MANDIANT

MANDIANT CONSULTING DATASHEET

Ransomware Defense Assessment

Benefits

- Understand your organization's true exposure to sophisticated modern ransomware attacks
- Uncover existing operational deficiencies of your security program targeted by ransomware threat actors
- Identify specific organizational assets at higher risk of being affected by ransomware attacks
- Receive highly actionable technical and strategic recommendations to reduce the likelihood and impact of ransomware attacks and improve overall resilience to protect critical assets
- Prioritize budgets, investments and resources to effectively combat ransomware attacks

Evaluate and improve your cyber defenses to combat ransomware attacks

Ransomware and multifaceted extortion have become the top threats for organizations of all shapes and sizes. The multibillion-dollar industry behind these threats can cripple business operations for days or months. Ransomware attackers have intensified their missions by threatening vital data and impacting infrastructure at such a level that it is deemed a national security threat in certain parts of the world.

Ransomware tradecraft continues to mature, as attackers now deploy more manual and targeted attacks and forego automated scripts and self-spreading malware. It is imperative that security teams develop stronger defenses against this critical threat.

Overview

The Mandiant Ransomware Defense Assessment uses a combination of workshops, technical reviews and attacker simulation exercises to offer an expert evaluation of your existing technical and operational security controls. Our goal is to help you effectively prevent, detect, contain and respond to the deployment of ransomware and multifaceted extortion attacks in your specific environment.

After the assessment is complete, Mandiant delivers recommendations to help minimize the likelihood, impact and cost of a ransomware incident for your organization. Since no two organizations are alike and attackers are continually changing their techniques, Mandiant experts create customized, actionable implementation priorities to help your organization achieve a ransomware resilient security program.

Mandiant consultants also provide opportunities to further test and expand your defensive operational and technical controls. If desired, expanded assessments and exercises can work toward ransomware-related security objectives aligned to your organization's security investment plan (Table 1).

Our Approach

The Ransomware Defense Assessment is delivered through **a series of three core evaluations** that address your security program's cyber defense capabilities in the event of a ransomware attack.

1. Operational Capability Assessment

This portion of the service focuses on four competencies required for effective and rapid cyber defense against a ransomware attack. Through a series of documentation reviews, interactive subject matter expert workshops and targeted personnel interviews, we assess the following critical domains:

- **Security Architecture.** Technologies, controls and networks required to combat adversaries and resume business operations.
- **Response.** People, processes, and technology capacities required to swiftly respond.
- **Communications.** Internal and external communication processes used to deliver messages to key stakeholders including cyber insurance agencies, legal counsel and your own organization.
- **Recovery.** The specific approach to remediation and recovery activated from this attack type.

2. Adversary Detection Assessment

This portion of the assessment tests your team's capabilities to detect and stop a ransomware attack in-progress. Mandiant consultants simulate threat actor behavior to demonstrate the full impact of a successful ransomware attack and its ability to cripple business operations. Our experts employ tools and techniques used by real-world ransomware threat actors, derived from actual incident response engagements, not hypothetical scenarios.

A collaborative red team is delivered by performing the following phases of engagement to realize the true capabilities of a ransomware attacker in your specific environment:

- **Assumed Breach.** Simulation of an initial breach through a Mandiant-controlled command and control payload or other means to determine the impact of any one user or system being compromised by a ransomware attack.
- **Reconnaissance.** Mapping of internal network architecture and identifying targeted systems, users or groups that are commonly abused by ransomware threat actors.
- **Lateral Movement and Privilege Escalation.** Exposure of network vulnerabilities and misconfigurations to escalate privileges and move laterally across commonly targeted systems such as domain controllers, backup servers and file shares.
- **Ransomware Deployment.** After business-critical systems are accessed, simulation of worming and encryption tactics are deployed on the client network using popular, real-world ransomware attacker techniques.
- **Capability Collaboration.** Mandiant works with your security team to assess and improve capabilities for detecting modern ransomware group behaviors, discover indicators of compromise (IOCs) and reduce internal attack surfaces.

3. Configuration and Architecture Assessment

This portion of the assessment concentrates on the Active Directory configurations most often abused by ransomware attackers. Targeted technical reviews of these settings evaluate the overall Active Directory security posture and identify likely attack paths.

- **Group Policy Object (GPO) and Active Directory (AD) Review.** A look at GPO and AD configuration data from in-scope domains to identify existing misconfigurations in your environment that ransomware attackers frequently use for incident escalation.
- **Endpoint Configuration Review.** Examination of in-scope endpoint hardening configurations enforced by Active Directory to identify opportunities for configuration hardening against ransomware attacks in your specific environment.
- **Server Configuration Review.** Analysis of in-scope server hardening configurations enforced by Active Directory to identify hardening opportunities to protect against ransomware attacks in your specific environment.

Engagement Timeline and Deliverables

This service engagement takes one to five weeks on average, depending on your needs and the services you select. Each of the three core evaluations can be delivered separately or in any combination.

After the engagement is completed, Mandiant provides a detailed report that includes:

- Security weaknesses and gaps categorized by severity to your business
- Existing strengths of your organization's security processes and procedures
- Actionable prioritizations and next steps for strategic security improvements
- Technical control recommendations to enhance ransomware detection, prevention and response capabilities

You can request a technical briefing for internal stakeholders on lessons learned, along with an executive briefing that summarizes the dangers posed by ransomware and the impact of a real attack on your organization.

Beyond the core Ransomware Defense Assessment methodologies, enhancements (Table 1) can be added to any engagement for an additional cost.

TABLE 1. Additional offerings for engagement enhancements by category.

Operational Capability Assessment

Tabletop Exercise	Test the effectiveness of your organization's existing incident response plans, escalation procedures and business continuity communications through reenactment of a real-world ransomware event remediated by Mandiant.
Crown Jewels Assessment	Identify the critical assets that matter most to your business and appear highly attractive to adversaries performing a ransomware attack. Receive a custom asset risk profile from informational and systemic viewpoints.
Playbook Creation	Receive customized, actionable ransomware-related incident response plan guidance including best practice process prerequisites, roles/responsibilities and effective workflows.
ThreatSpace™ Cyber Range	Experiment hands-on with real-world ransomware attack scenarios to rehearse and refine your incident response in a consequence-free environment.

Adversary Detection Assessment

External Penetration Test	Identify common ransomware vulnerabilities and misconfigurations on your organization's systems, services and applications that are exposed to the Internet.
Social Engineering Assessment	Evaluate employee security awareness, policies, procedures and technical controls that are intended to stop ransomware attackers from obtaining access to your vital networks, critical assets and sensitive data.
Purple Team Assessment	Practice detecting complex, modern ransomware group behaviors, find indicators of compromise (IOCs) and reduce your internal attack surface with the help of Mandiant consultants every step of the way.
Attack Surface Mapping	Discover a holistic view of your attack surface landscape and externally exposed assets, uncovering unknown attack vectors that often lead to a ransomware compromise.

Configuration and Architecture Assessment

Disaster Recovery Architecture Review	Assess your organization's current backup environment, backup management processes and restoration plans against large-scale ransomware attacks. Hardening and improvement recommendations are provided to address each area.
Active Directory Security Assessment	Improve important processes, configuration standards and security controls required to effectively secure an Active Directory environment and its supporting infrastructure against ransomware attacks.
Cloud Security Assessment	Evaluate your existing cloud security and hardening techniques to protect against ransomware attacks on popular cloud-based assets, including Microsoft 365, Microsoft Azure, Amazon Web Services and Google Cloud Platform.

Learn more at **www.mandiant.com/consulting**

Mandiant
11951 Freedom Dr, 6th Fl, Reston, VA 20190
(703) 935-1700
833.3MANDIANT (362.6342)
info@mandiant.com

About Mandiant
Since 2004, Mandiant® has been a trusted partner to security-conscious organizations. Today, industry-leading Mandiant threat intelligence and expertise drive dynamic solutions that help organizations develop more effective programs and instill confidence in their cyber readiness.

MANDIANT
YOUR CYBERSECURITY ADVANTAGE