Cyber Risk Monitoring.

Fact sheet

Measure your risk and security posture with comprehensive visibility and daily updates that address gaps and maximize security ROI through actionable data.

Level 1

Level 1 of Cyber Risk Monitoring (formerly known as the Verizon Risk Report) evaluates your organization from an external viewpoint. Using BitSight, data is gathered from 200+ public data sources on the internet. External risk vectors are evaluated using BitSight, along with information from Recorded Future (RF) and the Verizon Data Breach Investigations Report. These vectors are categorized by compromised systems, diligence issues, user behavior, and public disclosures. A security posture score is established and a fully automated daily report is available through Verizon's Unified Security Portal.

Level 1 external risk vectors are listed to the right.

- Botnet infections
- Spam propagation
- Malware
- Unsolicited communications
- Potentially exploited systems
- Open ports
- TLS/SSL certificates/ configuration
- Web application headers
- Sender Policy Framework (SPF)
- Domain Keys Identified Mail (DKIM)
- Patching cadence
- Server, desktop, and mobile software
- Insecure systems
- DNSSEC records
- File sharing
- Exposed credentials
- Public data breaches
- Dark web threat intelligence

Level 2

Level 2 builds on Level 1 and further refines your security posture score by including data collected from inside the organization. This internal evaluation assesses your posture and uncovers risks by searching for malware, unwanted programs and dual usage tools within your endpoint, infrastructure and application firewall traffic.

One or more endpoint data sources is required for the purchase of Level 2 and the options include Cylance, CrowdStrike, Lookout and Tanium. In addition to endpoint data sources, we offer two non-endpoint data integration options including DNS Safeguard/Cisco Umbrella and Palo Alto firewalls running SLR Probe. The Level 2 risk vectors are all provided in addition to the Level 1 data sources and are categorized by malware, unwanted programs, dual use tools, and infrastructure issues.

Examples of Level 2 risk vectors are listed to the right.

- Endpoints with Backdoors, Bots, Downloaders, Droppers, Dual-Use Tools, Exploit Attempts, FakeAVs, Generic Malware, Infostealers, Parasites, Ransomware, Rootkits, Trojans, Viruses, Works, Cracking Software, Keygens, Monitoring Tools, Password Crackers, Remote Access Tools, Adware, Corrupted/Generic Potentially Unwanted Programs, Games, Hacking Tools, Scripting Tools and Toolbars
- Risks from actions related to MITRE Attack Tactics such as Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discover, Lateral Movement, Collection, Command and Control, Exfiltration, Impact, Malware, Exploit and Post-Exploit
- Risks from actions related to custom attack tactics such as Machine Learning, Custom Intelligence, Falcon Overwatch, Falcon Intel for Enterprise and Mobile endpoints and Insecure Security Posture
- Mobile devices with Adware, Ad Droppers, Backdoors, Bots, Chargeware, Click Fraud, Data Leaks, Developer Mode Enabled, Exploits, Malicious Content, Man-in-the-Middle Attacks, Mission Passcodes, Non-App Store Signers, Out-of-date Operating Systems/ Patch Levels, Phishing Content, Riskware, Rogue Wifi, Rooted/Jailbroken, Root Enablers, Span, Spyware, Surveillanceware, Toll Fraud, Trojans, Unencrypted, Unknown Sources, USB Debugging Enabled, Vulnerabilities and Worms
- Risks from Malicious Applications, User Misbehavior, Expired SSL Certificates and Systems in Poor Health

verizon

Level 3

True visibility comes when external and internal risk evaluations are combined with recurring assessment activities designed to identify risks threatening your organization, assets and brand reputation. This level enables a 360-degree assessment of your security posture by integrating a review of behavior, culture, process and policy into the Level 1 and Level 2 data. We provide a custom-tailored audit of your security posture, including expert assessments, diagnostic methods leveraging best-of-breed solutions, and 100 hours of professional services to help implement posture improvements.

Level 3 risk vectors include those from Levels 1 and 2, along with culture and process risk vectors identified during the audit. Examples are listed to the right.

- External vulnerability
- IP reputation
- NetFlow
- Web applications
- Internal vulnerability
- E-mail filter
- Firewall
- Endpoint systems
- Phishing
- Physical inspection
- Policy, process, and procedure
- Wireless

Vendor Risk Dashboard.

Through the proliferation of outsourcing and cloud-based technologies, the digital enterprise today touches numerous third parties. Each brings a level of risk to your organization; after all, your security is only as good as its weakest link. A breach at one of your vendors may expose critical proprietary or customer data that could impact your brand or reputation, and put your business at risk.

The Vendor Risk Dashboard allows you to monitor the security posture of the vendors and partners you do business with. The dashboard provides you with a comprehensive view of your security risk posture through customized, actionable intelligence and risk ratings on your subscribed third parties.

With timely notification, you can proactively identify potential issues, better allocate resources, and work with your supply chain against the most dangerous threats. The reports can also be effective in evaluating mergers and acquisitions, offering a better understanding of risk exposure and potential mitigation strategies.

In the dashboard, users can start with a threat level and security rating tailored to the industry of the vendor selected. You can also create customized groups of vendors, see prioritized threat vectors, and view multiple graphs showing the aggregated scores of all vendors and vendor groups.

Portfolio Management.

Portfolio Management is an add-on service. You can view an executive summary of your related legal entities (i.e. subsidiaries) or drill down to more detailed views. You can also easily switch between views of related entities without logging out, allowing for more rapid scanning of the portfolio. The Portfolio Dashboard allows you to review various charts reflecting the overall portfolio security posture and threat level scoring, while the Manage Portfolio view allows you to view a hierarchal representation list of your subsidiaries.

Learn more.

Cyber Risk Monitoring will improve the way you develop and measure your security strategy. Learn more at: enterprise.verizon.com/products/security/cyber_risk_monitoring

verizon