INTEGRATIONS OVERVIEW

Use this document to understand integrations for Mandiant Security Validation (MSV):

- MSI Integrations (Supported and recommended for new integration configurations)
- Legacy Integrations (Supported for existing integration configurations)

MSI Integrations

This document covers the the MSI method of creating an integration. This method is the recommended approach for configuring new integrations in Security Validation.

See the following sections for more information:

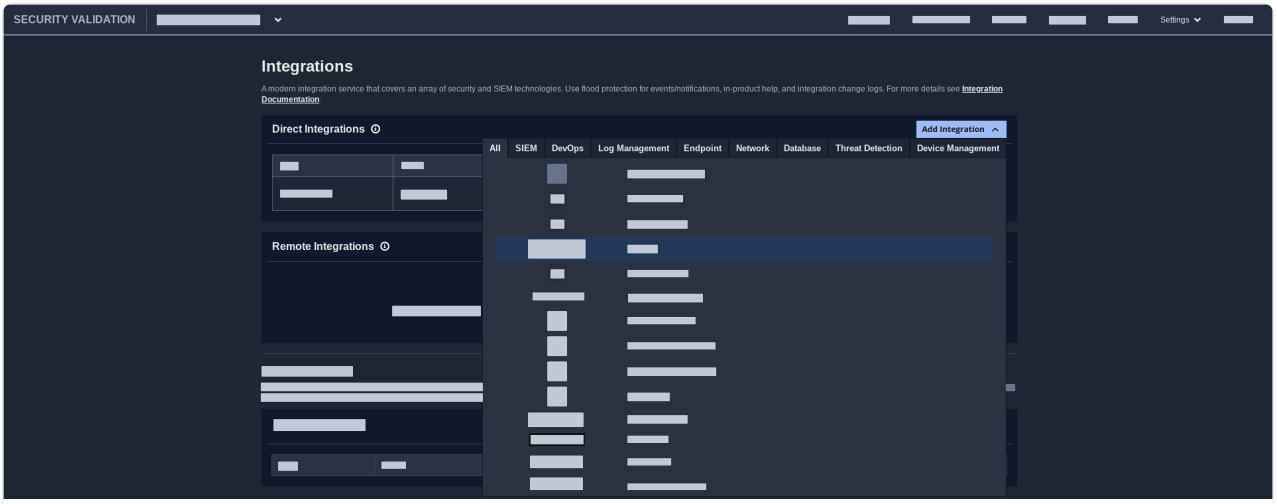
- **Overview**
- **Video overview**
- **Prepare your environment**
- **Supported technologies**

Overview

Integrations are a primary component of the Security Validation platform. By integrating with third-party technologies, the platform receives events that let you measure the effectiveness of those solutions. You can integrate with technologies that broadly fall into one of the following main categories:

- SIEM
- Database
- DevOps
- Endpoint
- Network
- Database
- Threat Detection
- Device Management

For Security Validation (Mandiant Advantage Security Validation (MA-SV) and supported releases of MSV), use the Direct and Remote Integrations tables to take advantage of the latest Integrations platform.



Direct and Remote Integrations Tables in Security Validation

If you already have Legacy Local and/or Remote Integrations set up, and they are working for you, you may continue to use them. If they start to have issues, or you need to upgrade to a newer SecTech version not supported by Legacy Integrations, or Google Support recommends it, you can switch to the new Integrations platform so that you can take advantage of the latest features and functionality.

Benefits of MSI integrations

- **New and updated Integrations**: The Mandiant integrations platform covers an array of integrations and security technology platform versions.
- **Frequent updates to Integrations**: In addition to updates that occur in Security Validation releases, improvements and bug fixes are released in the **latest security update (https://docs.mandiant.com/home/msv-security-update-downloads)**.
- **Low-touch configuration**: Mandiant provides in-product help that is specific to your integration and a change log showing any relevant updates to the Integrations platform.
- **Notification flood protection**: On Legacy Integrations, only specific third-party technologies let you control notifications. For Direct/Remote Integrations on the modern platform, regardless of the technology you're integrating into Security Validation, you get control over the limits on event and alert notifications.

Direct and Remote Integrations

- **Direct**: Any third-party security technology that the Director can connect to directly without having to use the Director to Actor communications.
- **Remote**: Any third-party security technology that the Director needs to connect to over a Director-to-Actor communication channel.

Adding an integration using the Direct Integration approach doesn't always work because communication is prevented by network boundary issues. In that case, you can configure a Remote Integration. Remote Integrations are integrations that are installed on a Security Validation platform Actor that then communicates over a network boundary through an integrated proxy function.

Video overview

Prepare your environment

Prerequisites

- **On-prem only**: Direct and Remote MSI Integrations require Mandiant Security Validation (MSV) 4.13.0.0 or later
- **Remote Integrations**: You must meet the requirements listed in **Configure Remote Integrations (https://docs.mandiant.com/home/msv-remote-integrations)**.

- **Network requirements**:
  - **Standard deployments**: If you have a cloud technology behind an access control list (ACL) on a firewall or other network security system, add the following egress IP address to your ACL: `35.184.185.156`
  - **Hosted Director deployments**: If you're on a Hosted Director (`https://d01-cxxx.verodin.cloud`), your egress IP address is different from standard deployments. Work with your account representative to determine this value and what needs to be opened on your firewall infrastructure for MSI integration support.

- **User access**: Users require either System Admin or Power User privileges to configure Integrations. For more information, see **Security Validation User Groups and Permissions (https://docs.mandiant.com/home/msv-user-groups-and-permissions)**.

Variable mappings

As you move from Legacy Integrations to MSI Integrations, note the following variables that need to be changed:

```
IPS = "%IPS%"
ACTOR_IPS = IPS
HOSTNAMES = "%HOSTNAMES%"
ACTOR_HOSTNAMES = HOSTNAMES
DOMAINS = "%DOMAINS%"
EMAIL_SENDERS = "%SENDERS%"
EMAIL_RECIPIENTS = "%RECIPIENTS%"
USER_ACCOUNTS = "%USER_ACCOUNTS%"
START_TIME = "%START_TIME%"
END_TIME = "%END_TIME%"
LIMIT = "%LIMIT%" # used for sql integrations
OFFSET = "%OFFSET%" # used for sql integrations
```

Limitations

- An Integration (Direct or Remote) that includes a proxy cannot be edited. Clicking **Save** does not save the changes and the Edit Integration dialog remains on the screen. As a workaround:
  1. Temporarily remove the proxy from the integration configuration (For the Proxy field, select **None - No Proxy Profile** and save the changes to the integration configuration.
  2. Once the changes are saved, edit the integration configuration again to add the proxy information. Save your edit.

Supported technologies

Security Validation provides Integrations for common security technologies. While all integrations have some shared configuration, there are differences. The Integrations user interface walks you through the entire configuration. Differences include available queries, variables that can be used, and fields used in mapping events from your technology to the integration in the platform. Non-SIEM integrations can also be identified as security technologies with prevention and detection settings.

The Mandiant Advantage App for Splunk (https://splunkbase.splunk.com/app/6128) and **The Mandiant Advantage App for QRadar (https://exchange.xforce.ibmcloud.com/hub/extension/3a996a7812c185dea2bf3731347b8226)** can also be used with Security Validation. These apps let you view information from Security Validation directly in Splunk and QRadar using the Security Validation Overview and Details Dashboards.

The following tables show important information about all integrations, organized by type. Information, such as the name of an integration and minimum supported version (if applicable), is included.

- If the supported version/API is listed as "N/A", then the technology either has no version or a specific version is not needed for the Security Validation integration to work.
- Most of the security technologies in the table work on both Direct and Remote Integrations. Any exceptions are called out in the configuration documentation.
- Common proxies (NTLM, Kerberos, and so on) are supported when they reside between the security technology and Remote Actor. In cases where another proxy is present between the Director and Actor, we cannot guarantee that this scenario will work.

SIEM (https://docs.mandiant.com/home/msv-siem)

Integration Name	Supported Version/API
AT&T USM Anywhere	API v2
AWS Cloudtrail	AWS Python client (boto3 version 1.16.63)
AWS GuardDuty	AWS Python client (boto3 version 1.16.63)
Alertlogic (Preview)	API v2
Alien Vault (Preview)	AlienVault 5.3.x
Anomali Security Analytics (Preview)	API v1
Arcsight	7.5+
Cisco FirePower (Remote only)	v7 or later
Crowdstrike LogScale	API v1
CrowdStrike Next-Gen SIEM Search	API v1
Darktrace	Threat Visualizer v6.1
Devo	API v2
Elasticsearch	7.2
Exabeam Cloud	
Exabeam Datalake	
Extrahop Reveal 360	Extrahop Reveal 360 (cloud)
Google BigQuery	API v2
Google Chronicle	API v1alpha
Google Cloud Logging	API v2
Graylog	3.3.3 4.2.2

Integration Name	Supported Version/API
IBM Qradar	v7.3
Juniper JSA	
LogRhythm Cloud	Rest API 7.7+
LogRhythm ElasticSearch	7.2.x 7.3.x
LogRhythm SQL	7.2x 7.3x 7.7x
Logzilla	
Microsoft Azure Log Analytics	API v1
Microsoft Azure Sentinel	API v1
Microsoft Graph API	
OpenSearch	2.9+
RSA NetWitness Respond	11.x 12.3 onward
Rapid7 InsightIDR	N/A
SQL (Preview)	• MS SQL • MySQL • Postgres • Oracle
Security Onion ELK (Preview)	
Security Onion ELSA (Preview)	
Securonix	
Splunk	8.x (API V1) 9.x-10.x (API V2)
Sumo Logic	API v1

Database **(https://docs.mandiant.com/home/database)**

Integration Name	Supported Version/API
ClickHouse	23.9+
Snowflake	API v2

DevOps (https://docs.mandiant.com/home/msv-devops-integrations)

Integration Name	Supported Version/API
AWS CloudWatch	AWS Python client (boto3 version 1.16.63+)

Endpoint (https://docs.mandiant.com/home/msv-endpoint-integrations-413-dnu)

Integration Name	Supported Version/API
Carbon Black PSC	AppServices API v6 Investigate API v2
Carbon Black Protection	API v2
Carbon Black Response	API v7
Cisco AMP (Preview)	API v1
Crowdstrike	API v2 (Raptor Release) API v1 (deprecated)
Cybereason	16.x-17.x
Cylance	API v2
Duo (Preview)	
Endgame	API v1
Exabeam Analytics	i54
Microsoft Defender for Endpoint	Plan 2
Netskope	• API v1 • API v2 (Preview)
Palo Alto Networks Cortex XDR	API v1
Palo Alto Networks Cortex XSIAM	API v1
SentinelOne	API v2.1
Sophos Cloud	
Symantec DLP	All

Integration Name	Supported Version/API
Symantec Endpoint Protection	14.3+
Symantec Endpoint Security	API v1
Tanium Threat Response	API v1
Trellix Endpoint Detection & Response (EDR)	API v2
Trellix Endpoint Security (HX)	API v3
Trellix Enterprise Security Manager	API v2
Trellix Network DLP	Endpoint 11.x
Trellix ePolicy Orchestrator (ePO)	5.10.0+
Trend Micro Trend Vision One	API v3
VMware AppDefense (Preview)	API v1

Network (https://docs.mandiant.com/home/network)

Integration Name	Supported Version/API
Checkpoint	R80 and later
Extrahop Enterprise	9.3
Palo Alto Networks Next-Gen Firewall	Panorama V8.1-11.2
RSA NetWitness Logs & Packets	11.x
Tipping Point	5.5.5.x
Trellix Email Security - Cloud (ETP)	API v1
Trellix IPS	API v2
Trellix Network Security (NX)	NX device software version greater than 9.0.2
iBoss	

Threat Detection (https://docs.mandiant.com/home/threat-detection)

Integration Name	Supported Version/API
F5 Threat Stack	API v2
Secureworks Taegis XDR	V1

Device Management (https://docs.mandiant.com/home/device-management)

Integration Name	Supported Version/API
Fortianalyzer	7.2.2

Legacy Integrations

This document applies to Classic/Legacy Integrations. You may continue to use these integration configurations. While no active development is happening for these integrations, we continue to provide Classic/Legacy Integrations in the product. You do not have to move to MSI Integrations. If your support engineer or TSC recommends or you choose to move to MSI Integrations, you can take advantage of the latest features and functionality. For more information, see the MSI Integration documentation in the **Integrations Overview** (https://docs.mandiant.com/home/msv-integrations-overview).

Need access to the Integration information offline? We've created a **PDF of all general available MSV Integration features** (https://docs.mandiant.com/help/download-full-pdf/id/620d7e13ccb103e8557b25b0/cid/637278c2057fb00b713611af). This was last updated Nov 15, 2023.

- Links in the Table of Contents will take you to a page in the PDF.
- Links in the body of the PDF will take you to the Mandiant Docs Portal (which requires you to sign in using your Mandiant Advantage credentials) or a page on the internet.
- If an image has a link, it takes you to a larger version of the image in the Mandiant Docs Portal.

Integrations are a primary component of the Validation Platform. By integrating with security devices, the platform receives events that allow you to measure the effectiveness of those devices. You can integrate with the following types of security devices:

- Security information and event monitoring (SIEM) solutions
- Intrusion detection systems (IDS)
- Intrusion prevention systems (IPS)
- Firewalls
- Data loss prevention solutions (DLP)
- Log management platforms
- Threat Intelligence Platforms (TIPs)
- Threat Intelligence Feeds (TIFs)

The TIPs and TIFs are part of the Threat Actor Assurance Module (TAAM) and are used to pull in information for Threat Actors. For all others, the platform gathers empiric data on detections and event generation when Jobs are processed.

Mandiant Advantage Security Validation (MA-SV) has Integrations for over 50 different technologies. While all integrations have some shared configuration, there are differences. This includes available queries, variables that can be used, and fields used in mapping events from your technology to the integration in the platform. Non-SIEM integrations can also be identified as security technologies with prevention and detection settings. **Mandiant Advantage for Splunk**

(https://docs.mandiant.com/home/ma-mandiant-advantage-for-splunk) can also be used with Security Validation, allowing you to view information from Security Validation directly in Splunk using the Security Validation Overview and Security Validation Details Dashboards.

This video walks you through configuring integrations in the Mandiant Advantage Security Validation (MA-SV) platform.

Network requirements

If you have a cloud technology behind an access control list (ACL) on a firewall or other network security system, add the following egress IP address to your ACL:

- `34.135.50.52`
- `34.41.192.72`

Additional resources

To help you with your integration configuration, the following topics are available:

- **Integration Queries Overview** (https://docs.mandiant.com/home/msv-integration-queries-overview)
- **Variables used in Integration Queries** (https://docs.mandiant.com/home/msv-variables-in-integration-queries)
- **Integrations - Field Details** (https://docs.mandiant.com/home/msv-integrations-field-details)

Supported technologies

The following tables display important information about all integrations, organized by type (SIEM, Network, Endpoint, and TAAM). Information such as an integration's name, vendor, minimum supported version, remote capability, and proxy support capability, is included. Integration technologies may be listed in more than one table.

> If the supported version/API is listed as "N/A", it means that the technology either does not have versions or that a specific version is not needed for the Security Validation integration to work. If the supported version/API is listed as "All", it means that all versions of the technology work with the Security Validation integration.

SIEM

Integration Name	Vendor	Supported Version/API	Remote Capable?	Proxy Support Local?[1]
AlertLogic (https://docs.mandiant.com/home/msv-alertlogic)	Alert Logic	APIv3	Yes	No
AlienVault (https://docs.mandiant.com/home/alienvault)	Alientvault	5.3.x	No	No
ArcSight (https://docs.mandiant.com/home/arcsight)	Micro Focus	6.8, 6.11	Yes	No
Microsoft Azure Log Analytics (https://docs.mandiant.com/home/msv-microsoft-azure-log-analytics)	Microsoft	APIv1	Yes	Yes*
Microsoft Azure Sentinel (https://docs.mandiant.com/home/msv-microsoft-azure-sentinel-2227)	Microsoft	APIv1	Yes	Yes*

Mandiant

Integration Name	Vendor	Supported Version/API	Remote Capable?	Proxy Support Local?[1]
Chronicle Backstory (https://docs.mandiant.com/home/msv-chronicle-backstory)	Chronicle	APIv1	No	Yes*
Cisco Firepower Management Center (FMC) (https://docs.mandiant.com/home/msv-cisco-firepower-management-center-fmc)	Cisco	5.5+	No	No
Devo (https://docs.mandiant.com/home/msv-devo)	Devo	APIv2	Yes	Yes
Elasticsearch (https://docs.mandiant.com/home/msv-elasticsearch)	Elastic	5.x, 6.x, 7.x	Yes	No
Exabeam Data Lake (https://docs.mandiant.com/home/msv-exabeam-data-lake)	Exabeam	DL-i33.1	Yes	Yes*
Trellix Helix (https://docs.mandiant.com/home/msv-fireeye-helix)	Trellix	API v1	Yes	Yes*
Google BigQuery (https://docs.mandiant.com/home/msv-google-bigquery)	Google	API v2	No	No
Google Cloud Logging (https://docs.mandiant.com/home/msv-google-cloud-logging)	Google	API v2	No	No
Graylog (https://docs.mandiant.com/home/msv-graylog)	Graylog	3.3.3+	Yes	Yes*
Juniper Secure Analytics (JSA) (https://docs.mandiant.com/home/msv-juniper-secure-analytics-jsa)	Juniper Networks	7.2.x, 7.3.x	Yes	No
LogRhythm Elasticsearch (https://docs.mandiant.com/home/msv-logrhythm-elasticsearch)	Logrhythm	7.2.x, 7.3.x	Yes	No
LogRhythm SQL (https://docs.mandiant.com/home/msv-logrhythm-sql)	Logrhythm	7.2.x, 7.3.x	No	No
LogZilla (https://docs.mandiant.com/home/msv-logzilla)	Logzilla	6.9+	Yes	Yes*
Trellix Enterprise Security Manager (https://docs.mandiant.com/home/msv-mcafee-enterprise-security-manager-esm)	Trellix	9.6.0, 10.1	Yes	No

Integration Name	Vendor	Supported Version/API	Remote Capable?	Proxy Support Local?[1]
RSA NetWitness Respond (https://docs.mandiant.com/home/msv-rsa-netwitness-respond)	RSA	N/A	Yes	Yes
IBM QRadar (https://docs.mandiant.com/home/msv-ibm-qradar)	IBM	7.2.x, 7.3.x, 7.5x	Yes	No
Securonix SNYPR (https://docs.mandiant.com/home/msv-securonix-snypr)	Securonix	Latest Version	Yes	Yes*
Splunk (https://docs.mandiant.com/home/msv-splunk)	Splunk	6.x+	Yes	Yes*
Splunk Enterprise Security (https://docs.mandiant.com/home/msv-splunk-enterprise-security)	Splunk	4.8.x+	Yes	Yes*
Sumo Logic (https://docs.mandiant.com/home/msv-sumo-logic)	Sumo Logic	19.x	Yes	Yes*
Threat Stack (https://docs.mandiant.com/home/msv-threat-stack)	Threat Stack	APIv2	Yes	Yes*

[1]If you see Yes* for Proxy support, it does not include Socks and NLTM.

Network

Integration Name	Vendor	Supported Version/API	Remote Capable?	Proxy Support Local?[2]
Check Point (https://docs.mandiant.com/home/msv-check-point)	Check Point	R71+	No	No
Cisco Firepower Management Center (FMC) (https://docs.mandiant.com/home/msv-cisco-firepower-management-center-fmc)	Cisco	5.5+	No	No
AWS CloudTrail (https://docs.mandiant.com/home/msv-aws-cloudtrail)	AWS	N/A	No	No
AWS CloudWatch (https://docs.mandiant.com/home/msv-aws-cloudwatch)	AWS	N/A	No	No

Integration Name	Vendor	Supported Version/API	Remote Capable?	Proxy Support Local?[2]
Darktrace (https://docs.mandiant.com/home/msv-darktrace)	Darktrace	N/A	Yes	Yes*
Exabeam Advanced Analytics (https://docs.mandiant.com/home/msv-exabeam-advanced-analytics)	Exabeam	N/A	Yes	Yes*
Trellix Network Security (NX) (https://docs.mandiant.com/home/msv-fireeye-integration)	Trellix	API v1.2; CMS >=7.6	Yes	Yes*
Trellix Email Security - Cloud (ETP) (https://docs.mandiant.com/home/msv-fireeye-etp)	Trellix	N/A	Yes	Yes
AWS GuardDuty (https://docs.mandiant.com/home/msv-aws-guardduty)	AWS	N/A	No	No
Trellix Network DLP (https://docs.mandiant.com/home/msv-mcafee-epo-dlp)	Trellix	15.x, 16.x	Yes	No
Palo Alto Networks Firewalls/Panorama (https://docs.mandiant.com/home/msv-palo-alto-networks-firewallspanorama)	Palo Alto	7.x - 10.x	Yes	Yes*
RSA NetWitness (https://docs.mandiant.com/home/msv-rsa-netwitness)	RSA	3.3.3.3	Yes	No
Security Onion - ELK (https://docs.mandiant.com/home/msv-security-onion-elk)	SecurityOnion	All	Yes	No
Security Onion - ELSA (https://docs.mandiant.com/home/msv-security-onion-elsa)	SecurityOnion	All	Yes	No
Symantec Data Loss Prevention (DLP) (https://docs.mandiant.com/home/msv-symantec-data-loss-prevention-dlp)	Symantec	All	No	No
Threat Stack (https://docs.mandiant.com/home/msv-threat-stack)	Threat Stack	API v2	Yes	Yes*

Integration Name	Vendor	Supported Version/API	Remote Capable?	Proxy Support Local?[2]
Tipping Point IDS/IPS (https://docs.mandiant.com/home/msv-tipping-point-idsips)	Trend Micro	4.1.x	Yes	Yes*
VMware AppDefense (https://docs.mandiant.com/home/msv-vmware-appdefense)	VMWare	API v1	Yes	Yes*

[2]If you see Yes* for Proxy support, it does not include Socks and NLTM.

Endpoint

Integration Name	Vendor	Supported Version/API	Remote Capable?	Proxy Support Local?[3]
Carbon Black CB Protection (https://docs.mandiant.com/home/carbon-black-cb-protection)	Carbon Black	API v1	Yes	Yes*
Carbon Black CB Response (https://docs.mandiant.com/home/msv-carbon-black-cb-response)	Carbon Black	>= 5.5	Yes	No
Carbon Black Cloud (https://docs.mandiant.com/home/msv-carbon-black-cloud)	Carbon Black	Alerts API v6	Yes	Yes*
Cisco Advanced Malware Protection (AMP) (https://docs.mandiant.com/home/msv-cisco-advanced-malware-protection-amp)	Cisco	API v1	Yes	Yes*
CrowdStrike (https://docs.mandiant.com/home/msv-crowdstrike)	Crowdstrike	API v3.x	Yes	Yes*
Cybereason (https://docs.mandiant.com/home/msv-cybereason)	Cybereason	16.x,17.x	Yes	Yes*
Cylance (https://docs.mandiant.com/home/msv-cylance)	Cylance	API v2	Yes	Yes*
Microsoft Defender Advanced Threat Protection (ATP) (https://docs.mandiant.com/home/msv-microsoft-defender-advanced-threat-protection-atp)	Microsoft	N/A	Yes	Yes*

Integration Name	Vendor	Supported Version/API	Remote Capable?	Proxy Support Local?[3]
Endgame (https://docs.mandiant.com/home/msv-endgame)	EndGame	API v1	Yes	Yes*
Trellix Endpoint Security (HX) (https://docs.mandiant.com/home/msv-fireeye-endpoint-security)	Trellix	API v1.2 ; CMS >=7.6	Yes	Yes*
Trellix Endpoint Security (https://docs.mandiant.com/home/msv-mcafee-epo)	Trellix	5.5+	Yes	Yes*
Trellix Network DLP (https://docs.mandiant.com/home/msv-mcafee-epo-dlp)	Trellix	5.5+	Yes	Yes*
Netskope (https://docs.mandiant.com/home/msv-netskope)	Netskope	78.1.0.333+	Yes	Yes*
Palo Alto Networks Cortex XDR (https://docs.mandiant.com/home/msv-palo-alto-networks-cortex-xdr)	Palo Alto Networks	API v1	Yes	Yes*
SentinelOne (https://docs.mandiant.com/home/msv-sentinelone)	SentinelOne	API v2	Yes	Yes*
Sophos Central (https://docs.mandiant.com/home/msv-sophos-central)	Sophos	API v1	Yes	No
Symantec Data Loss Prevention (DLP) (https://docs.mandiant.com/home/msv-symantec-data-loss-prevention-dlp)	Symantec	All	Yes	Yes*
Symantec Endpoint Protection (https://docs.mandiant.com/home/msv-symantec-endpoint-protection)	Symantec	14.x	Yes	No

Integration Name	Vendor	Supported Version/API	Remote Capable?	Proxy Support Local?[3]
Threat Stack (https://docs.mandiant.com/home/msv-threat-stack)	ThreatStack	API v2	Yes	Yes*
VMware AppDefense (https://docs.mandiant.com/home/msv-vmware-appdefense)	VMWare	API v1	Yes	Yes*

[3]If you see Yes* for Proxy support, it does not include Socks and NLTM.