TippingPoint®_Secure_Virtualization_Framework

Leading IPS Platform Secures Virtual Data Centers

TippingPoint security solutions are deployed by thousands of organizations worldwide, including many Fortune 1000 and Global 1000 companies. The combination of purpose-built intrusion prevention system (IPS) platforms, enterprise-class management, and industry-leading threat research and security filter development has positioned TippingPoint as a trusted partner for securing the largest data centers.

Moving_Proven_TippingPoint_Security_into_the_Virtual_Data_Center

Many organizations are now migrating their data centers to virtualization in order to take advantage of its promise of improved efficiency and cost savings. Some of these advantages include: system consolidation (including shared storage), reduced space requirements, reduced power and overall hardware requirements, quicker application delivery, improved disaster recovery, and better overall management flexibility.

These advantages cannot be realized if the virtualized infrastructure is at risk of data compromise, does not meet security regulatory requirements, or is at risk of downtime caused by cyber threats. Furthermore, enterprises want solutions that are trusted and have been proven to be effective over time for large enterprise protection. After all, the virtualized infrastructure and its applications are subjected to the same threats that impact the traditional data center. So as organizations accelerate the migration of production workloads and mission-critical assets to the virtualized infrastructure, security requirements become a strategic element of their migration plans.

In response to this need for trusted and proven security solutions specifically for virtualization, TippingPoint is expanding its security and management portfolio to address the unique requirements of the virtualized data center. The TippingPoint Secure Virtualization Framework (SVF) is designed specifically for implementing best-of-breed threat protection for the virtualized infrastructure. It incorporates the advantages of its trusted and proven physical data center solutions into this new environment and provides the following benefits:

- Extends TippingPoint's industry-leading threat research capabilities, breadth of protection, ease-of-use, and automation capabilities to include virtual infrastructure
- Enables TippingPoint customers to extend their existing processes, methodologies, tools and knowledge to secure their virtual infrastructure
- Provides unmatched management, visibility and control on internal virtual networks

Active_Threat_Blocking_for_Virtualized_Data_Centers

Active threat blocking means that filters detect malicious traffic and stop it before it can compromise or damage the virtualized data center infrastructure or its data assets. Unlike detect and alert models that require manual intervention to mitigate detected threats, TippingPoint's solutions enable virtualized traffic to be thoroughly inspected up to the application layer and for malicious traffic to be automatically blocked in real-time without false positives.

TippingPoint®_Secure_Virtualization_Framework

Leading IPS Platform Secures Virtual Data Centers

The highest priority for securing virtualized environments is protection of both the virtual hosts and the virtual machines ("VMs") operating within the hosts. TippingPoint's modern network security platform and intrusion prevention system (IPS) is purpose-built to protect the virtualized data center from ever-evolving, global security threats. These threats target both the virtual hosts and the VMs contained within them. Together with TippingPoint Digital Vaccine® Labs (DVLabs), its premier research organization for vulnerability analysis and discovery, TippingPoint provides the best preemptive protection for vulnerabilities and zero day attacks targeting the operating system (OS), application, services and the most popular virtual platforms including VMware ESX/vSphere, Citrix XenServer and Microsoft HyperV.

Optimize_Protection_with_IPS_Appliance_Offload_or_Local_Inspection

From its many enterprise IPS deployments, TippingPoint has learned that no two networks are alike and that organizations need solutions that can be flexible enough to fit their specific business and risk-requirements. TippingPoint has incorporated two unique approaches into its Secure Virtualization Framework (SVF) to provide deployment and configuration flexibility:

TippingPoint Virtual Controller (vController)
The TippingPoint vContoller takes advantage of the performance characteristics of the purpose-built TippingPoint N-Platform (IPS), delivering the best performance and accuracy in its class for detecting and stopping threats up to the application layer. The vController provides a direct path to the TippingPoint IPS Platform (appliance) to inspect and control VM-to-VM communications. Using the VMSafe API, the vController efficiently directs appropriate traffic to TippingPoint's appliance and its leading threat suppression engine (TSE) ensures the optimal performance and control required in the virtual data center. The vController and IPS Platform also operate in unison to support HA capabilities, including fail over of the vController when HA requirements and configured policy dictate.

TippingPoint Virtual Intrusion Prevention System (vIPS)
The TippingPoint vIPS builds upon the vController by providing a purpose-built IPS virtual appliance for deployments where a physical IPS device is not practical. Some implementations where a virtual IPS appliance may be attractive include:

- 'Office-in-a-box' ROBO deployments where all workloads are virtualized within a single, redundant box
- Disaster recovery (DR) environments
- Public cloud environments where security is offloaded to cloud along with production workloads
- Peak demand capacity due to seasonality where cost constraints dictate a lower cost solution

Full_Virtual_Machine_Isolation_and_Segmentation

In the physical data center, it is a common practice to segment or isolate application servers used in sensitive areas such as HR applications, CRM and their associated database servers. Likewise in the DMZ, systems are isolated, like Web applications and their associated database servers, DNS, e-mail ,etc. When these systems are virtualized, the need for isolation remains; in fact, the need may be greater since these machines now share the same hardware resources. TippingPoint enables traditional networks to be segmented by putting physical appliances between them and, with the N-platform, allows hosts to be segmented without putting an appliance in front of every connection. By utilizing the VLAN translation features of the new platform, IPS inspection can be consolidated for a number of system segmentation boundaries.

After enabling host isolation centrally, TippingPoint applies that same isolation model to the virtualized data center. By tapping into the VMSafe API, TippingPoint is able to isolate VMs within a host or across hosts using either the vController to offload inspection and enforcement, or vIPS for inspection in the virtualized infrastructure. All three methods, including VLAN translation for host

TippingPoint®_Secure_Virtualization_Framework

Leading IPS Platform Secures Virtual Data Centers

segmentation; VController for off-loaded VM and host segmentation; or vIPS for locally executed VM and host segmentation, provide the benefits of stopping threat cross-contamination among data center assets, enabling enterprises to meet security mandates and regulatory requirements such as PCI-DSS.

Unmatched_Virtualization_Visibility_and_Control_with_Reflex_Integration

In addition to the security challenges that virtualization presents, one of the greatest challenges for administrators deploying virtualization is management, visibility and control of the virtualized infrastructure. Considering the ease of creating and moving critical applications within a virtualized environment, this challenge is greatly magnified in the virtualized data center compared to the physical data center.

Recognizing this need, TippingPoint has partnered with Reflex Systems to bring customers the visibility and control necessary to effectively configure, manage and control enterprise security effectively within the virtualized data center. This is in addition to the TippingPoint Security Management System (SMS), which provides a valuable tool for configuring security policy management, monitoring and reporting. TippingPoint's integration with VMware's VMsafe APIs via Reflex System's vTrust and Reflex's Virtual Management Center (VMC) provides many advantages.

- Automatic discovery and graphical mapping of virtual infrastructure topology
- Supports Separation of Duties (SOD) between operations and network/security teams
- Security teams can monitor vSwitch and VM changes to identify tampering or disablement of security controls
- Upgradeable and compatible with full Reflex VMC
- Complete visibility and control over entire virtual infrastructure

Consistent_Security_Policy_and_Enforcement_Between_the_Virtual_and_Physical_Data_Centers

The TippingPoint SMS is an enterprise-class management platform that provides administration, configuration, monitoring and reporting for multiple TippingPoint IPS platforms. Because the TippingPoint SMS provides a scalable, policy-based operational model, it enables straightforward management of large scale IPS deployments across both physical and virtualized infrastructure.

Additionally, SMS enables separation of duties (SOD), which is among the most critical elements of ensuring secure virtual infrastructure. SOD is maintained by providing a unified and centralized IPS management platform for enforcement of security policies regardless of infrastructure type.

The TippingPoint SMS provides granular traffic inspection policy profiles, and enables inspection of any traffic flows according to user requirements, including VM to VM, and Host to Host policy configuration. It also enables consistent policy management across physical and virtualized deployments – from "office-in-a-box" security policy configurations, where remote sites are set up by combining required apps and other elements into a virtualized package, to virtualized web apps, to core network deployments that have their own set of security configuration requirements.

This granular security management combined with the integrated Reflex vCenter and available Virtualization Management Center (VMC) delivers optimal flexibility, visibility and control for comprehensive virtualization security management.

Persistent_Security_for_Mobile_VMs

A key advantage of the vIPS is the ability to maintain the same security policy and IPS enforcement for VMs as they are moved for disaster recovery or for other business reasons to other hardware resources. By placing the IPS within the virtual infrastructure, there is no break in traffic inspection or in active blocking of threats,

and no alteration of the security policies that have been established for a given VM, even as VMs are relocated. This persistent protection and configuration flexibility enables liberal movement of VMs in the most dynamic virtualized data centers. It also enables rapid deployment of VMs into new environments.

Proven, timely threat coverage from DVLabs

TippingPoint's DVLabs team is the premier security research organization for vulnerability analysis and discovery. The team consists of industry recognized security researchers that apply their cutting-edge engineering, reverse engineering and analysis talents in their daily operations. Among IPS vendors, TippingPoint is the undisputed leader in vulnerability discoveries.

The by-product of these efforts fuels the creation of vulnerability filters that are automatically delivered to TippingPoint customers' IPS Platforms through the Digital Vaccine service. The Digital Vaccine Service ensures evergreen (always up-to-date) protection against emerging threats. Digital Vaccines are delivered to customers at least twice a week, or immediately when critical vulnerabilities emerge, and can be deployed automatically with no IT interaction required. Digital Vaccine filters are created to not only address specific exploits, but also for potential attack permutations, protecting customers from zero-day threats to operating systems, services, applications and virtual infrastructure.

Corporate_Headquarters: 7501B North Capital of Texas Hwy. > Austin, Texas 78731 USA > +1 512 681 8000 > +1 888 TRUE IPS
European_Headquarters: Herengracht 466, 2nd Floor > 1017 CA Amsterdam, The Netherlands > +31 20 521 0450
Asia_Pacific_Headquarters: 47 Scotts Road #11-03 Goldbell Towers > Singapore 228233 > +65 6213 5999