Remote Working Security Assessment

Solution brief

Know where your vulnerabilities are.

With the rapid growth in remote working, organizations may be increasingly exposing themselves to cyber threats.

Many companies have become increasingly dependent on virtual private networks (VPNs) in order to securely connect remote workers to the business network. Your VPN security may not be properly configured to handle a large increase in this virtual workforce.

What you need is a quick and lightweight way to help ensure your remote access to the network remains fully secure and properly configured.

Remote Working Security Assessment.

Verizon's Remote Working Security Assessment provides a comprehensive view into an enterprise's security posture relating to remote workers. This completely virtual analysis can be finished in as little as two weeks and requires no intrusive access into your systems as data collection is conducted from the cloud. The outcome is a clearer understanding of your security risks related to remote working and a prioritized set of recommendations for reducing the risk of compromise.

This assessment can be relevant to public and private institutions in both regulated and unregulated industries, and for companies of all sizes to help them understand how prepared they are to continue and expand their remote working capabilities. To gather the best information, systems are evaluated two different ways during the process: a remote access environmental assessment and a remote access VPN penetration test.

Remote access environmental assessment.

Verizon's methodology is designed to quickly evaluate and determine any policy, people, or process-related weaknesses in a company's remote working environment. It does so with minimal disruption to the day-to-day essential processes that keep operations running. As the standard for this assessment, the controls to be tested are:

- Policies
- Asset management
- Access control
- Remote access
- Logging and monitoring
- Configuration and patch management
- Encryption
- Identity and access management

During the initial phase of the environmental assessment, we work with you to identify the relevant documentation and individuals that are required to perform the assessment. We then review the provided documents and conduct interviews to clarify any security controls that are not fully documented.

During the data analysis, we assess your remote working program maturity, performance, and scope relative to your security requirements. We then develop compliance and maturity scores from this analysis, and identify the company's performance around those security requirements.

VPN penetration test.

The objective of a VPN penetration test is to identify security weaknesses introduced by a VPN solution that could be exploited by motivated malicious individuals to gain unauthorized access to critical internal systems and resources. Please note that Verizon does not attempt to bring any services or systems down with Denial of Service attacks. Instead, we use a series of vulnerability scanning tools and manual techniques to identify, validate, and exploit security vulnerabilities, and all testing activities are closely coordinated with the organization to ensure there are no negative impacts to normal business operations.

verizon

Testing of VPN-related resources.

Testing includes:

- Examination of the VPN client solution, ensuring anti-virus software functionality and endpoint restrictions are not able to be bypassed by the end user
- Targeted penetration tests of VPN servers from an external, internet-facing perspective. Without credentials, we attempt to exploit vendor device vulnerabilities as well as misconfigurations, and deprecated or insecure encryption protocols being used
- Credential theft. With credentials you provide, such as those of a typical employee that may have been phished or had their laptop stolen, we test access controls over the VPN as well as what information can be harvested from the client system and used to further access on the internal network
- Review of any pre- and post-authentication checks, such as Multi-Factor Authentication (MFA), certificates, anti-virus signature reviews, etc. in an attempt to bypass all or part of the authentication process

The combination of tests and tools varies based on target platforms and location. Where Verizon identifies critical or high-risk vulnerabilities, clients will be immediately notified so that corrective action can be undertaken. Moderate and low risk vulnerabilities that have been identified will be detailed in the final report of findings.

Reporting and next steps.

We provide a report on our findings as well as detailed, prioritized recommendations designed to help you improve information security protections and avoid or reduce the risk to identified business systems.

Not sure what to do with the final report? We can help you with a detailed roadmap for implementing our recommendations. If you select this option, we will work with you to determine the recommendations to be included in the roadmap, and then develop detailed project definitions, timing, costs and staffing projections for each project. This can give you a clear path to peace of mind.

Why Verizon.

As an award-winning leader in cybersecurity, we keep up with the rapidly changing nature of cyber threats by processing billions of security events each year, analyzing evolving threats at our global security operations centers, performing forensic investigations for companies around the world, and sharing our knowledge through industry-recognized content like the annual Data Breach Investigations Report.

We differ from other security service providers because our substantial risk and incident experience lets us understand the real-world threats you face and the potential vulnerabilities in each system. And, our years of practical experience in developing and implementing security programs across all industries lets you know that our priority is your long-term success.

Learn more.

For more information on Verizon's Remote Working Security Assessment, contact your account representative.

For the 2020 Data Breach Investigations Report, go to: enterprise.verizon.com/resources/reports/dbir

verizon