ADDENDUM TO SECURITY TECHNOLOGY MANAGEMENT SERVICE DESCRIPTION

IDPS/NGFW Solutions

Service Scope

The Security Technology Management service provides support for IDPS / NGFW solutions with the following feature sets:

- Service Operations activities and responsibilities described in the Security Technology Management service description.
- Integration to core detection capabilities is provided by the Managed Detection service.
- Some service and/or technology features may require an additional charge to the management fee. Supported features availability is dependent on the underlying technology support.

Supported Features

Threat Prevention

Threat prevention, provided by solution vendor, helps protect against viruses (including those embedded in HTML, Javascript, PDF and compressed files), spyware, worms. Add-on capabilities include Drive-by Protection and Behavioral-Botnet Detection.

URL Filtering

URL filtering, provided by the firewall vendor, allows control of access to internet websites by permitting or denying access to specific websites based on predetermined criteria and threat intelligence databases.

Web Content Filtering

Web Content Filtering is used to help prevent computer users from viewing inappropriate web sites or content.

Application Control

Provides Layer 7 Application classification across all ports.

Sandbox Analysis

Using static and dynamic analysis over multiple operating systems and application versions, this feature analyzes samples of files and links and tags items for further investigation. If a sample is categorized as malicious, then it will be automatically contained to prevent contamination.

Virtual Private Network (VPN)

Configuration of encrypted communication links available based on a selected supported device . Support provided for both site-to-site connections and remote user VPN clients.

Network DMZ segments

Configuration of additional network DMZ segments.

Table 1: Supportability For Solution Vendor Subscriptions With Category

	IDPS	NGFW
Threat Prevention	X	X
URL Filtering		X
Web Content Filtering		X
Application Control		X
Sandbox Analysis	X	X*
High Availability	X	X
Remote User VPN Setup		X**
Site to site VPN Setup		X**
Network DMZ		X**

*Requires an extra fee
**VPN & Network DMZ segments – support for one VPN connection and configuration of one local network DMZ segment. Additional support will require an extra fee.

Optional Premium Service Features

Emergency Access to Managed Technology ("Break The Glass")

The "Break The Glass" change service feature is a process that allows Client to make emergency changes on the Technology. In the event a requested change requires a faster response than the applicable SLA defined for an emergency change, the Client emergency contact may contact Trustwave and request direct access to the Technology. Upon such request:

- Trustwave will configure the appropriate access for Client and communicate to Client once access is granted.
- Upon request for "Break The Glass" Trustwave will provide the Authorized Individual with the password
- Client will make the required change and return back access to the technology to Trustwave upon completion.
- Trustwave shall have two (2) business days to review the devices review the configurations and policies of the Managed devices to ensure they align with Trustwave's MSS policies and maintain acceptable security posture
- During the time that the Technology is under Client's control and during the following two (2) business day period when Trustwave conducts its quality assurance review before reassuming control of the Technology, Trustwave shall not (i) be liable for any damages that may arise, or (ii) be responsible for meeting any of the SLA's.

Trustwave responsibilities and acknowledgements

- Configure the list of Client administrative hosts provided by the Client and create rules to allow their access to the Technology.
- Identify emergency change requests and determine whether the request is in-scope with the terms of the Service.
- Perform credential transfer to Client once a call has been received.
- Review Technology for security posture and do quality assurance within two (2) business days after “Break The Glass” protocol completion.

Client responsibilities and acknowledgements

- Provide Trustwave a list of contacts who may perform emergency changes.
- Provide Trustwave with a list of emergency contacts who may request administrative control to the Managed Technology during the Break The Glass process.
- Submit emergency requests using the Fusion Portal and call Trustwave SOC with ticket number requesting immediate action.
- Update support ticket with changes that were performed on the Technology and request to cancel admin access.