SERVICE DESCRIPTION

Managed Application Control (MAC)

Application control solutions allow customers to enforce a policy that determines what applications are trusted and allowed to run on endpoints. These solutions (which provide real-time visibility into executables running across their environment including file creation as well as file and registry modification, and registry) are effective security solutions but often difficult to manage and maintain. Trustwave's Managed Application Control (MAC) MSS, which leverages market-leading Carbon Black's Cb Protection technology, assumes the resource-intensive management and maintenance responsibilities that accompany application whitelisting.

Base Features of Service

The MAC service provides the following components:

- Service Initiation/Transition – Activities required to establish the Managed Application Control MSS between Trustwave and client.
- Service Management – Activities involving the system configuration of policies, maintenance, and health monitoring & management provided by the Security Operations Center.

Service Initiation/Transition

During this phase, Trustwave SOC analysts partner with the customer to take control of Cb Protection Console Management responsibilities. Service Initiation/Transition occurs in one of two ways:

- Existing Client deployment within the Client's environment – Trustwave will assume management of the existing Client Device(s)
- New Client deployment within the Client's environment – New agents are deployed and configured. After deployment of MAC endpoint agents and standalone management system, Trustwave will assume management of those devices. (Deployment and configuration of Cb Protection endpoint technology is not included within the scope of MAC MSS. For new deployments, there is an expected baseline transition between the deployment entity and Trustwave to ensure smooth transition on the customer's behalf.)

Application Management

All Managed Application Control services are delivered from Global Security Operations Centers (SOCs) located strategically across the globe.

Policy and Configuration Management

Trustwave maintains an overall change control and configuration management procedure for its support infrastructure and associated managed services that support Client-specific implementations. Changes that could affect the operation of Client systems are coordinated with appropriate Client IT staff. Change control is managed by establishing an initial configuration and then using a documented change request procedure and validation exchange for all future changes.

- Submitting configuration change requests is dependent on the type of request.
- Incident tickets for blocks – These requests are created by using the Approval Request feature of the MAC software.
- Non-Block incident tickets or Problem and Service Requests - These types of requests will be submitted via email by the Customer Service Desk. The Customer Service Desk shall be the single point of contact for Authorized Users for all Non-block related Incidents and Service Requests. Valid Service Requests submitted via email by the Customer Service Desk include:
    - security policy change
    - device control policy change
    - new trusted publisher approval
    - reputation-based approval change request
    - custom rule request
    - trusted software /trusted directory change request
    - add/deleted endpoints for managed service
    - evaluate new releases
- Trustwave will perform the following actions as part of the service in accordance with Client's Whitelisting Security Policy:
    - local approval
    - temporary override code generation
    - revocation of local approval
    - local approval policy change
    - global approval

Client Device Access Model

Trustwave will need direct access to the Cb Protection Management console to execute MAC MSS. The customer will retain full administrative access to the Client Management Console Device and provide appropriate access to execute the authorized activity necessary for successful execution of the Managed Application Control MSS. (If Trustwave is not granted full Admin access, Client must create user accounts for every member of the MAC Support Team for the CB Protection server.) Examples of access methods can be found in the **Client Responsibilities** section of this document.

Proactive and Preventative Maintenance Services

Trustwave will analyze Incident trends related to the service and recommend actions to reduce future Incidents. Some of the incident types analyzed include:

- block or file propagation levels
- platform imaging problems
- backup alerts
- database alerts

Trustwave will prepare recommendations on a monthly basis to be reviewed by the Client. These recommendations may include, but not be limited to:

- recommended reputation approvals
- trusted updates
- custom policies
- whitelists additions
- suggested bans

Any recommendations approved by Client will be submitted via a Service Request to authorize Trustwave to take action.

Reporting

On a monthly basis, Trustwave will provide reports to the client to demonstrate trends and levels of service activity. These reports provide visibility in the benefits received from the solution.

Trustwave Responsibilities

- The Trustwave SOC will communicate with Key Contacts only.
- The Trustwave SOC will configure the MAC software in accordance with the Customer's Whitelisting Security Policy and approved Service Requests and Incidents.
- Trustwave will assess the impact of each Service Request and document this information within the Ticketing System.
- On a monthly basis, Trustwave will provide the following reports:
    - infrastructure health check
    - whitelist analysis
    - tickets processed by type
    - resolution timeframe by type
    - significant issues and status

Client Responsibilities

- Provide access to the Cb Protection server to be leveraged with the Managed Application Control MSS through a direct connection to the Cb Protection server (Requires whitelisting the Trustwave IP range on the firewall. If this option is not available, there may be non-standard connectivity options leveraging a "Jump Server").
- Authorized Users must submit their non-block Incident tickets, problem or Service Requests through the Customer Service Desk.
- Block incident tickets will be submitted through the approval request feature within MAC software.
- The client will be solely responsible for all such actions taken and outcomes associated with these activities that are performed in accordance with Client's policies and procedures and any other action taken pursuant to client's directions and instructions.
- The Customer Service Desk will work with the appropriate Client representatives to get approval, re-work the Service Request, or reject the Service Request.
- Approved updates made by the Client to the Customer Whitelisting Security Policy will be reviewed with Trustwave in an agreed-upon meeting with a date clearly communicated at least 14 days prior to when the updated Customer Whitelisting Security Policy is scheduled to be activated. Changes to the Customer Whitelisting Security Policy do not change the services provided by Trustwave within this service description. If compliance with the revised Customer Whitelisting Security Policy requires changes to the scope of this service, or additional costs would be incurred by Trustwave, those changes must be provided for in a separate agreement.

- Agree to an Emergency Policy Review meeting if requested by Trustwave. This could be due to the number of Incident tickets submitted to the Trustwave SOC greatly exceeding the average daily ticket total for the previous month or as anticipated. The Emergency Policy Review will determine the corrective action required to resolve the anomaly in the environment by submitting an emergency Service Request to the Trustwave SOC.
- Submit approved Trustwave recommendations via a Service Request to authorize Trustwave to act.

Roles and Responsibilities

Client will designate the following roles for Trustwave to work with in execution of the service.

Role	Description
Services Point-of-Contact	This will be the key Client contact for Trustwave. This person would be considered the service owner and would be responsible for providing management and review of the service operations. This would also be the person who would be provided the service and compliance reports.
IT Whitelisting Security Policy Administrator	This will be the Customer representative who is responsible for establishing and communicating the Customer Whitelisting Security Policy. The individual will also have the authority to set policies and guidelines documented in the Customer Whitelisting Security Policy and that govern the actions taken as part of the service.
Server/Systems Administrator	This person/team will be responsible for all of the infrastructure administration of the Management Console servers, including database administration, OS patching and hardware maintenance.
Desktop Manager	Define/communicate policies, test interoperability, deploy initial clients, and deploy patches.
Infrastructure/Network Administrator	Ensure firewall and network compatibility.
Windows Active Directory Administrator	Manages security groups and directory model.
Service Desk and Support Key Contact	A designated party that has the authority to make decisions related to these high profile/high impact incidents that generally fall into exception-based categories.

Service Level Objective

Trustwave will provide 24 hours 7 days/week email support to respond to incidents and perform configuration changes in accordance with the following timetable (priorities are defined in the **Definitions** section of this document):

- Priority 1 (Urgent): 4 hours
- Priority 2 (High): 8 hours

- Priority 3 (Normal): 24 hours
- Priority 4 (Low): 72 hours

Exceptions. The following exceptions are excluded from the time used to calculate the Service Level Performance:

- Inability to access the Cb Protection Console due to infrastructure or network outages outside of Bit9's control.
- Customer supplied hardware or software which cannot perform at the necessary levels to meet the service levels, provided MAC advises Customer of the issue, and that such hardware or software does not perform at the levels required to meet the specified requirements.
- Changes implemented by Customer related to infrastructure, functions, or business processes without prior notification to MAC to accommodate such changes with a Service Request or the Change Control Process.
- During the time when an Emergency Policy Review has been requested and scheduled until the time when the emergency Service Request is implemented.
- Changes made via the Cb Protection Console by an individual outside the MAC MSS organization.
- Customer will use best efforts to apply Cb Protection software patches to the Cb Protection application server(s) on a monthly basis, to the licensed endpoints on a quarterly basis and upgrade to the most current maintenance or major release of the Software within six (6) months of its general release date.

For purpose of SLA, the Cb Protection agents running on endpoints are more than one quarter behind or the Cb Protection application server(s) are more than one patch behind for updates ("Grace Period"), then the MAC SLA does not apply and MAC will use best efforts to support the service. If any Incident covered by a documented fix in a patch or maintenance release occurs during the Grace Period, those Incidents will be excluded from the MAC SLA calculations.

Any change to the MAC SLA must follow the Change Control Process.

Definitions

Authorized Users means Users associated with the Supported Endpoints that are included in the service and are authorized to directly interact with the Customer Service Desk and indirectly through transferred Incidents to the Trustwave SOC.

Client Initiation Information means Client-provided information relating to the Client environment and Client's Device policies and rulesets.

Client Management Console Device(s) means an appliance that communicates with and controls the Client's endpoint agents.

Client Device(s) means an appliance or endpoint that analyses network / endpoint, identifies network / endpoint based threats and applies a predefined action.

Change Request means A request for an adjustment to an approved process, Customer Whitelisting Security Policy or system.

Customer Whitelisting Security Policy Means The official documentation, agreed to and approved by Client, of security policies and guidelines that is the sole source for Trustwave related to the handling of Service Requests and Incidents.

Customer Service Desk Customer's point of contact for end-users reporting issues or making requests.

Emergency Policy Review Means an off-schedule meeting with the authorized client contact scheduled within twenty-four (24) hours of the request due to an anomaly within the Client

environment that is generating a high volume of Incident tickets that requires an update of the Customer Whitelisting Security Policy to resolve the situation.

Incidents Means an unplanned interruption to a service or a reduction in the quality of a service caused by the MAC software, known or unknown. (e.g. Block remediation, software approval requests)

Key Contacts means Restricted Client contact list.

Managed Device(s) means the Client's Device(s) and the Client's Management Console Device(s).

Priority 1 (Urgent Severity Level) means an Incident causing a complete and immediate work stoppage with (i) severe measurable business implications; or (ii) effects on a broad group of end users.

Priority 2 (High Severity Level) means an Incident causing significant impairment or delayed work on a business process for (i) a group of end users; or (ii) an individual end user with significant measurable business implications.

Priority 3 (Normal Severity Level) means an Incident not precluding a group of end users or an individual end user from conducting time-sensitive work. There are no immediate and/or serious measurable business implications.

Priority 4 (Low Severity Level) means A routine Incident with minimal to no business impact.

Resolution/Workaround means includes an update to the Incident in the Ticketing System with a note of the action taken to resolve the Incident or the proposed workaround.

Product Update(s) are vendor-provided product and security enhancements to the Managed Device(s) that come in the form of firmware updates or new versions of the software. These updates typically include new or enhanced features, product improvements and security patch fixes.

Provisioning Activities means all activities that must be performed prior to beginning the service to include, but not be limited to, technical access to console, access to the SQL server, Customer Whitelisting Security Policy definition, and completion of Trustwave's Incident Management Process.

Security Operations Center (SOC) means the Trustwave operational and security incident management facilities operated 24 hours a day x 7 days a week, 365 days a year.

RMA Device(s) means a repaired or replaced Managed Device.

RMA Process means the relevant manufacturer's return authorization process for the refund, replacement, or repair during the relevant product's warranty period.

Security Update(s) are vendor-provided security enhancements that add additional protection or update the existing protection engines included with the device. These updates are typically very small in nature but are more frequent than Product Updates.

Service Request means A request by Client to Trustwave's Customer Service Desk.

SLO means the service level objective targets referred to in this Service description.

Supported Endpoints means the list of laptops and desktops that Client has approved to be managed under the service.

Ticketing System means tool used in the logging and tracking of Incidents and Service Requests.

Ticket is a record of activities or alerts and documented within the TrustKeeper Client Portal.

TrustKeeper Client Portal means the Trustwave's TrustKeeper service management web portal.

Trustwave Platform means the Trustwave managed security service infrastructure utilized in providing the Security Device Management service.