MANDIANT

YOUR CYBERSECURITY ADVANTAGE

RANSOMWARE DEFENSE VALIDATION

SERVICE DESCRIPTION | v1

Mandiant Managed Validation Service Description

Revision 1

Mandiant Contact Information:

Website: www.mandiant.com

Support Email: customersupport@mandiant.com

Support Number +1-888-668-8987

Mandiant Security Validation

With over 15 years of experience at the forefront of cyber security and cyber threat intelligence, Mandiant's mission is to make every organization secure from cyber threats and confident in their readiness. Mandiant delivers dynamic cyber defense solutions powered by industry-leading expertise, intelligence, and innovative technology.

Ransomware Defense Validation Subscription

Mandiant Ransomware Defense Validation (the "RDV Subscription") is a Security Validation Subscription run by Mandiant focused on providing customers a clear understanding of their ability to withstand the end stage of a ransomware attack: The encryption of data on critical infrastructure. The results produced from the Subscription help drive better understanding of security control efficacy and reduced risk for their business.

The Subscription provides clear pass or fail results for how endpoint security controls perform when specific ransomware attempts to encrypt files or directories. As detailed in this Service Description, the RDV Subscription is designed to provide clear expectations, a streamlined deployment, and easy-to-consume reports.

The results of Ransomware Validation tests are communicated through a streamlined user interface accessible via the Mandiant Advantage portal. These automatically generated results are supplemented with monthly discussions and quarterly business reviews to help ensure an understanding of how to interpret results and what upcoming validation tests will focus on.

Subscription Details

The RDV Subscription gives flexibility to incrementally expand beyond validating a single endpoint and security zone as needed after an initial endpoint within a single security zone is brought online and stable.

The RDV Subscription is available as a 'Fully Managed' subscription. Customers have 24x7 self-service access to the latest results which include curated ransomware specific reports from Mandiant Threat Intelligence.

The Ransomware content delivered with the RDV subscription is updated automatically and driven by the latest threats Mandiant sees attacking our customers' industries and peers.

Functionally, the Subscription is driven by the automated execution of actions which deploy and test Mandiant's "Repurposed Ransomware" within the production environment. This repurposed ransomware is a differentiator, and developed by Mandiant's expert malware reverse engineering team.

Ransomware Defense Validation Delivery and Onboarding

Onboarding

All MSV Subscriptions start with an onboarding phase to set expectations, introduce Mandiant team members, and pre-schedule important QBRs. On or shortly after the Order Effective Date of the RDV Subscription, the customer will receive a welcome email with instructions for accessing the Mandiant Advantage portal.

Expectations will be defined and discussed during a 50 minute "Kick-Off" meeting, to be scheduled shortly after the Order Effective Date:

- **Create an achievement-based workflow**
- **Schedule QBRs with executive sponsors**
- **Run a transparent process with clear assignment of ownership and responsibility.**

Prior to the Subscription 'go-live,' it is the responsibility of the customer to take account of and own any change control procedures that require stakeholder action across internal departments (where applicable) as part of the onboarding and deployment process. The customer will be responsible for identifying resources up front with knowledge of the environment should they need to perform any enablement tasks for RDV (i.e., creating network egress routes, approving allow-list changes on endpoints, etc.)

Subscription Contacts | Customer

TITLE / ROLE	DESCRIPTION / JOB FUNCTION	
Executive Management or Sponsor	Director-Level through CISO (Chief Information Security Officers). Has decision-making authority and helps to hold the operational team accountable. Sets expectations relative to the overall metrics of the organization.	
Red Team Owner or 3rd Party Vendor	Responsible for managing the Red Team activities and reporting results.	
Security Operations Center	SOC (Security Operations Center) Manager, SOC Analyst (L3 (Layer 3)), Vendor Specialist, SME (subject matter experts)	
Endpoint Infrastructure Owner	Responsible for managing & deploying approved endpoint images to workstations and servers	
Endpoint Security Controls Owner	Responsible for Endpoint AV (Anti-Virus) (typically one owner per EP security technology), Endpoint Control Management Console	

	(Log Aggregation, Updates, Rules), Endpoint Policy Violation Reporting	
Network Infrastructure Owners	Responsible for managing and configuring core network services such as NTP, DNS, and Proxies	
Network Security Control Owners	Responsible for managing and configuring security controls such as Firewalls, Email, IDS/IPS, SEIMs	
Security Engineering Owners	Responsible for integrating data from security controls into an information system. Responsible for data backups and restoration	
Security Training and Awareness Owners	Internal resource or3rd party vendor providing security training and awareness to corporate and/or security staff.	

Subscription Contacts | Mandiant

Technical Account Managers

Mandiant will assign a technical account manager (TAM) to configure the system and provide periodic updates to the customer. This TAM will be the first point of contact for requests from the customer depending on the topic. The TAM will facilitate the automated generation of the reports through the RDV application and if needed, forward those reports to the customer. The TAM will review the reports monthly with the customer. Mandiant will rotate the TAM as needed based on internal decisions, customer preference, or specific phase of the subscription.

Other Mandiant Resources

Mandiant will also provide other resources for various phases of the subscription. Those resources and their responsibilities are detailed below:

MANDIANT RESOURCE	ROLE / RESPONSIBILITIES
Advantage Platform Ops Team	Provisioning the customer and end users with access to Advantage
Field Engineering Team	Provisioning the RDV tenant within the Advantage Security Validation
Principal TAM	Attend kick-off meeting and monthly and quarterly reviews. Provide backup to TAM as needed.
Account Rep	Attending kick-off meeting, manage subscription renewals and upgrades. Attend monthly and quarterly reviews
Customer Support	Field inbound inquiries from customers related to typical use of RDV, escalate to TAMs (Technical Account Manager) as needed.

Threat Intelligence & Malware Reverse Engineering Teams	Provide representation at quarterly reviews and updates on ransomware families Mandiant will be delivering in the next quarter.

Subscription Initiation and Delivery

Subscription will begin once the customer has been provided credentials to access the Ransomware Defense Validation application via the Mandiant Advantage portal. This provides immediate access to ransomware-specific threat intelligence.

Validation tests will begin executing after on-boarding and actor installation has completed. Daily status will be available immediately once validation tests begin.

Ransomware Defense Validation System Requirements:

Parameter	Requirement
Operating Systems Supported	Server: Windows Server 2012R2, Windows Server 2016, Windows Server 2019 Workstation: Windows 8, Windows 10, Windows 11
Host Execution Environment	Physical Machine, VM (Virtual Machine) in local environment, VM in cloud environment
Network Requirements	Network accessibility for traffic on port 443 to Mandiant specified FQDNs (fully qualified domain names)

Ransomware Defense Validation Subscription Setup & Operation

This phase centers around setting up the customer's account.

Onboarding into RDV	• Advantage Organization Created • Customer Points of Contact identified • MSV Team Assigned • QBR1 meeting scheduled with Exec Sponsor • MBR1-3 meetings scheduled with Operational Team Leaders

Phase Two: System Setup:

System Setup begins with an overview of the RDV Subscription and planning for the endpoint setup. Shortly after the RDV Subscription begins, the following will take place:

System Setup	• Kick-off Meeting Occurs • End Users invited to Advantage • Security Technology Identified & Cataloged • OS (Operating System), version, and auto-update configuration for standard distribution of Windows endpoint image identified • Security Zone Created • Network path from targeted machine in production security zone to Advantage established • Endpoint Actor registered to Advantage RDV • Customer network proxy configured on actor (if required) • Endpoint Actor Allowed List in endpoint security control

	• Endpoint Actor Online • Endpoint Actor executes “Hello World” Job successfully.

Customer Required Actions:

Component	Requirements
Endpoint Machine	• Provide a *dedicated* physical or virtual windows machine within their preferred security zone. This machine will host the endpoint actor • Provide a credentials for a System Profile with permissions to access the endpoint machine.
Endpoint Operating System	• Install the latest approved endpoint image on the dedicated machine.
Endpoint Security Controls	• Allow list the Mandiant Actor Application in endpoint security control software.
Endpoint Actor	• Install the specified endpoint actor application from Mandiant. • Verify the endpoint actor is “connected” to the “Advantage Platform”
Network Path	• In some cases, where a network proxy is involved, the proxy configuration must be communicated to Mandiant • The customer will need to allow-list our endpoint (*.mandiant.com)
Ransomware Defense Validation Reporting Portal	• A web-based reporting portal where customers can view the results of evaluations run on their behalf.

Phase Three: Execution

Execution involves validating the following action and expected results based on the most current Ransomware Defense Validation content available to the customer.

Validation Action	Goal
Endpoint Prevention for Repurposed Ransomware	• Endpoint security control **PREVENTS** all Ransomware encryption attempts in current content pack • MBR with Customer Occurs

(Recurring) Update of Content and System

Throughout the RDV Subscription term, Mandiant will update the ransomware content delivered and validated in the customer environment. The RDV application itself will undergo typical upgrades and security patches as needed.

(Recurring) Execution and Reporting on Use Cases

The TAM will continue to supervise the automated execution of Actions against the customer's endpoint security controls. As defined in this Service Description, reporting is provided via two methods

(1) Self-service review by the customer 24x7 via a login to Mandiant Advantage and selection of the RDV application.

(2) Monthly reviews with the TAM to explain results, answer questions, and review any discrepancies.

(Recurring) Quarterly Business Review

Mandiant will provide regular status reporting to include monthly RDV Subscription reporting. Reports will be generated by the RDV application and complimented with the following specific deliverables:

- Update on focus areas for upcoming subscription content
- Review of any improvements or beneficial changes to the RDV subscription the customer will automatically inherit
- Understanding and agreement on the need for endpoint / security zone expansion
- Capture of customer feedback
- General updates on other Security Validation portfolio products if requested

Subscription Details

The following sections detail the RDV Subscription provided to our customers

Ransomware Defense Validation

The SaaS-based, Ransomware Defense Validation managed service will rapidly help organizations understand their security infrastructure gaps and vulnerabilities. Further, the service will improve their overall ability to defend against ransomware attacks.

Ransomware Defense Validation is powered by top threat intelligence, automated content delivery, and modern automation. These capabilities combine to unlock a high velocity, low-touch approach to quickly deliver actionable outcomes.

USE CASE	DESCRIPTION	REQUIREMENTS AND QUESTIONS TO CONSIDER
Ransomware Defense Validation	Endpoint Images running production security controls will be tested for efficacy to prevent the encryption of data by specific families or variants of Mandiant-provided repurposed ransomware.	Requirements: Actor agent installed and allow listed on at least one windows-based endpoint with a secure network route to the Advantage platform

Reporting Cadence

Interval	What's Delivered
DAILY	Automated execution of the latest Ransomware Content delivered via the RDV subscription on or more endpoints
WEEKLY	Summary reports published to Advantage for self-service review and/or export by customers
MONTHLY	Live Readout of monthly progress
QUARTERLY	Stakeholder review of quarterly progress and a preview of next quarter's plan

System Access

The customer will receive access to the RDV application via Mandiant Advantage Login. The RDV application supports "pivots" to threat intelligence data such as Malware Battlecards, Ransomware Profile Summaries, and Ransomware Reports. The application will be hosted by Mandiant.

Once provisioned, customers can login here: https://advantage.mandiant.com

Technical Support

For technical services, customers will contact their assigned Technical Account Manager

Customer Support Email: customersupport@mandiant.com

Customer Support Number +1-888-668-8987

Documentation

Documentation for RDV will be made available as needed by the TAM and is also accessible in a self-service manner for customers via the “Knowledge Center” integration with the RDV application.