buildings at the then current rate.

- **Policy, Process, and Procedure Assessment**: Verizon evaluates Customer's development and management of corporate information cybersecurity policies that align to risk-reducing controls. The results from the Policy, Process and Procedure assessment will be used to calculate a portion of the Risk score and will be detailed in the semi-annual Level 3 - Culture and Process View report. Verizon will report Customer's Policy, Process, and Procedure Assessment Score, Trend and Recommendations to help reduce risk through better policies, processes, and procedures.

1.3.3.3 **Executive Culture and Process Assessment Report.Assessment**. Verizon will provide Customer an Executive Culture and Process Assessment Report of the Culture and Process Assessment containing the following:

- Executive Culture and Process Assessment Score –(to understand the individual scores across the 12 risk assessments.
-); Executive Culture and Process Assessment Trend –(to trend an organization's risk, from the perspective of multiple reporting periods and as identified in the Verizon DBIR, and identify an organization's ongoing Culture and Process posture.
-); and, Executive Culture and Process Assessment Recommendations –(a prioritized set of recommendations to reduce Culture and Process risk based on items identified in the 12 risk assessments.).

1.5.3.3.4 **Professional Services**. Verizon Risk Report Level 3 includes up to 100 hours per year of remote advisory and consultative professional services that Customers may use to assist with implementation of the recommendations provided in the Customer's Levels 1, 2 and 3 reports. The 100 professional services hours are to be used during the Service Commitment and any unused hours are not subject to carry over for renewal terms. The purchase of recommended products and/or services must be contracted via a separate agreement with their respective suppliers.

1.46 Verizon Risk Report Deliverables

1.46.1 **Verizon Recommendations.Prioritization.** Verizon Risk Report provides Customer with 5 recommendationsprioritized risk vectors based on the risk vectordata gathered during assessments, correlated with the DBIR industry insights, and Recorded Future insights from Customer's internalcustomer-provided information.

1.46.2 **Verizon Security Posture Score.** Verizon Risk Report provides a score from 0 (lowest) to 1,000 (highest) of Customer's comprehensive security posture based on: all provided risk vector assessments, combined with the DBIR Industry prioritization, input from Recorded Future brand and credential information, and Recorded Future cross validation. In addition, a Security Posture Score is provided for each Level purchased: Outside-In View; Inside-Out View; and Culture and Process Viewsecurity posture for each Level purchased.

1.46.3 **Verizon Confidence Level.** The Verizon Risk Report service is designed to provide Customers with a 360 degree view of their risk posture when all three levels (Verizon Risk Report Level 1, Level 2 and Level 3) are deployed. To help Customers understand their risk posture based on the data reviewed and analyzed, and the data that has not been reviewed and analyzed, the Verizon Risk Report provides a confidence level for the Security Posture Score, that is rated from 1 (low) to 100 shown on a scale of low to (high,), which represents the confidence of the Security Posture Score given the data that has been reviewed and analyzed at each Level purchased: Outside-In View; Inside-Out View; and Culture and Process View.. Each Level of Verizon Risk Report analyzes a

particular aspect of Customer's security posture and the three levels combine to provide a more comprehensive view of Customer's security posture.

1.46.4 **Verizon Threat Level Score**. Verizon Risk Report provides a score1 (lowest) to 5 (highest) of Customer's comprehensive threat level based on: all provided risk vector assessments coupled with Recorded Future company specific brand and credential information, Recorded Future insights based on internal information, and DBIR industry information.

1.46.5 **Combined External and Internal Security Posture Report**. Verizon Risk Report maps each risk vector to one or more category within the selected security framework and provides a category grade, ranging from A (highest) to F (lowest), within each security framework. Customer may select the format of the risk report to align with one of the following security frameworks: (certain frameworks may require additional payment for the framework provider):

- DBIR Incident Classification Patterns;
- NIST Framework for Improving Critical Infrastructure Cybersecurity v1.0 (Cybersecurity Framework);
- NIST Framework for Improving Critical Infrastructure Cybersecurity v1.1 (Cybersecurity Framework);
- NISTIR 8183 Cybersecurity Framework Manufacturing Profile;
- NIST 800-53 Rev 4 Security and Privacy Controls for Information Systems and Organizations;
- NIST 800-53 Rev 5 Security and Privacy Controls for Information Systems and Organizations;
- ISO/IEC 27001:2013 Information Security Management Systems;
- ISO 27799 Protected Health Information Security Management;
- ISO/IEC 27018 Public Clouds Privacy Framework;
- Payment Card Industry (PCI) Data Security Standard Version 3.2;
- FFIEC Cybersecurity Maturity Model updated October 2017.

1.46.6 **Report Updates**. Verizon Risk Report provides, as applicable based on assessment provided and Customer requirements, daily updates of the external and internal risk vectors and Recorded Future external and internal validation insights., as applicable. Verizon Risk Report Level 3 — Culture and Process View also provides quarterly and/or monthly updates to the culture and process risk vectors which updates the comprehensive security posture and threat level. Certain assessments are only done on a semi-annual basis as denoted within each assessment description.

1.5 **Excluded Services**. Any BitSight services, such as IP Address modification required to be addressed with BitSight to correct the BitSight rating, must be handled directly between the Customer and BitSight under a separate agreement.

1.6.7 **Verizon Disclaimer of Warranties**. In addition to the warranties and disclaimers in the Agreement, Verizon does not warrant that the Verizon Risk Report and Deliverables guarantee protection of Customer's computer or network systems against cybersecurity threats. Verizon does not warrant the accuracy of third party information provided to Customer. Customer acknowledges that no tool or system can provide a complete or holistic view of the customer's environment or security posture. The Verizon Risk Report provides a snapshot in time based on available data of the Customer's security posture using the methodology and scanning described, but does not provide a guarantee against cybersecurity threats.

2. SUPPLEMENTAL TERMS

2.1 **Data Ingestion.** Where applicable, NetFlow records will be ingested either from Verizon's IP backbone or from a Connection Kit located on Customer premises.

2.2 **Security Operations Center Support.** Where applicable, SOC support for the Service will be provided remotely from Verizon SOC locations in the United States, Europe and Asia on a 24x7x365 basis.

verizon

2.3 Customer Responsibilities

2.3.1 **Deployment Kit**. Where applicable, Customer must complete a Verizon deployment kit and provide such deployment kit to Verizon within 15 Business Days of the kick-off meeting or Verizon may terminate Customer's Service Order. Verizon may charge Customer for any expenses incurred by Verizon (including labor fees) through the date of termination.

2.3.2 **Maintenance Contracts.** Where required, Customer will (a) at its own expense, procure and maintain with each applicable vendor adequate maintenance contracts and all licenses necessary for the Data Sources to enable Verizon to properly perform Service; (b) comply with Service prerequisites and operational procedures as set forth in the applicable terms; and (c) promptly inform Verizon of any changes in Customer Environment and any changes to the nomination and/or authorization level of the Authorized Contacts responsible to oversee, monitor or evaluate the provision of Service.

2.3.3 **Interoperability.** Where applicable, Customer acknowledges that modifications or changes to the Data Sources (such as future releases to the Data Source's operating software) or to the Customer Environment may cause interoperability problems, inability to transmit data to Verizon, or malfunctions in a Data Source and/or the Customer Environment. Customer will give Verizon written notice (notice via email is acceptable) of any modifications or changes within 5 Business Days after making any such changes. Customer acknowledges that it is Customer's responsibility to maintain, at its sole cost and expense, the Customer Environment to ensure that the Customer Environment is interoperable with each Data Source.

2.3.4 **Service Equipment.** Where applicable, Verizon may require certain collection equipment to collect NetFlow from Data Sources and to forward such NetFlow records to the SMC (e.g., Connection Kits). If Verizon determines that such collection equipment is needed on Customer's Site, Customer must provide the necessary equipment subject to Verizon's specifications, either: (a) through direct procurement from equipment provider, or (b) through Verizon as a separate CPE procurement. Verizon will configure and access such equipment remotely.

2.3.5 **User Interface.** In connection with the provision of Service, Verizon may provide Customer with one or more user Logins to access a User Interface. Customer will at all times keep its Login strictly confidential and will take all reasonable precautions to prevent unauthorized use, misuse or compromise of its Login. Customer agrees to notify Verizon promptly upon learning of any actual or threatened unauthorized use, misuse, or compromise of its Login. Verizon is entitled to rely on Customer's Login as conclusive evidence of identity and authority. Customer will be liable for all activities and charges incurred through the use of Customer's Login, and will indemnify, defend and hold Verizon Indemnitees harmless from all liabilities, losses, damages, costs and expenses (including, without limitation, reasonable attorneys' fees and costs) incurred by Verizon to the extent resulting from the use and/or compromise of Customer's Login, unless the unauthorized use, misuse or compromise of Customer's Login is solely attributable to Verizon's gross negligence or willful misconduct.

2.3.6 **Installation Sites and Equipment.** For premise based ingestion, Customer will prepare any installation site in accordance with Verizon's instructions to ensure that any equipment that interfaces with Customer's computer system is properly configured as required for the provision of Service and operates in accordance with the manufacturer's specifications. All Customer premise based Data Sources must have a routable network path to and be compatible with the Connection Kit. Customer will install and maintain software agents required for the provision of Service to Data Sources on Customer network, at its cost. If Customer fails to make any preparations required herein and this failure causes Verizon to incur costs during the implementation or provision of Service, then Customer agrees to reimburse Verizon promptly for these costs.

verizon

2.3.7 **Additional Customer Obligations.** Customer understands that, in addition to the other Customer obligations described in this Service Attachment, Customer must comply with the following obligations.

- Ensure that Customer contacts are available for Verizon, for the kick-off call and at other times as required throughout the term of the Service Order.
- Responsible to cause any remedial actions or responses to be taken based on information Verizon provides to Customer about its interactions with CIPs or domains disclosed to Customer.
- Customer understands that service interruption may occur if Customer initiates network routing changes to the IP addresses listed on the CIP and that Customer is responsible for any such service interruption.
- Customer is responsible for actual travel and expense costs per quarterly (or optional monthly) assessment, unless the Customer has purchased pre-paid travel and expense costs for the assessment work and/or on-site summary report review.

2.3.8 **Consent.** Customer consents to Verizon's scanning and monitoring of Customer IP (CIP) and associated network components in the performance of the Verizon Risk Report service, the collection, use, processing, analysis and disclosure to Customer Authorized Contact of Customer's Internet traffic data, and the use of threat intelligence pertaining to CIP in an aggregated and anonymized form in connection with Verizon's portfolio of security servicesswith Verizon's portfolio of security services. Customer represents and warrants that: (i) the Customer provided list of CIP addresses contains only IP addresses assigned or allocated for the exclusive use of Customer and/or Customer Affiliates over which Customer has control; and, (ii) Customer has all legally required consents/permissions from CIP users for Verizon's performance of the Service.

2.3.9 **Feedback.**2.2 **Intellectual Property.** The intellectual property contained in Verizon Risk Report service, including Third Party Information, are protected by copyright, trade secret law, and other intellectual property law, and by international treaty provisions. All rights not expressly granted in this agreement are reserved by Verizon and its Third Party licensors and suppliers. All copyrights, patents, trade secrets, trademarks, service marks, trade names, moral rights, and other intellectual property and proprietary rights in the Verizon Risk Report and Third Party software and services will remain the sole and exclusive property of Verizon and the relevant Third Party licensors and suppliers. Customer may provide suggestions, comments, or other feedback (collectively, "Feedback") to Verizon or the Third Party. Such Feedback is voluntary and neither Verizon nor the Third Party is required to hold it in confidence. Verizon and Third Party may use Feedback for any purpose without obligation of any kind to Customer. To the extent a license is required under intellectual property rights to make use of the Feedback, Customer hereby grants Verizon and the Third Party, as applicable, an irrevocable, non-exclusive, perpetual, royalty-free license to use the Customer Feedback., and are deemed Confidential Information. All rights not expressly granted in this agreement are reserved, respectively, by Verizon and its Third Party licensors.

2.4 **Warranties**

2.4.1 **Verizon's Disclaimer of Warranties.** Customer acknowledges that impenetrable security cannot be attained in real-world environments and that Verizon does not guarantee protection against breaches of security, or the finding or successful prosecution of individuals obtaining unauthorized access. Verizon does not warrant the accuracy of information provided to Customer hereunder. THE WARRANTIES AND REMEDIES SET FORTH IN THIS SERVICE ATTACHMENT ARE VERIZON'S EXCLUSIVE WARRANTIES AND CUSTOMER'S SOLE REMEDIES FOR BREACH OF WARRANTY, IF ANY, BY VERIZON.

2.4.2 **Customer Warranty.** Customer represents and warrants that:

a) the deliverables, documentation, and other information provided by Verizon in connection with Service will be used solely for purposes of protecting Customer from abusive, fraudulent, or unlawful use or access to its information, systems and applications including Verizon's public

Internet service and Customer will not market, sell, distribute, lease, license or use any such deliverables, documentation or information for any other purposes;

b) the list of Customer (CIP) addresses provided by Customer contains only IP addresses that have been assigned or allocated for the exclusive use of Customer and/or Affiliates of Customer over which Customer has control;

c) it has obtained or will obtain all legally required consents and permissions from users of CIP for Verizon's performance of Service, including without limitation the collection, use, processing, analyses and disclosure to Customer of Customer's Internet traffic data and the use of threat intelligence pertaining to CIP in an aggregated and anonymized form in connection with Verizon's portfolio of security services;

d) Customer will maintain up-to-date list of CIP addresses by revising and executing the CIP Schedule as applicable and provide the revised and executed CIP Schedule to Verizon; and

e) Customer will comply with all the Confidentiality obligations.

Customer shall indemnify, defend or settle and hold Verizon Indemnitees, and Verizon's associates, officers, directors, employees and partners harmless from and against all losses, damages, costs and expenses (including allocable costs of in-house counsel and other legal fees) associated with any claims, suits, judgments, settlements, investigations, fines, consent decrees, requests for information, or other dispute resolution, enforcement, regulatory or legal proceedings or actions of any kind, suffered or incurred directly or indirectly by Verizon Indemnitees from or arising out of Customer's breach of any of the representations and warranties above or based on, arising out of or relating to Customer's use or interpretation of third party information and Net Intel Information provided by Verizon.

2.4.3 **Third Party Warranties.** For any third party products and/or services incorporated as part of the Verizon Risk Report Service, Customer will receive only the warranties offered by such third party either directly to Customer or to the extent Verizon may pass through such warranties to Customer.

2.5. **Third Party Information.** Customer may request that Verizon perform Service related to a third party's information, including Vendor Monitoring. Customer hereby represents and warrants to Verizon that if it makes such a request, Customer will have obtained such third party's authorization to engage Verizon to perform Service to access such third party's information prior to Verizon's commencement of services. Customer agrees to indemnify, defend and hold Verizon Indemnitees harmless from any and all loss, damages, liabilities, costs and expenses (including legal expenses and the expenses of other professionals) resulting directly or indirectly from Verizon's alleged lack of authority to access the third party's information in connection with the Service.

2.6 **Term and Termination**

2.6.1 **Service Commitment**. The Service Commitment is for a 1 year term, 2 year term or, 3 year term. At the end of a Service Commitment, the Agreement will automatically renew for subsequent 1 year terms at the then current 1 year term price, unless a Party provides the other Party with notice of its intent not to auto-renew the Agreement at least 90 days prior to the expiration of the Service Commitment term. Customer may opt to purchase a different Service Commitment term with advance notice 90 days prior to the expiration of a Service Commitment or auto renewed term.

2.6.2 **Order Cancellation**. If Customer requests cancellation of Service, or Verizon cancels Service as a result of Customer's failure to provide the necessary information or reasonable assistance required by Verizon to provision such Service, Customer will pay any set-up fees and other amounts accrued for such Service through the date of such termination, plus an amount equal to any applicable annual third party license fee, which Customer acknowledges are liquidated damages reflecting a reasonable

measurable of actual damages and not a penalty. Customer will pay the invoice for such charges in accordance with the terms of the Agreement.

2.6.3 **Service Termination.** Customer accepts and agrees that, in the event (i) Customer terminates any order for convenience or (ii) Verizon terminates any order for Cause prior to the end of the order term, then Customer will pay Verizon all unpaid fees payable under this Service Attachment and the applicable order for the remainder of such order term, including Early Termination Charges and any applicable annual third party license fee, which Customer acknowledges are liquidated damages reflecting a reasonable measure of actual damages and not a penalty. Customer will pay the invoice for such charges in accordance with the terms of the Agreement.

2.7 **Third Party Products or Services.** Customer agrees that Verizon will not be liable for any damages caused by hardware, software, or other products or services furnished by parties other than Verizon, its agents, subcontractors, or any damages caused by the products and/or services delivered by or on behalf of Verizon which have been modified, serviced, or otherwise attended to by parties other than Verizon or without Verizon's prior written and express consent. Customer acknowledges that third party products and services are a component of Verizon Risk Report, including BitSight, Recorded Future, Tanium, and Cylance. Customer acknowledges that Verizon will not be liable for any damages resulting, directly or indirectly, from any act or failure to act by Customer or any third party (including, without limitation, the non-performance, defaults, omissions or negligence of any third party that provides telecommunications services in the country or countries in which Customer's premises or systems are situated and other countries from, across, to or in which Service is provided by or on behalf of Verizon). Customer will be subject to the terms of use of the third party products and/or services that are a component of Verizon Risk Report, and Customer may be required to agree to third party end user license terms.

2.7.12.4 **Third Party End User Terms**. For Verizon Risk Report Level 1, Customer must accept BitSight Supplier Terms, as same may be modified from time to time by BitSight, located at https://service.bitsighttech.com/accounts/tos/e33b9043-bcab-4550-8891-278a77b397ca. For Verizon Risk Report Level 2, Customer must accept Tanium and Cylance end user terms, as same may be modified from time to time by the respective suppliers, as follows: (i) as to Tanium, the user terms located at: https://tanium.com/tanium-software-terms/; and, (ii) as to Cylance, the user terms located at: https://pages.cylance.com/mssp-eula-agreement.html.

2.8 **Verizon Materials.** If in connection with the provision of Service Verizon installs or provides any hardware or software (Verizon Materials), then Customer will use the Verizon Materials for internal purposes only as further defined in this Service Attachment. Customer will not distribute, reproduce, or sublicense the Verizon Materials. Customer will not reverse engineer, decompile, or disassemble or otherwise attempt to discover source code of the Verizon Materials. Verizon has the right to revoke the use of the Verizon Materials at any time. In such event, Customer will, at its sole cost and expense, promptly return the Verizon Materials to Verizon. Customer's right to use the Verizon Materials automatically terminates upon termination or cancellation of the Service Order or upon completion of the portion of Service for which the Verizon Materials are provided.

2.9 **Confidential Information.** Customer acknowledges that the following information constitutes Confidential Information hereunder: (a) the methods, systems, data and materials used or provided by Verizon in connection with the provision of Service and (b) the results of Verizon's assessment of Customer and all reports issued by Verizon in connection with such results including, without limitation, security analyses and insight ("Net Intel Information"). Customer will disclose Net Intel Information only to Customer employees with a need to know for the purposes set forth in this Service Attachment and who are bound to confidentiality obligations at least as restrictive as those set forth in the Agreement and this Service Attachment. In no event may Customer use lesser efforts to protect Net Intel Information from use or disclosure not permitted under the Agreement than it uses to protect its own highly-sensitive confidential information, or less than reasonable efforts. The term Confidential Information will not include information that is comprised of statistical information, or other aggregated

information regarding security vulnerabilities, security configurations and the like insofar as such information does not identify Customer or Customer's computer network or computer systems.

2.5 **Third Party Warranties.** For any third party products and/or services incorporated as part of the Verizon Risk Report Service, Customer will receive only the warranties offered by such third party either directly to Customer or to the extent Verizon may pass through such warranties to Customer.

2.6 **Service Commitment**. The Service Commitment is for a 1 year term, 2 year term or, 3 year term. At the end of a Service Commitment, the Agreement will automatically renew for subsequent 1 year terms at the then current 1 year term price, unless a Party provides the other Party with notice of its intent not to auto-renew the Agreement, or to purchase a different Service Commitment term, at least 90 days prior to the expiration of the Service Commitment term.

2.7 **Service Termination.** If the Service is terminated during a Service Commitment term, Customer will pay Early Termination Charges and any applicable third party license fee, in accordance with the payment terms of the Agreement.

3. **FINANCIAL TERMS.** Customer will pay the non-recurring charges (NRCs) and monthly recurring charges (MRCs) per Verizon Risk Report Level (or per other specified item) as set forth in the applicable Agreement. Unless expressly indicated otherwise, all NRCs will be invoiced upon ~~Order Confirmation~~Commencement Date and the initial MRCs will be invoiced upon Service Activation.

~~4. **DEFINITIONS.** The following definitions apply to Verizon Risk Report, in addition to those identified in~~ Date. Customer is responsible for actual travel and expense costs per quarterly (or optional monthly) on-site assessment and/or summary report review, unless the ~~Master Terms of your Agreement.~~

~~Term~~	~~Definition~~
~~**Authorized Contacts**~~	~~Customer personnel authorized by Customer to access the Security Dashboard and to interact with Verizon for the Service.~~
~~**Connection Kit**~~	~~Equipment installed on the Customer's premises used to set up secured monitoring and/or management connections between the Data Sources and one or more Security Management Centers.~~
~~**Customer Environment**~~	~~The network and/or information technology infrastructure in which Customer Data Sources reside.~~
~~**Data**~~	~~Machine-generated information that can be digitally transmitted and processed.~~
~~**Data Source**~~	~~Any source of NetFlow either coming from Verizon's global IP backbone or from Customer premise devices, for this service Customer edge routers facing the public internet.~~
~~**Login**~~	~~IDs, account numbers, personal identification numbers or codes, passwords, digital certificates or other means of authentication.~~
~~**NetFlow**~~	~~Information from routing devices which represents header data including: source and destination IP Address, IP Protocol Type (e.g. TCP, UDP, ICMP, etc.), source and destination Port, TCP Flags (e.g. SYN, ACK, FIN, etc.), number of packets in the flow, number of bytes in the flow, start and end time of the flow.~~
~~**Order Confirmation Date**~~	~~Verizon will confirm Customer's order via email and the date of this email is the Order Confirmation Date. The Order Confirmation will confirm the Service service(s) requested.~~
~~**SOC (Security Operations Center)**~~	~~A data center where the Verizon security analysts work.~~
~~**User Interface**~~	~~A web-based portal, dashboard, or other electronic means to share information and reports with customers that pertains to Security Incidents that are identified and escalated to the customer.~~

~~**Verizon Indemnitees**~~	~~Verizon, its parents, subsidiaries and affiliates, and its and their respective directors, officers, members, partners, employees, agents, contractors, successors and assigns.~~

verizon

EXHIBIT A

Contract ID#_____

Customer IP Address Schedule ("CIP Schedule") to the Verizon Risk Report Service Attachment

_____ ("Customer")

Address:

By:_____
Name:_____
Title:_____
Date:_____

1. **Description.** Verizon Risk Report, as described in the service attachment, requires that Verizon perform services for Customer utilizing a list of Customer provided IP addresses (collectively, "CIP") as provided by Customer at the kick-off meeting referenced in the service attachment.

Location/Site	IP Addresses

Customer has purchased pre-paid travel and expense costs for on-site work.