Mandiant

DATASHEET

Remote Security Assessment

Benefits

- Understand your organization's exposure related to remote work
- Reduce the likelihood and impact of incidents due to the compromise of remote work related assets
- Receive corrective and tactical recommendations to help maximize security of existing remote infrastructure
- Generate assessment with low organizational impact

Assess and improve the security of remote access and operations

Mandiant has been at the forefront of cybersecurity and cyber threat intelligence since 2004. Our incident responders have been on the frontlines of the most complex breaches worldwide. We have a deep understanding of both existing and emerging threat actors, as well as their rapidly changing tactics, techniques, and procedures.

Overview

As organizations increasingly adopt and expand remote work models, they need to manage staff working from home using a variety of end user computing and collaboration platforms. While organizations adapt to the remote work model, cyber attackers are not slowing down. If anything, they seek to exploit organizations during such times of change and uncertainty. Any sudden increase in remote working has the potential to change the attack surface and vulnerability of enterprise networks.

Mandiant Remote Security Assessments are designed to help your organization understand the nature of and changes in attack surface exposure due to remote work. These assessments are tailored to your organization to minimize the risk of impacting system availability during testing and are delivered remotely with limited involvement of your security team. After a Remote Security Assessment, Mandiant provides recommendations to reduce risk by minimizing the likelihood, impact, and total cost of a security incident caused by compromised remote access infrastructure, remote workstations, and collaboration technology.

Two variations of this service are available:

Each of these remote security assessments can be delivered remotely in approximately one week.

Each assessment includes a detailed report with:

- Executive summary
- Technical observations
- Actionable recommendations for improvements

	Remote Access Security Assessment	Remote Endpoint Security Assessment
Description	Provides your organization with a view of their remote access infrastructure, collaboration tools, security controls, and policies. Organizations can use this assessment to validate the security posture of their remote access solutions and collaboration platforms and ensure that security best practices are followed when securing access and data across these platforms.	Examines the security posture of your organization's email and remote workstation security configurations and technologies. The Remote Endpoint Security Assessment also demonstrates potential malicious code execution that may establish initial entry into remote workstations.
Phase 1	**Strategic phase:** Documentation review and workshops are conducted to collect information about infrastructure, policies, and practices, which are compared against best practices recommended by Mandiant experts.	**Phishing exercise**: Simulated email phishing campaigns are launched against in-scope personnel to assess email security and employee security awareness.
Phase 2	**Technical testing:** Targeted attacks are simulated against remote access infrastructure using the latest attacker techniques to validate findings from the strategic phase.	**Host assessment:** Targeted attacks are simulated against remote endpoints using the latest attacker techniques.
Diagram