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: Outside-in view - see the forest for the trees.

The outside-in view evaluates your organization from an external viewpoint. Using BitSight, data is gathered from public sources on the internet. External risk vectors are evaluated to provide a security posture score. A fully automated daily report is available through Verizon's Unified Security Portal.

- Based on 200+ public data sources on the internet
- Automated, daily report
- Data sources include BitSight, Recorded Future, and Verizon Data Breach Investigations Report (DBIR)

Risk vectors

Includes external risk vectors 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.

- 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: Inside-out view - an MRI for your enterprise.

Level 2 of Cyber Risk Monitoring further refines your security posture score through an internal evaluation that searches for malware, unwanted programs and dual usage tools within your endpoints and infrastructure.

- Builds on Level 1 and includes data collected from inside the organization
- Evaluate endpoints and infrastructure to assess posture and uncover risks
- Data sources include Tanium, Cylance on top of all Level 1 sources

Risk vectors

Includes the external risk vectors from Level 1 and adds internal risk vectors sourced from Tanium and Cylance. These additional vectors are categorized by malware, unwanted programs, dual use tools, and infrastructure issues.

- Unexpected running services
- End of life software in use
- Vulnerable firmware versions
- Systems in poor health
- Endpoint visible wireless networks
- Dual homed devices
- Unusual connections
- Anomalies/misconfigured password & audit policies
- User misbehavior
- SSL certificate issues
- Network segmentation
- Unapproved established connections
- Application risks
- Anomalies that could indicate compromise
- Endpoints with generic malware, ransomware, trojans, fakeAVs, backdoors, viruses, downloaders, rootkits, infostealers, remnants, worms, exploit attempts, droppers, or bots
- Endpoints with generic potentially unwanted programs, adware, games, keygens, toolbars, scripting tools, remote access tools, corrupted PUPs, hacking tools, or portable applications
- Endpoints with dual use or remote access tools, password crackers, cracking software, monitoring tools

* Formerly known as the Verizon Risk Report

verizon✓

Level 3: 360° visibility - A culture and process view.

True visibility comes when external and internal risk evaluations are combined with an in-depth review of the security culture and processes within an organization. The culture and process assessments deploy automated tools coupled with human intelligence for a comprehensive view of security and risk posture.

- Adds the capstone to Level 1 and Level 2 data by taking behavior, culture, process and policy into consideration
- Includes 100 hours of professional services to help implement posture improvement
- Enables a 360-degree assessment of security posture

Risk vectors

Includes the external risk vectors from Level 1, the internal risk vectors from Level 2, and adds culture and process risk vectors sourced from a custom-tailored Verizon audit. These additional risk vectors include:

- 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✓