Mandiant

ADDRESSING SECURITY CONCERNS WITH SECURITY VALIDATION

Safety and security of the production environment is paramount, and increasing the effectiveness of controls is a core use case for security instrumentation. The Validation Platform has been designed to ensure the security and safety of its users.

- All network communication on the Validation Platform management plane is fully encrypted.
- A second layer of encryption is used to facilitate the secure registration between the Director and the Actor.
- The Director's HTTPD process runs with SSLFIPS enabled.
- The Actor can only communicate with the Director to which it is registered.
- All sensitive user data, including the secure tokens created during Actor registration, are encrypted at rest using AES256.
- Safeguards are in place to ensure that the real malware used inside the platform is processed safely and cannot be used to compromise production systems.

Safety Practices for User Data

Access to sensitive user data is strictly monitored and controlled by Mandiant. We prioritize safe handling of user data and enforce the following measures:

- Subcontractors are prohibited from accessing sensitive user data.
- The use of third-party services in critical IT maintenance is prohibited.
- Access to user data is limited and viewing activity is monitored through access logs.
- Background checks and non-disclosure agreements are enforced for individuals who access sensitive user data.

Network Communications

The platform's management plane is a web service that is fully encrypted using TLS 1.2. No other management communications or ports are required for the management plane to communicate between the Director and Actors.

While it is recommended that you also enable SSH to the components of the platform, this is optional and not required.

Even though Security Validation Actors may communicate over any allowed protocol by the networks in place, this is only done when executing Attacker Behaviors to test the security controls in place on the network.

See **Network Communication Architecture** **(https://docs.mandiant.com/home/msv-network-comm-architecture)** and **Network Communication Requirements** **(https://docs.mandiant.com/home/msv-network-comm-req)** for more details.

Actor Registration

The Actor registration process is a secure mechanism that ensures a Security Validation Actor can only receive communications from the Director to which it is registered. This process is also secured with an incremental layer of encryption. Here's how the process works:

1. On the Director, an Actor configuration is created. This starts an unregistered Actor in a Pending state with a generated security code for registration that is valid for 15 minutes.
2. Once an Actor of any type is installed, the Actor Registration process is initiated.
3. After the process is initiated, the security code created in Step 1 is transmitted between the Actor and the Director.
4. Once this code has been successfully validated, the Actor will move from Pending Actors and into the registered Actors list. During this process a secure token is generated that acts as the shared secret between the Actor and the Director. All subsequent communication utilizing TLS between the Director and the Actor will be authenticated using this token.

The secure tokens are also stored in an encrypted portion of the Director database, further enhancing the security of the solution.

Communication Between the Director and Actor

- Information sent from the Director to the Actor, depending on configuration:
    1. Non-optional information
        a. **Director's IP:** The Director's IP is provided to the Actor.
        b. **Current Time:** The current time of the Director is provided to the Actor.
    2. Configuration dependent information
        a. **Proxy Configuration (Admin User Config):** If the Actor is explicitly configured to be "behind" an Authenticating Proxy, the Authentication information is provided to the Actor.
        b. **NTP:** If the Actor is explicitly configured to use "internal" NTP, the Director's NTP server IPs are provided to the Actor.
        c. **DNS:** If the Actor is explicitly configured to use "internal" DNS, the Director's DNS server IPs are provided to the Actor.
        d. **Network Configuration:** If the Actor's network is reconfigured via the Director, all the network information is provided to the Actor, including private subnet ranges.
        e. **SSH Keys:** If an Action requires an SSH key, the SSH key is provided to the Actor.
        f. **Login password:** If a user sets a login password on the Actor, that password is sent to the Actor.
        g. **Certificate (HTTPS):** If a private certificate is configured for communications, that certificate is sent to the Actor.
- Information sent from the Actor to the Director:
    1. Non-optional information
        a. **Actor's IP:** The Actor's IP is sent to the Director.
        b. **Current Time:** The Actor's current time is provided to the Director.
        c. **User:** The Actor's username is sent to the Director.
        d. **OS package information:** The OS package information is sent to the Director to help it determine if an OS upgrade is required.
        e. **Output / Logs of Actions:** All logs of Actions run on the Actor are sent to the Director.
    2. Configuration dependent information
        a. None currently exist.

Life Cycle of Malicious File Transfer Actions

The Director encrypts the malicious file and sends it to the source Actor. The source Actor receives the malicious file and stores it obfuscated in a temporary directory. Next, the network security control test is run, where the malicious file is transferred from the source Actor to the destination Actor. Finally, the malicious file is deleted from both the source and destination Actors after the Action completes.

Safe use of Malware in Security Validation

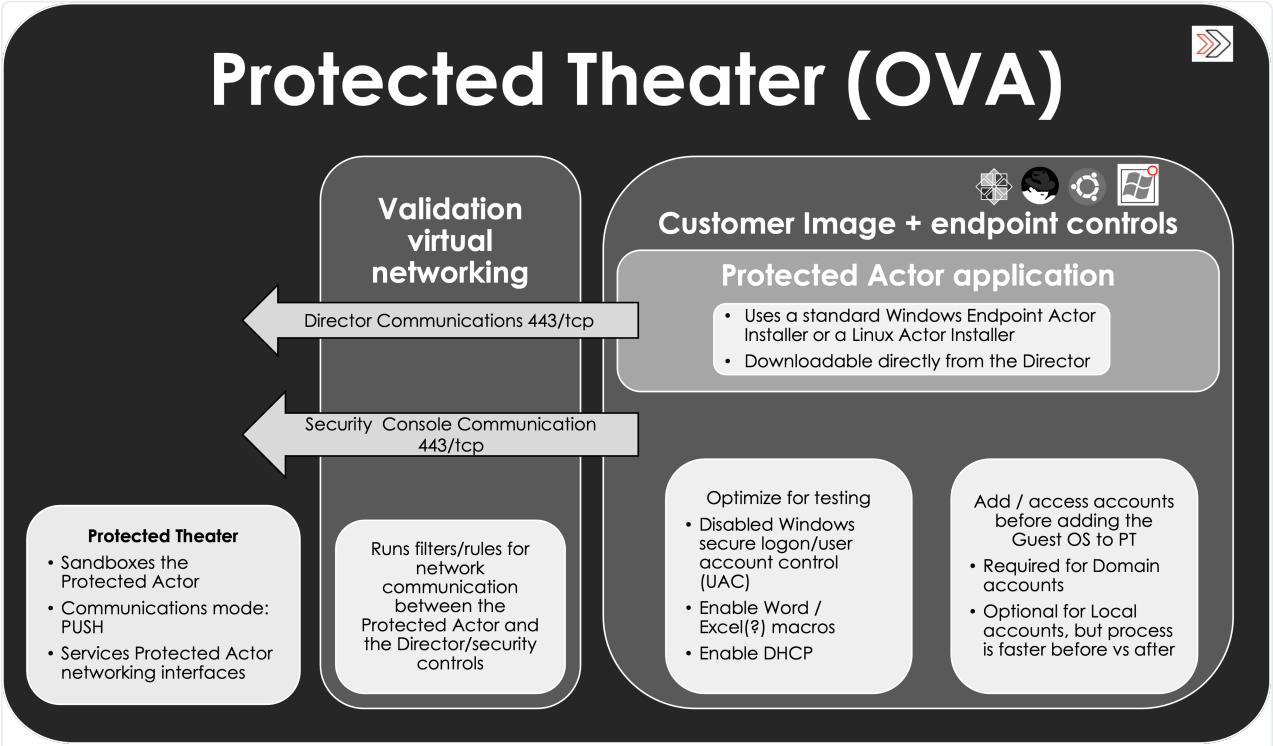
Security Validation security content leverages real attacker behaviors and real malware to ensure the accuracy of our tests and prevent the possibility of false positives when evaluating the performance of security controls. Safety is maintained through multiple mechanisms designed into the platform.

1. Actors only communicate with other Actors when tasked by the Director.
2. When executing network Actions, the platform is in full control of both endpoints for communication. Actors take on the role of Attacker or Target, based on the instructions they receive from the Director, and mimic the type of system required to make attacker behavior credible.
3. Security Validation categorizes the Actions designed to test endpoint security controls into Destructive and Non-Destructive categories.
    a. Non-destructive endpoint security tests can be processed directly on endpoints where the Actor software is installed and registered to the Director.
    b. Destructive tests (wipers, bootloader attacks, ransoms, etc.) can be processed safely inside the Protected Theater, a sandbox designed specifically for testing these controls safely with snapshot and rollback capability.
    c. Destructive tests can only be processed in the Protected Theater.
    d. The creation of destructive Actions requires an approval workflow to be completed inside the Director by authorized personnel.

Protected Theater Overview

The Security Validation Protected Theater (PT) provides an isolated and nested virtualization environment for the testing of endpoint security controls against destructive behaviors. The Protected Theater is an OVA or VHD virtual image that is hosted on VMware Virtual Infrastructure.

1. "Gold" images of the Windows systems deployed to end user hosts are ingested into the Protected Theater.
2. Once the gold image is ingested, you're able to sign into the image to download the Security Validation Windows Actor executable and register in a manner similar to other Actors.
3. As with the Windows Actor operating outside the Protected Theater, the local Validation Platform agent executable is the only file that must be added to the Allow list for operation. Security Validation has confirmed that this configuration operates with Carbon Black, Cisco AMP for Endpoints, Cylance, Symantec and Microsoft® Windows® Defender endpoint protection software.

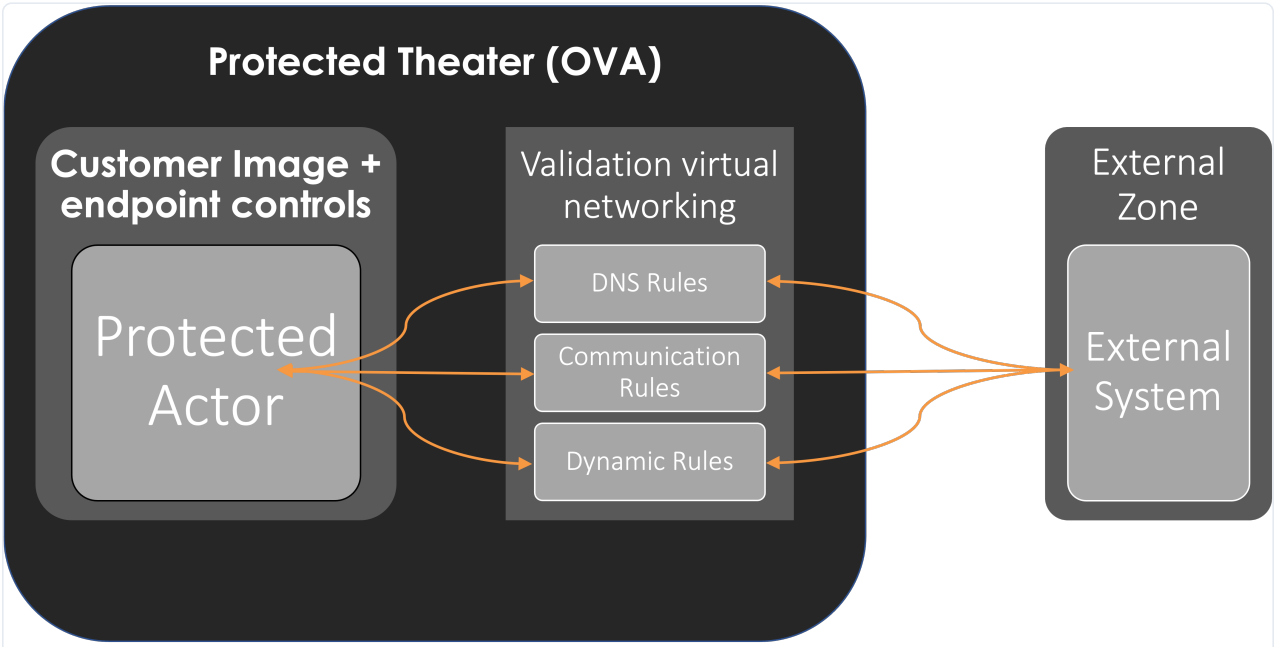


Overview of PT environment & functionality

Protected Theater Network Protections

The Protected Theater uses the Security Validation Virtual Network. This is used to isolate network connectivity, working similarly to a firewall. There is also a built-in DNS server.

- By default, the Security Validation Virtual Network only allows the Protected Actor to communicate with the Director through port 443.
  - Users with the Admin role can also update the configuration to allow additional ports.
  - All other traffic is blocked.
- The built-in DNS server responds to all queries with an IP Address of 1.2.3.4.
  - The IP Address can be configured on the Advanced Settings page. (Go to **Settings** > **Director Settings**. The Systems Settings page opens. Then click **Advanced Settings**).
  - If other DNS responses are required, configure those by going to **Environment** > **Protected Theaters**.



Overview of PT Communications

Protected Theater Endpoint Protections

A snapshot of the image is created before you run your first malicious Action in the Protected Theater and each time you update the PT. You can also add a new snapshot manually by editing the Protected Theater.

After you run a Malicious Action, or a Group that includes a Malicious Action, the Windows or Linux image is rolled back to the snapshot, which is a known good state. In reverting to a known good state, any changes from running Host CLI Actions (such as file system and DNS entries) will no longer exist. No additional Jobs will run until this rollback is complete and the Actor has checked back in. This allows the effectiveness of the security stack to be demonstrated without the risk of infecting the actual environment.

Platform Security

The following list details the process for how security is baked into Security Validation product offerings:

Functional area	MSV	MA-SV
Patches	Customer must apply the patches	Applied as they become available, Actors being upgraded from the Director
Communications	Encrypted	Encrypted
Actor management Interface	Customer determines ingress connections to the Director	Automatically limited ingress connections to Director
Customer IP space	Customer's responsibility	Limits access to customer IP space and any public pull Actor IPs
Certificates	Customer's responsibility	Automatically maintained for Actors and Directors

Mandiant Advantage Security Validation (MA-SV) Specific Security Measures

Data Management Policy

Question	Answer
How is user data segmented?	Customer-specific data stored in the databases is logically separated from other customers' data, which provides segmentation and isolation across a multi-tenant environment.
Is the database shared?	No, the database is separated.
What is the architecture?	Google Cloud
What controls are there to prevent data spill between instances?	The database is logically separated to prevent data spill between instances.
How many resources are shared?	All are shared, as MA-SV is a multi-tenant environment.
Does the client get their own instances?	Yes
What country is the data hosted in?	The United States
Who has access to the data?	Authorized Mandiant employees with the need to access the data for maintenance or related purposes will be granted access.

Question	Answer
Who ultimately owns the data acquired by MA-SV use (events, logs, and so on)?	The customer
What is the data used for?	Performing services as agreed in the statement of work
What is the data retention?	See the Mandiant Data Retention and Backup Policy.
How do we ensure data is protected?	Any credentials required for accounts used to access systems such as hosts, proxies, or cloud accounts are salted, hashed, and then stored in a database which is encrypted at rest. Mandiant performs key rotation on a yearly basis in order to ensure that customer data is kept secure. In the event there is any indication of compromise we can rotate said keys immediately as well.
How/when is the MSV director patched?	The MA-SV Director is patched in accordance with Mandiant's internal policies, applicable to all customer facing applications. To summarize, critical issues are resolved within 48 hours. In the event a patch creates a change functionality in anyway, ad-hoc maintenance windows are established and notifications are sent to customers before/after these events.
Is it possible to use external auth (2FA) to authenticate into the SaaS director (i.e. how would we authenticate and can we tie in our own MFA to the director)	We support providers enabling SAML 2.0 for third party authentication.
Any extra considerations for Cloud Validation Module in all of the preceding categories?	There are no differences pertaining to the Cloud Validation Model.