verizon

Cyber Risk Monitoring +

1. GENERAL

1.1 **Service Definition.** Cyber Risk Monitoring 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. Cyber Risk Monitoring consists of three service levels: Level 1 – Outside-In view, Level 2 – Inside-Out view, and Level 3 – Culture and Process. The three levels can be stacked to provide 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 Cyber Risk Monitoring Level provides specific recommendations, based on the available data, to aid Customer in addressing vulnerabilities, prepare for potential threats, and improve its risk management position.

1.2 **Service Implementation**. Verizon will send automated communications to Customer's personnel authorized by Customer to access the Customer portal and to interact with Verizon for the Service (Authorized Contacts) to establish, access, administer, and utilize the Service. Verizon will assign a project manager to assist Customer in operationalizing the Service, including configuration and deployment. 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 Cyber Risk Monitoring portal.

1.3 **Cyber Risk Monitoring Level 1 – Outside-In View**~~.~~ . 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 **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 on 21 External Risk Vectors which includes four categories: Compromised Systems, Diligence, User Behavior and Others, such as publicly disclosed data breaches 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.

verizon

1.3.2 **External Threat Intelligence**. The external assessment also includes Recorded Future's deep web and dark web data that highlight potential threats and global trends, including company brand mentions and company credentials over the past two years.

1.3.3 **Verizon Data Breach Investigation Report (DBIR).** The external assessment also provides incident classification patterns based on the DBIR attack vectors, attack varieties, motives, industries, geographies, and customer size to prioritize the BitSight External Risk Vectors. DBIR Incident Classification Patterns include: Crimeware, Denial of Service, Physical Theft & Loss, Payment Card Skimmers, Insider Privilege Misuse, Cyber-Espionage, Point of Sale Intrusions, Web Application Attacks, Miscellaneous Errors, and Everything Else.

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

1.3.5 **Portfolio Management**. Customers may also purchase Cyber Risk Monitoring Level 1 for their related entities which includes BitSight's subsidiary and affiliate monitoring reports. Customer or Customer related entities may also purchase Cyber Risk Monitoring Level 2, Level 3, and optional features for such subsidiaries and affiliates.

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

1.4 **Cyber Risk Monitoring Level 2 – Inside-Out View**~~.~~. The internal risk score is an inside-out assessment which focuses on internal risk and hygiene vectors measured using both Customer provided endpoint technology, and/or Verizon provided endpoint technology, and are combined with Cyber Risk Monitoring Level 1 for a fuller view of Customer's cyber security posture. This internal security posture is analyzed through the receipt of customer provided endpoint data (using Cylance and/or CrowdStrike and/or Lookout API's) and/or the deployment of Verizon provided agents (using Cylance and/or Tanium) 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. With the implementation of Level 2, if a customer has already implemented these following non-endpoint products into their environment, they can choose to also feed data from their Palo Alto firewall appliances running SLR Probe and/or Cisco Umbrella/DNS Safeguard for DNS requests into the evaluation process for creating the internal risk score~~The internal risk score is an inside-out assessment which focuses on two groups of internal risk vectors: Infrastructure, measured using Tanium technology, and Endpoint Threat Management, measured using Cylance technology, and both are combined with Cyber Risk Monitoring 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~~.

1.4.1 ~~**Infrastructure Internal**~~**Endpoint Risk Vectors.** Cylance risk vectors identify endpoints running Backdoors, Bots, Downloaders, Droppers, Dual-Use Tools, Exploit Attempts, FakeAVs, Generic Malware, Infostealers, Parasites, Ransomware, Remnants, Rootkits, Trojans, Viruses, Worms, Cracking Software, Generic Dual-Use Detections, Keygens, Monitoring Tools, Password Crackers, Remote Access Tools, Endpoints with Adware, Corrupted PUPs, Games, Generic PUPs, Hacking Tools, Portable Applications, Scripting Tools, Toolbars and Other PUPs. CrowdStrike risk vectors identify endpoints with activity that aligns to the MITRE tactics of Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, Impact, Malware, Exploit, Post-Exploit and custom CrowdStrike tactics of Machine Learning, Custom Intelligence, Falcon Overwatch, Falcon

verizon

Intel – Enterprise, Falcon Intel – Mobile and Insecure Security Posture. Lookout risk vectors identify mobile endpoints running Adware, App Droppers, Backdoors, Bots, Chargeware, Click Fraud, Data Leaks, Developer Mode, Exploits, Malicious Content, Man-in-the-Middle Attacks, No Passcodes, Non-App Store Signers, Out-Of-Date OS's, Out-Of-Date Patch Levels, Phishing Content, Riskware, Rogue Wi-Fi, Root/Jailbreaks, Root Enablers, Spam, Spyware, Surveillanceware, Toll Fraud, Trojans, Unencrypted Devices, Unknown Sources, USB Debugging, Vulnerabilities and Worms. Tanium risk vectors include: Identify Malicious Applications, Systems in Poor Health, Identify Out-of-Date Passwords, Identify User Misbehavior - Screen Saver Passwords, Identify Windows SSL Certificates~~The Infrastructure group is analyzed using Tanium technology and its internal risk vectors, 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.

1.4.2 **Endpoint ~~Threat Management~~Hygiene Vectors**. Cylance hygiene vectors identify endpoints running Portable Applications and Remnants. Tanium hygiene vectors include: Application Risks, Uncommon Port Usage, Unusual Connections, Unusual Running Services, and Windows OS Risks. These hygiene vectors can change over time~~The Endpoint Threat Management group uses Cylance technology to assess internal risks posed by malware, potentially unwanted programs (PUPs), and dual use tools~~.

1.4.3 **Additional Non-endpoint Data Integrations.** Verizon continuously seeks additional data integrations to improve Cyber Risk Monitoring. The addition of Palo Alto integration includes an additional twenty-nine vectors evaluating firewall activity and policies. Cisco Umbrella and Verizon DNS Safeguard include five risk vectors evaluating domain name server (DNS) requests and policies. These risk vectors can change over time.

1.5 **Cyber Risk Monitoring Level 3 – Culture and Process View.** The Culture and Process score provides a 360 degree security risk assessment of Customer's overall culture and processes when combined with Cyber Risk Monitoring Level 1 and Level 2. Verizon will deploy automated tools and human intelligence to generate an assessment of 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 with recommendations for improvements to Customer's security posture.

1.5.1 **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.

1.5.2 **Executive Report of Culture and Process Assessment**. Verizon will provide Customer an Executive Report of the Culture and Process Assessment containing the 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 **Professional Services**. Cyber Risk Monitoring 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.

1.6 **Cyber Risk Monitoring Deliverables**

1.6.1 **Verizon Prioritization.** Cyber Risk Monitoring provides Customer with prioritized risk vectors based on the data gathered during assessments, correlated with the DBIR industry insights and customer-provided information.

1.6.2 **Verizon Security Posture Score.** Cyber Risk Monitoring provides a score from 0 (lowest) to 1,000 (highest) of Customer's security posture for each Level purchased.

1.6.3 **Verizon Confidence Level.** Cyber Risk Monitoring provides a confidence level for the Security Posture Score, rated from 1 (low) to 100 (high), which represents the confidence of the Security Posture Score given the data that has been reviewed and analyzed at each Level purchased. Each Level of Cyber Risk Monitoring 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.

1.6.4 **Verizon Threat Level Score**. Cyber Risk Monitoring provides a score 1 (lowest) to 5 (highest) of Customer's comprehensive threat level.

1.6.5 **Combined External and Internal Security Posture Report**. Cyber Risk Monitoring 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;
- NIST Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (NIST SP 800-171);
- ~~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;
- American Institute of Certified Public Accountants System And Organizational Control 2 (AICPA SOC 2);
- Australian Cyber Security Center – Protect – Essential Eight;
- Center for Internet Security Critical Security Controls v7 (CIS v7);

- Federal Reserve Bank of India Cybersecurity Maturity Model;
- Health Insurance Portability and Accountability (HIPAA);
- Massachusetts Standards for the Protection of Personal Information (201 CMR 17.00);
- NERC/FERC Critical Infrastructure Protection Cyber Security Reliability Standards (NERC/FERC CIP);
- New York State Department of Financial Services Cybersecurity Requirements for Financial Services Companies (23 NYDFS 500).

1.6.6 **Report Updates**. Cyber Risk Monitoring provides daily updates of the external and internal risk vectors and Recorded Future external and internal validation insights, as applicable. Cyber Risk Monitoring Level 3 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.

1.6.7 **Verizon Disclaimer of Warranties**. In addition to the warranties and disclaimers in the Agreement, Verizon does not warrant that Cyber Risk Monitoring 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. Cyber Risk Monitoring 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 **Consent.** Customer consents to Verizon's scanning and monitoring of Customer IP (CIP) and associated network components, 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 with 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.

2.2 **Intellectual Property.** The intellectual property contained in Cyber Risk Monitoring service, including Third Party Information, are protected by copyright, trade secret law, and other intellectual property law, and by international treaty provisions, and are deemed Confidential Information. All rights not expressly granted in this agreement are reserved, respectively, by Verizon and its Third Party licensors.

~~2.3 **Third Party Information.** Customer may request that Verizon perform Service related to a third party's information, including Vendor Risk Dashboard. 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.~~

2.43 **Third Party End User Terms**. For Cyber Risk Monitoring 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 Cyber Risk Monitoring 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://www.tanium.com/software-termshttps://tanium.com/tanium-software-terms/; and, (ii) as to Cylance, the user terms located at: https://pages.cylance.com/mssp-eula-agreement.htmlhttps://pages.cylance.com/mssp-eula-agreement.htmlhttps://pages.cylance.com/mssp-eula-agreement.ht.https://pages.cylance.com/mssp-eula-agreement.html.

2.54 **Third Party Warranties.** For any third party products and/or services incorporated as part of the Cyber Risk Monitoring 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.

2.65 **Service Commitment**. The Service Commitment is for a one year term, two year term or, three year term. At the end of a Service Commitment, the Agreement will automatically renew for subsequent one year terms at the then current one 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.

2.76 **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 Cyber Risk Monitoring Level (or per other specified item) as set forth in the applicable Agreement. Unless expressly indicated otherwise, all NRCs will be invoiced upon Commencement Date and the initial MRCs will be invoiced upon Service Activation 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 Customer has purchased pre-paid travel and expense costs for on-site work.