

What does your firewall look like?



Managed Firewall Service

SECURE YOUR HOSTED ENVIRONMENT WITH TERREMARK'S MANAGED FIREWALL & APPLICATION LEVEL FIREWALL SERVICE

Ensure the security of your company's resources with Terremark's Managed Firewall and Managed Application Level Firewall Service, fundamental parts of the Terremark Secure Information Services (SIS) framework.

STOP DATA BREACHES BEFORE THEY HAPPEN

Network firewalls must do one thing; keep unauthorized visitors from accessing valuable corporate and business data. Instead of providing only edge deployed point products that achieve a base level of security, Terremark's Managed Firewall Service embeds firewall security and layers throughout the network and inspects internal traffic to ensure that network firewall security becomes a transparent, scalable, and manageable aspect of your business infrastructure. Using technologies from leading firewall solution providers such as Cisco, Fortinet and Check Point, among others, Terremark's SOC will ensure the identification and blocking of complex threats before they occur.

Terremark's Managed Firewall service integrates with other key SIS features such as SIEM, Log Aggregation, full packet capture, VPN, antivirus, intrusion prevention system (IPS), web filtering, database monitoring, managed patching, anti-spam and traffic shaping to deliver a true multi-layered security platform capable of scaling to multi-gigabit core networks.

HOW IT WORKS

A traditional firewall forms the basic building block of an organization's network security architecture. Terremark only uses technology with superior performance and capabilities to maximize network uptime and protection of business-critical operations.

Rapid adoption of voice, video, collaborative traffic and access to corporate databases is driving the need for firewall engines that operate at very high speeds and that also support application-level inspection. While standard Layer 2 and Layer 3 firewalls prevent unauthorized access to internal and external networks, Terremark's Network Firewall Management

Service can be enhanced with application-level inspection to examine, identify, and verify application types at Layer 7. This prevents attackers using application level hacking from joining the network or attacking databases with key corporate information. Additionally, Managed Firewall Services are critical for PCI compliance

After assisting with the deployment and setup, Terremark Secure Operations Center (SOC) aggregates appropriate firewall events and logs. This allows detection of unusual or suspicious access to the environment, internal and external attempts to scan or map the network, and apparent activities by worms, viruses, Trojans or spyware. In addition, this method allows the detection of activity that represents known, emerging, or suspected attack patterns using both signature and non-signature based methods.

Terremark's security professionals have extensive experience in handling events/incidents, and through the use of our current toolset, we can identify, detect and remediate in real time to minimize impact to your environment.

WHAT'S INCLUDED:

- Procure, install, and configure chosen or provided firewall appliances and engines into Customer's network using standard deployment procedures
- Provision connectivity between the firewall appliances and the security analytics software and management tools
- Customization the Application Layer Firewall to ensure that hackers are deterred and visitors to your site are kept secure.
- Develop customized, flexible security policies that prevent unauthorized access to all resources
- Commence initial baseline learning process to establish standard network, host, and application behavior of the firewall appliances
- Proactive monitoring 24 hours per day, 7 days per week from Terremark's primary and secondary SOC locations
- Ongoing tuning and management of firewall appliance and management application configuration settings to ensure successful discovery and mitigation of all threats
- Industry-leading Cisco, Fortinet, Check Point, Imperva, F5, and Citrix Netscaler hardware is available