SECURITY AS A SERVICE
This service helps you to protect your virtual servers within Calligo’s CloudCore Infrastructure as Service. Traditionally the cloud services provider is responsible for securing the data centre, infrastructure and hypervisor, with the end user organisation responsible for the operating system, applications, users and data. Whilst you have the flexibility to protect your servers using your preferred security product, you can now take advantage of Calligo’s managed security as a service. Using Trend Micro’s Deep Security software, we help you protect your cloud environment from data breaches and business disruptions.

TREND MICRO DEEP SECURITY
Deep Security is a modular product that includes anti-malware, web reputation, firewall, intrusion prevention, integrity monitoring, and log inspection. These combine to ensure server, application, and data security across your cloud environment. Unlike traditional anti-malware solutions most of the Deep Security components are implemented at the hypervisor-level. It leverages Deep Security’s tight integration with VMware to automatically detect new VMs and apply context based policies for consistent security across your cloud.

PREVENT DATA BREACHES AND BUSINESS DISRUPTIONS
- Detects and removes malware from virtual servers in real time with minimal performance impact
- Blocks malware that attempts to evade detection by uninstalling or otherwise disrupting the security program
- Shields known and unknown vulnerabilities in web and enterprise applications and operating systems
- Sends alerts and triggers proactive prevention upon detection of suspicious or malicious activity
- Tracks website credibility and protects users from infected sites with web reputation threat intelligence from Trend Micro’s global domain-reputation database
- Identifies and blocks botnet and targeted attack command and control (C&C) communications using unified threat intelligence from Trend Micro’s global domain-reputation database

Comprehensive security for cloud servers
Protection from data breaches and business disruptions
Shield vulnerabilities before they can be exploited
Eliminate the pain of emergency patching
Demonstrate compliance
Modular, Gold, Silver or Bronze service to meet all requirements
Fully managed Calligo service
Reduce cost and complexity of implementing security controls and policies
A MODULAR APPROACH

<table>
<thead>
<tr>
<th>Service</th>
<th>Bronze</th>
<th>Silver</th>
<th>Gold</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anti-malware with web reputation</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Intrusion prevention</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Bidirectional host-based firewall</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Integrity monitoring</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Log inspection</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

ANTI-MALWARE WITH WEB REPUTATION

- Integrates VMware vShield Endpoint APIs to protect VMware virtual machines against viruses, spyware, trojans, and other malware with zero in-guest footprint
- Delivers an anti-malware agent to extend protection to physical, virtual, and cloud servers.
- Includes improved performance through VMware ESX-level caching and deduplication
- Optimizes security operations to avoid antivirus storms commonly seen in full system scans and pattern updates from traditional security capabilities
- Protects from sophisticated attacks in virtual environments by isolating malware from critical operating system and security components
- Integrates with the Trend Micro™ Smart Protection Network™ global threat intelligence for web reputation capabilities that strengthen protection for servers and virtual desktops.
- Included as standard for Calligo’s hosted desktop service: CloudDesk.

INTRUSION PREVENTION

- Examines all incoming and outgoing traffic for protocol deviations, policy violations, or content that signals an attack
- Protects against known but unpatched vulnerabilities by virtually patching (shielding) them from an unlimited number of exploits, pushing protection to thousands of servers in minutes without a system reboot
- Assists with compliance (PCI DSS section 6.6) to protect web applications and the data they process
- Defends against SQL injection, cross-site scripting, and other web application vulnerabilities
- Includes out-of-the-box vulnerability protection for all major operating systems and over 100 applications, including database, web, email, and FTP servers
- Provides increased visibility and control over applications accessing the network

www.calligo.cloud
INTEGRITY MONITORING
- Monitors critical operating system and application files, such as directories, registry keys, and values, to detect and report malicious and unexpected changes in real time
- Uses Intel TPM/TXT technology to perform hypervisor integrity monitoring for any unauthorized changes to the hypervisor, thereby extending security and compliance to the hypervisor layer
- Reduces administrative overhead with trusted event tagging that automatically replicates actions for similar events across the entire data centre
- Simplifies administration by greatly reducing the number of known good events through automatic cloud-based whitelisting from Trend Micro™ Certified Safe Software Service

LOG INSPECTION
- Collects and analyses operating system and application logs in over 100 log file formats, identifying suspicious behaviour, security events, and administrative events across your data centre
- Assists with compliance (PCI DSS section 10.6) to optimize the identification of important security events buried in multiple log entries

- Forwards events to SIEM system or centralized logging server for correlation, reporting, and archiving.

IMPLEMENTATION

Some components and the design of specific vDCs may require local installs of Deep Security appliances. Where needed it is the client, and not Calligo’s, responsibility to provide the required compute resources.

MANAGED SERVICE
Calligo’s Security as a Service is a managed service. Calligo will implement the required service and manage all the components. This includes monitoring, updating and reporting. Specific customised configurations, such as may be required for PCI DSS 3.0 or HIPAA, are subject to a consultancy fee.

Like all security products the Deep Security service cannot protect against all forms of malicious attack. It should be used in conjunction with other tools and controls to form a layered approach to protection, these include user education, regular data backups and Disaster Recovery services.

DOCUMENT CONTROL
For details visit: www.calligo.cloud/smallprint

Copyright © 2016 Calligo Limited.
Not to be reproduced without permission.