MANAGED ENDPOINT PROTECTION - SERVICE GUIDE

Last Modification Date: 05/13/2022
Exported and Shared on: 01/30/2023

For additional information, visit www.intervision.com

CONTENTS

1 SERVICE DESCRIPTION

Managed Endpoint Protection Service covers malware detection, prevention, and containment for designated endpoints. This includes managed Cisco AMP for Endpoints protection, managed services via trained and focus cybersecurity experts, alerting of malware issues, and reporting of malware protection activity.

This managed service is provided for each endpoint – servers, workstations, laptops, and other Windows and RedHat/CentOS Linux-based, Mac, Android, and iOS endpoints. The service is designed to have all qualified endpoints covered with Malware Protector; a partially covered environment is not acceptable.

2 SERVICE DETAILS

This service is designed to provide endpoint malware protection and managed support of Malware Protector platform, policies, and incidents:

- Provides managed software to protect endpoints from malware and computer viruses
- AMP Software Troubleshooting and Support
- Alerting and ticketing of malware incidents
- Remediation guidance for malware infections
- Automated analysis of unknown rarely seen executables – cloud-based sandbox file execution to determine if executable is malicious
- Ongoing operations by knowledgeable Cybersecurity Operations Center staff
- Malware Protector software updates
- Malware protector administrative support with 24/7/365 coverage
- Proactive isolation of compromised Endpoints
- Activity and summary reporting

3 IMPLEMENTATION

The rollout of the Malware Protector platform has multiple steps to help ensure a successful deployment. However, this may vary depending on unique client environments or requirements. Below is the typical implementation process:

- Customer provides details on environment (operating systems, types of endpoints).
- Hosted Café SOC creates audit mode groups/policies and sends Malware Protector installation link to the customer.
- Customer deploys Malware Protector software (in audit mode) to a set of test machines in tandem with their current anti-virus solution for a short period of time
- Hosted Café SOC reviews the audit mode findings that include initial detections from Malware Protector, and customer reports any issues (machine performance, execution issues, etc.).
- Hosted Café SOC provides recommendations for whitelists/exclusions to the customer.
- Customer approves change list, and Hosted Café SOC makes the necessary changes.
- Hosted Café SOC moves existing installed endpoints to active/quarantine mode.
- Hosted Café SOC provides customer with new Malware Protector link to deploy active/quarantine mode agent on remaining systems.
- Customer deploys software to the rest of their environment and then removes any other anti-virus software.
- Hosted Café SOC provides reports of machines with Malware Protector software installed.
- Customer deploys Malware Protector to any missing machines not in the inventory report.
- Upon successful implementation, Hosted Café SOC will move into normal Malware Proctor runtime state with 24/7 production support.

4 SUPPORT

Hosted Café maintains a 24/7 operations center (Hosted Café SOC) which serves as the designated administrative contact for Malware Protector support. The Malware Protector technical support model provides unlimited support for the customer-designated IT contact (eg. IT Director, InfoSec Director, System Admin, etc.). However, direct end-user support is not included but may be obtained through Hosted Café HelpDesk services.

Phone, email, and ticket-based support activities include:

- AMP Software Troubleshooting and Support
- Policy management
- White-listing assistance
- Initiate deep scans
- Malware incident response –
    - Details of the event
    - File investigation
    - Recommend remediation actions
    - Malware infection root cause analysis
    - Platform administration and troubleshooting
    - Open and escalate issue with software to vendor
    - Standard reporting per client requirements
    - Hosted Café portal and Hosted Café portal access

Endpoint remediation such as manual file removal or operating system re-installation/reimaging is not included in this service. Complimentary services such as Managed Network Services, Help Desk, and Professional Services are available for these additional remediation capabilities.

5 HOSTED CAFÉ PORTAL(S)

The Hosted Café Managed Security Services portal provides access to Malware Protector events, incidents and reports. Client will have access to the Managed Cisco AMP console for full visibility to events, supported devices, policies, report and other critical information. Customers with Managed Security Service Manager will also have access to Malware Protector events and incidence through our SIEM. The Hosted Café portal is accessible via https://health.hostedcafe.com[1]

6 HOSTED CAFÉ SERVICE PORTAL

The Hosted Café service portal provides for the creation, tracking, and review of service tickets. All service ticket information is available via this portal and enables tracking of implementations, changes, releases, and general support issues. The Hosted Café Services portal is accessible via https://support.hostedcafe.com[2]

7 ALERTING

Malware Protector attempts to block malware. However, new threats such as unseen zero-day attacks may evade software detection. The service will alert upon critical or high risk events including an event such as “malware executed and not quarantined” via the ticketing system. These critical alerts are sent to both the 24/7 Operation Center and to the customer simultaneously.

Other non-critical events that are considered informational and do not require actions are collected and available through generated reports.

1 https://health.hostedcafe.com/
2 https://service.hostedcafe.com/

8 REPORTING

Malware Protector provides many operational, event, and activity reports. The following reports are available on demand within the Hosted Café Managed Security Services portal and may also be subscribed to for e-mail delivery:

- Managed Security Services Malware Protector: Computers with Failed Scans
- Managed Security Services Malware Protector: Detected Files Not Quarantined
- Managed Security Services Malware Protector: Failed Policy Update Attempts
- Managed Security Services Malware Protector: Last Scan Completed by Host
- Managed Security Services Malware Protector: List of Uninstalled Clients
- Managed Security Services Malware Protector: List of Vulnerable Applications by Computer
- Managed Security Services Malware Protector: Prevalence: Malware Executed and not Quarantined
- Managed Security Services Malware Protector: Threats Detected by Count
- Managed Security Services Malware Protector: Total Endpoints

Reports including malware file trajectory, sandbox activity, and research results are available on an as needed basis.

9 ROLES & RESPONSIBILITY MATRIX

	Hosted Café	Customer	Extended (Professional Services)
General			
Provide client escalation contacts and procedures		X	
Provide operating systems information		X	
Provide estimated number of endpoints to be installed		X	
Provide general network information (locations, bandwidth, bandwidth utilization) for Malware Protection software policy optimization		X	
Installation and Configuration			
Provide user name and password used to initiate scheduled scan		X	
Provide licensed software	X		

	Hosted Café	Customer	Extended (Professional Services)
Install software on machines		X	
Set up and administer Malware Protection software policies	X		
Identify which application, folder and files to exclude		X	
Configure exclusion: application, folder and files	X		
Monitoring and reporting			
Provide access to Hosted Café monitoring portal	X		
Configure malware activity dashboard in monitoring portal	X		
Manage incident notification profiles	X		
Provide ticket based notification for all high severity Malware incidents	X		
Provide reporting for overall malware activity	X		
Provide reporting for machines not checking in and not running scans	X		
Provide lists of endpoints with vulnerable applications	X		
Operations			
Provide agent software updates based upon InterVision supported versions **	X		

	Hosted Café	Customer	Extended (Professional Services)
Deploy/apply software update to endpoints ***	X		
Software vendor management	X		
Initiate unknown file investigations with Cisco Talos	X		
Update exclusion list per client requirements	X		
Update policy with new indicators of compromise	X		
Initiate a deep scans	X		
Update policies per client request	X		
Enable proactive isolation of compromised endpoints	X		
Infection and Remediation			
Malware quarantine (software)	X		
Root cause analysis of malware that is not quarantined or blocked	X		
Provide information relative to nature of malware infection	X		
Advise client on remediation actions for Malware not quarantined	X		
Trouble shoot endpoint devices not checking in or running scans		X	
Reimage endpoints machines infected by malware		X	

	Hosted Café	Customer	Extended (Professional Services)
Deep investigation of Malware Outbreak			X

*Extended services are optional services that can be provided with incremental fees. These services may be additional managed services or professional services

** InterVision is committed to providing your organization with the latest and greatest technology releases to protect your environment. InterVision supports Cisco recommended versions and may not be running on the latest version.

*** If an upgrade requires an uninstall of previous version, to mainitain SLA and incident response, client must assist InterVision with the unistall and reinstall process within 6-months of the request.

10 SUPPORTED ENVIRONMENT

Malware Protector is available for the following operating systems

Windows

Linux RedHat/CentOS

Android

iOS

Mac

See the AMP for Endpoints user guide at this permalink[3] for current system requirements:

11 ABOUT CISCO AMP FOR ENDPOINTS SOFTWARE

Managed Endpoint Protection is committed to using the best technology for malware detection, prevention and analysis. The service currently utilizes Cisco AMP for Endpoints that is a consistently leading breach detection and prevention technology as reported by NSS Labs Breach Detection Systems Report[4]. The NSS Labs comparative product test provides the details on how Cisco AMP achieved:

- 100% security effectiveness rating-the highest of all vendors tested
- The only vendor to detect and block 100% of malware, exploits, and evasion techniques during testing
- Fastest time to detection of all vendors tested
- Excellent performance with minimal impact on endpoint or application latency

Complete details of the software technology are available on the Cisco AMP for Endpoint website.

12 COMMERCIAL TERMS

The Managed Endpoint Protection Service is sold per endpoint defined as a workstation, laptop, server, virtual machine, mobile device, or any other operating system instance. A minimum of a 1-year commitment is required for new and add on purchases. This service is billed monthly, in advance of the coming month.

No other services are required to utilize Cisco AMP for Endpoints software.

3 https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf
4 http://www.cisco.com/c/m/en_us/offers/sc07/amp-analyst-report/index.html