Managed Security

HOSTING Managed Security leads the market in the proactive protection and compliance of your business-critical applications.

EXPLORER

Explorer provides the core security solutions necessary in today's ever-changing environment, including malware protection, firewall management, managed intersite VPN and managed patching on a default schedule.

VOYAGER

Voyager combines many of the services necessary for a secure environment – including all of the components of Explorer – plus a compliance dashboard, access to HOSTING security and compliance analysts, log management and security, intrusion detection and managed patching on a customized schedule.

PIONEER

Pioneer is our most sophisticated security and compliance offering – perfect for companies in regulated industries, industries that are often targeted by malfeasants, or anyone who wants to be certain that their business-critical applications are as protected as possible. It includes all of the components of Explorer and Voyager as well as managed compliance, web application firewall and security-as-a-service for web application firewall.

On the following pages are the individual components included in each service level (marked with the appropriate icons).

Management/Expertise

Managed Patching

Managed patching includes monthly patching for all systems and applications managed by HOSTING to mitigate vulnerabilities. As part of the process, HOSTING identifies available critical and security patches for supported operating systems and tests and deploys patches prior to deployment during the defined maintenance window. Customers are responsible for validating the continued operation of their applications following patch application.

In some instances, HOSTING will deploy patches to customer servers on customized schedules.

Firewall Management

HOSTING provides policy control for network traffic between security zones on the firewall. Our experts configure the firewalls according to customer architecture, monitor the firewalls, and provide break/fix replacement and trouble ticket support. Customers identify policy changes.

Managed Secure Remote Access

This service allows customer IT staff to establish secure connections with a remote, non-public computer network. HOSTING manages remote access VPN settings while the customer is responsible for end-user support and licensing/support for any alternative VPN clients it may choose to deploy.

Managed Intersite VPN

This service allows users/offices in multiple locations to establish secure connections with each other over a public network. HOSTING defines the policies, configures the VPN tunnel, and assists the customer with turn-up and troubleshooting as needed. The customer is responsible for remote endpoint for persistent point-to-point VPNs.

Malware Protection

HOSTING provides standard malware/anti-virus software protection for Windows (Symantec Endpoint Protection or SEP) and Linux (ClamAV) servers. We provide daily exhaustive scans of storage for malicious code and real-time monitoring of files accessed on the server. Customers receive daily updates to the detection engine and signatures.

The customer is responsible for configuring ClamAV services on Linux and using the SEP client interface to exclude files or directories from being scanned. Customers also must schedule custom scanning schedules using the SEP or ClamAV client.

Vulnerability Scanning

HOSTING executes internal and external scans across network infrastructure, server infrastructure, business-critical applications, and web technologies (IPV6, Ajax, SQL injection, etc.). We provide support and answers to vulnerability questions. The customer is tasked with responding to and remediating any vulnerabilities found.

Intrusion Detection

HOSTING monitors network and system activities for malicious activities or policy violations and seeks out security vulnerabilities based on a database of known threat signatures and rules. This service includes a 24 x 7 x 365 Security Operations Center staffed by analysts to monitor and validate the data and translate it into actionable insights for incident response and containment. HOSTING will notify the customer of verified incidents based on escalation procedures and make recommendations when necessary.

The customer is responsible for uploading SSL certificates for traffic that needs to be decrypted and taking action to remediate and close incidents. The customer should notify HOSTING of any networking and architecture changes and advise HOSTING of any unmanaged devices that are added to the service pool.

Security-as-a-Service for Intrusion Detection

Intrusion Detection SaaS includes a 24 x 7 x 365 Security Operations Center staffed by analysts to monitor and validate the data and translate it into actionable insight for incident response and containment. HOSTING will notify the customer of verified incidents based on escalation procedure and make recommendations when necessary.

The customer is responsible for responding to and remediating all incidents.

File Integrity Monitoring

File Integrity Monitoring utilizes an agent on protected servers to monitor the checksum for every file within a protected directory. If the checksum of a file changes, which indicates that the file has changed in some manner, an alert is created and the new hash is sent to multiple virus scanning services to determine if it matches any known vulnerabilities.

The customer must configure additional directories, or create exclusions of files intended to be monitored, and investigate changes associated with their unique components (e.g., application code).

Log Management

HOSTING collects, aggregates and compresses log data locally and then performs all subsequent processing, analysis, reporting, forensics and secure archiving. Logs are retained for one year. The customer is responsible for notifying HOSTING of any networking and architecture and must advise HOSTING of any unmanaged devices that are added to the service pool.

Daily Log Review

This service is a daily log review by analysts – a procedure that is required by many common compliance mandates, such as PCI DSS and HIPAA. Experts analyze event log data, track and escalate issues, and notify customers when any potential issues that might expose the organization to compliance violations are discovered.

The customer is tasked with responding to and remediating incidents.

Security-as-a-Service for Log Management

Log Management SaaS includes 24 x 7 x 365 monitoring and incident escalation along with ongoing tuning and management of the Web Application Firewall.

Web Application Firewall

The Web Application Firewall (WAF) interrogates web traffic in context with how the web applications work, and then deflects or alerts on anything suspicious.

The customer is tasked with remediating and closing incidents as needed.

Security-as-a-Service for Web Application Firewall

Web Application Firewall Security-as-a-Service includes 24 x 7 x 365 monitoring and incident escalation along with ongoing tuning and management of the WAF. The customer is responsible for assisting in the review of false positives to ensure that the WAF is tuned accordingly to develop the whitelist.

Security Support

Access to HOSTING Security & Compliance Analysts

Analysts are available via phone or email to guide customers using security best practices and co-administer policies for HOSTING managed environments. HOSTING Analysts react upon request to implement firewall/infrastructure-level mitigation strategies and answer general security-related customer questions.

The customer is tasked with responding to, investigating and mitigating threats.

Tools and Reporting

Security Posture Reporting

HOSTING Security Posture Reporting includes executive-level summary reports and more detailed “drill down” reports into customer security postures. Reports are accessible via the applicable vendor portals as well as the HOSTING Customer Portal.

Compliance Dashboard

The HOSTING Compliance Dashboard provides customers with a tool to capture their current progress on compliance against specific frameworks (e.g., HIPAA, PCI DSS, SOC, etc.) The dashboard allows customers to identify and document the necessary components of their environments required for compliance so that the chosen tasks can be delivered.

HOSTING security and compliance experts pre-load the dashboard with information relevant to the customer’s compliance requirements and document the necessary components of the environment so that the chosen tasks can be assigned.

The customer is tasked with providing and maintaining all control documentation (unless they have contracted with HOSTING for a level of service that manages this task).

Compliance Management

An IT Risk & Compliance Analyst is assigned to provide proactive technical functions covering the Infrastructure-as-a-Service and Compliance-as-a-Service components of the customer’s environment. The analyst will schedule and deliver recurring customer meetings to review metrics and provide additional business intelligence in key areas. Technical assistance is provided for complex compliance language and concepts.

The customer is tasked with providing oversight to recurring activities to ensure proper prioritization of tasks and containment of effort.