ADDENDUM TO SECURITY TECHNOLOGY MANAGEMENT SERVICE DESCRIPTION

# Endpoint Protection Solutions

## Scope, Features and Responsibilities

The Security Technology Management Service provides support for Endpoint Protection (EPP) solutions containing different feature sets.

- Supporting on-premises EPP platforms.
- Trustwave and Client responsibilities are covered under the ”Service Responsibilities” section of the Security Technology Management Service Description document.
- Client should ensure the availability of an active directory for import and synchronization of user and user groups on the platforms.
- Service does not provide direct support to end users. Client shall assume responsibilities for end user helpdesk services. Trustwave will support Client IT staff.
- Some subscriptions may require additional charge to the management fee and are specified in this service description.
- Integration to core detection capabilities is provided by Security and Compliance Monitoring services.

## Standard Supported Platform Capabilities:

### Anti-virus/Anti-spyware

Scan and help prevent virus and spyware attacks on Client computers using current virus definitions.

### File Reputation & App Behavioral Analysis

Zero-day threat and advanced malware protection through the use of, but not limited to, heuristics, reputation data, and file behavior.

### Host-based IPS & Host-based Firewall

Prevent unwanted changes to Client systems by restricting access to files, shares, registry keys, registry values, processes and services.

### Device Control

Block or allow the use of specific ports or types of devices that attach to Client computers, such as USB, infrared, and FireWire devices.

## Add-on Platform Capabilities, if available for the chosen technology subscriptions (requires extra fee):

### Application Control

Whitelist or blacklist applications to allow or block them from accessing system resources, registry keys, files, and folders.

### Web Control

Control site access and downloads by performing URL filtering, or by relying on safety ratings or web categories.

### Host Integrity Checks

Perform checks for the existence of antivirus software, patches, hot fixes, and other security requirements as defined in Client's host integrity policy.

### Unmanaged Device Detection

Configure Client computers to detect unmanaged devices that are introduced into the network. An unmanaged device refers to a device that is not running the EPP client software.

### Sandboxing

Some sandboxes may be integrated with EPP solutions to provide the option of blacklisting malicious files that are detected by the sandboxes. This helps to stop the execution of a malicious file on the endpoints and protect against lateral spread of that file on the network.