Quickly assess risks to prevent illicit access of confidential data.

Fact sheet

Espionage health check

verizon

The number of cyber-espionage attacks continues to rise. But this growing theft of valuable secrets and proprietary data doesn't affect government agencies and military contractors alone. Organizations across industries—from financial services to critical infrastructure—have all become common targets.

Through malicious e-mail attachments, embedded links and strategic web compromises, your systems can become infected and breached, and critical information can be stolen or damaged.

An Espionage Health Check includes testing for evidence of security breach on your networks. Recognize security breaches in progress, identify systems susceptible to criminal methods and persistent threats and mitigate intrusions and exploits. As we assess your potential vulnerabilities, we apply the intelligence we've gained from analyzing more than a decade of security events, including nearly 8,000+ confirmed breaches and more than 200,000 security incidents. Our experts can give you a clear view of the threats and areas of risk to your organization.

Tools to protect your organization from cybercrime

We take a multi-pronged engagement approach when performing the Espionage Health Check, by completing an on-site review and assessment of critical systems, as well as an analysis of Internet traffic patterns to detect communications with known bad actors and malicious traffic patterns. We assess cyberattack detection capabilities through multiple processes and tools for a broad view of potential risks.

It's ideal for obtaining a point-in-time evaluation of a possible breach and identifying potential risks, while providing recommendations for shoring up your defenses against cyber threats.

As part of the assessment, we:

- Produce forensic imaging of critical systems and network inspection, as well as disk and memory analysis.
- Examine and correlate active network connections, logs and data transfer flows involving critical systems to identify malicious activity and malware.
- Scan in-scope systems for correlation against our proprietary listing of indicators of compromise.
- Analyze key application and system files for evidence of suspicious or malicious files.

Using the results of our Espionage Health Check, you can better prepare for unanticipated cyber attacks, recognize areas of exposure and respond quickly to any current breaches. You'll receive a full management report that summarizes the results of our analysis and highlights any bad actors and questionable activity we detected. The report also provides recommendations of reinforcements, countermeasures and monitoring you can employ to help defend your organization from cyber-espionage.

90% of cyber-espionage breaches capture trade secrets or propietary information.[1]

Identify the most critical vulnerabilities you face—and get recommendations to reinforce your enterprise security.

Learn more:

To find out how an Espionage Health Check can help protect your organization, contact your account manager or visit:

verizonenterprise.com/products/security

1 Verizon 2016 *Data Breach Investigations Report*. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/