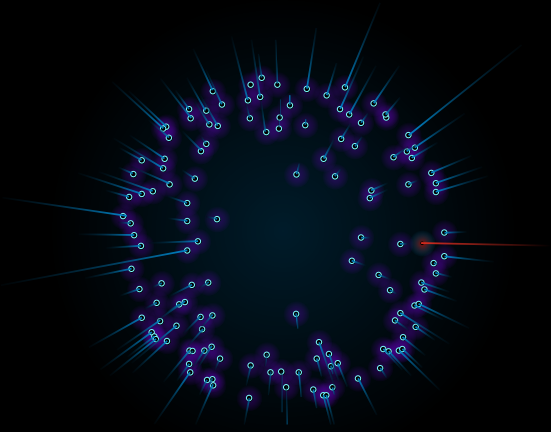
Verizon Risk Report

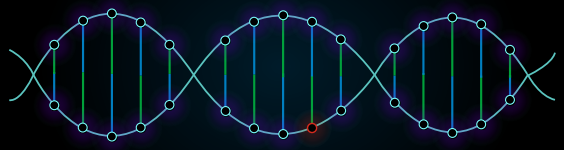
Measure your risk and security posture with comprehensive visibility and daily updates that address gaps and maximize security ROI through actionable data.



Level one: see the forest for the trees
Outside-in view

The outside-in view evaluates your organization from an external viewpoint. Powered by 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.

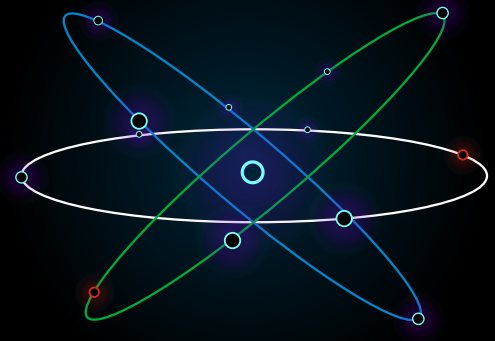
- Based on 200+ public data sources on the internet
- Automated, daily report
- Data sources include BitSight, Recorded Future, and Verizon Data Breach Investigations Report (DBIR)



Level two: an MRI for your enterprise
Inside-out view

Level two of the Verizon Risk Report further refines your security posture score through an internal evaluation that automatically searches for malware, unwanted programs and dual usage tools within your endpoints and infrastructure.

- Builds on level one 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 one sources



Level three: 360° visibility
Culture & 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 one and level two 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

verizon

Learn more at **VerizonEnterprise.com/products/security**

Threat vectors by level

Level 1

Outside-in view

Includes external risk vectors powered by BitSight. These vectors are categorized by compromised systems, diligence issues, user behavior, and public data breaches.

- 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
- Domain squatting
- File sharing
- Publicly disclosed credentials
- Public data breaches

Level 2

Inside-out view

Includes the external risk vectors from level one 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 tools, remote access tools, password crackers, cracking software, or monitoring tools

Level 3

Culture and Process view

Includes the external risk vectors from level one, the internal risk vectors from level two, and adds culture and process risk vectors sourced from a custom tailored Verizon audit. These additional threat vectors include:

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

verizon

Future availability of Level 3 is scheduled for 2019

Learn more at **VerizonEnterprise.com/products/security**