



The TippingPoint® Intrusion Prevention System (IPS) Platform achieves a new level of in-line, real-time protection, providing proactive network security for today's and tomorrow's real-world network traffic and data centers. The IPS Platform's next generation architecture adds significant capacity for deep packet traffic inspection, and its modular software design enables the addition of valuable network protection services to its proven intrusion prevention solution. This new best-of-breed IPS Platform redefines intrusion prevention as a foundation for comprehensive network security.

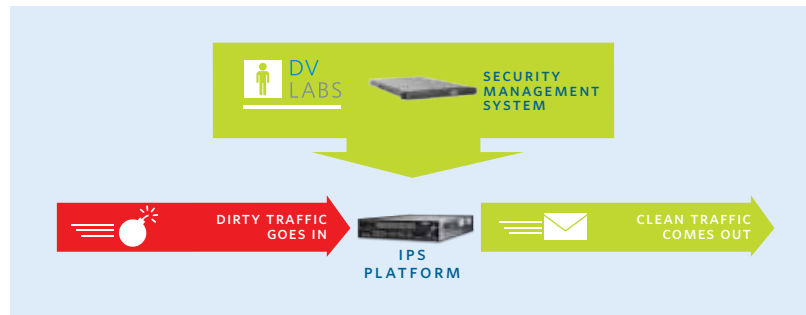


Industry_Proven_Proactive_Network_Security

TippingPoint_IPS_Platform

TippingPoint's broad enterprise customer base, including hundreds of Fortune 1000 customers, is evidence of its success at providing the best proactive defense for the enterprise network—from mission critical data centers, to the network core, to the perimeter, and even at remote and branch office sites. The TippingPoint network security solution, including the TippingPoint IPS, TippingPoint Security Management System (SMS), and its world class Digital Vaccine® Service, protect enterprise networks across the globe.

TippingPoint's_IPS_Platform



TippingPoint's latest technology takes proactive network defense to a whole new level. The IPS Platform offers unprecedented abilities to handle today's and tomorrow's increasing security demands—including the support of multiple IPS filter packs, all new security services, and scalable partner security solution integrations—all while delivering uncompromised performance.

TipingPoint_Intrusion_Prevention_System

Proven_In-Line_Threat_Protection

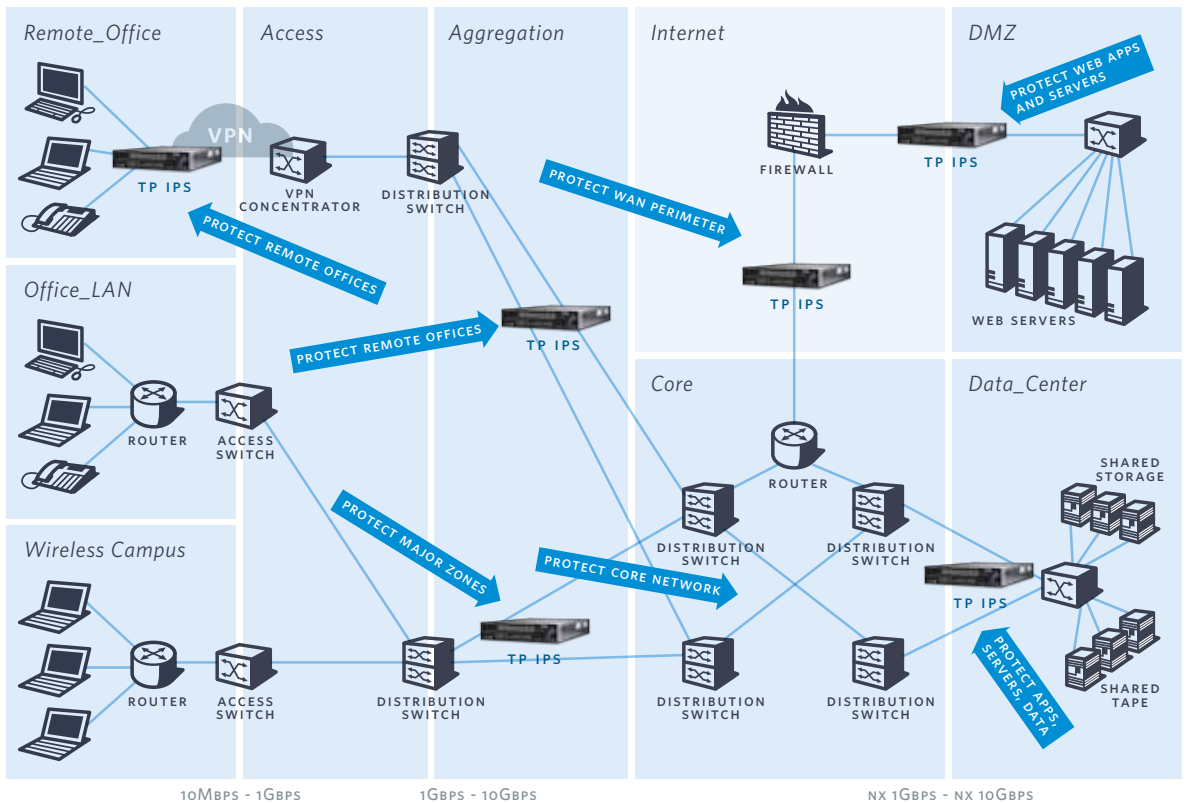
Since 2001, TippingPoint has been laser-focused on creating IPS's that provide proactive, in-line network protection, with an equal focus on ensuring network performance and availability. No network security solution remains in-line if it compromises network performance or uptime. According to a 2008 study by Infonetics Research, more enterprise IPS users trust TippingPoint IPS systems in-line than any other. ¹

New_Extensible_Security_Framework_Provides_a_Foundation_for_Growth

The TippingPoint IPS Platform includes an Extensible Security Framework which has a modular software design built to support faster development and deployment of new:

- > IPS filter packages
- > Security services
- > Partner security solution integrations

Enterprise_In-line_IPS_Deployments



Examples of these new IPS Platform capabilities include: customer-defined IP reputation services; the TippingPoint Reputation Service; the Web Application Digital Vaccine (DV); data leakage protection (filter sets); location-based policies (perimeter, core...) and customer developed filter sets using the TippingPoint Custom Shield Writer (CSW).

The modular design also enables further integrations with partner security solutions such as: vulnerability assessment and vulnerability management (VA/VM), forensics solutions, security information management (SIM) systems and network-based anomaly detection (NBAD) products.

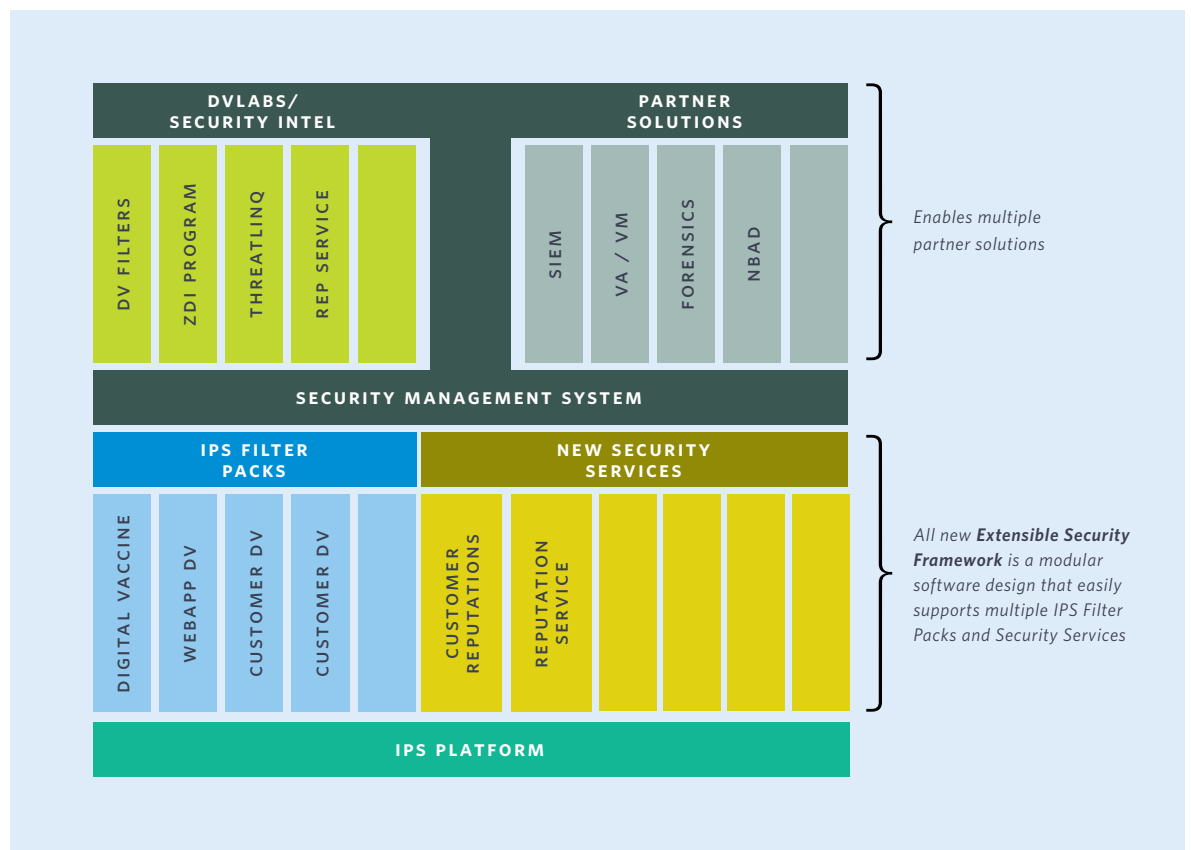
TipingPoint_Intrusion_Prevention_System

The TippingPoint IPS Platform supports a wide variety of traffic types and protocols, allowing organizations to meet the demands of complex, and continually evolving, enterprise network environments. The IPS Platform has uncompromising IPv6 and IPv4 simultaneous payload inspection and support for related tunneling variants (4in6, 6in4, 6in6), as well as IPv6 with VLAN and MPLS tags. There is full support for Mobile IPv4 traffic inspection, GRE and GTP(GPRS tunneling), and jumbo frames. This breadth of traffic coverage gives administrators the flexibility to deploy best-of-breed network protection where it is needed across the network.

New_Threat_Suppression_Engine_Delivers_Years_of_Future_Threat_Protection

The TippingPoint IPS Platform employs a brand new Threat Suppression Engine (TSE) designed to keep pace with the changing and quickly increasing threats and the evolving demands of today’s enterprise networks and data centers.

Enterprise_In-line_IPS_Deployments



TippingPoint’s intrusion prevention systems have set the standard for in-line security and the TSE enables a significant increase in simultaneous deep-packet inspection capacity for supporting future security services such as IP and DNS reputation services. Through a combination of pipelined and massively parallel processing hardware, the TSE is able to perform thousands of checks on each packet flow simultaneously. The proprietary TSE architecture utilizes custom ASICs and high-performance network processors to perform total packet flow inspection at Layers 2-7. Benefits of the new TSE include:

TippingPoint_Intrusion_Prevention_System

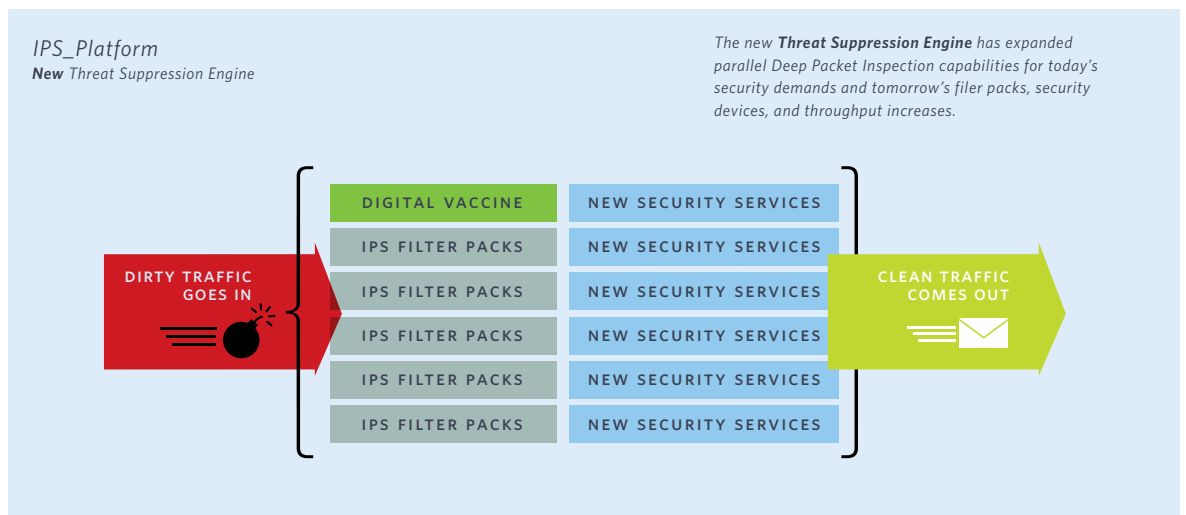
- Increased deep packet inspection capacity from additional parallel processing
- Greater threat protection to handle years of future threats
- Capacity to simultaneously run multiple IPS filter packs and security services

The new TSE provides the capacity to turn on all of the filters an organization needs to block malicious traffic from entering the network.

Proven_Reliability_and_Redundancy_Preserves_Availability_Performance_and_Security

The IPS Platform is designed to deliver unparalleled High Availability. This ensures that network traffic always flows at wire speed in the event of network error, internal device error, or even complete power loss. There

Enterprise_In-line_IPS_Deployments



are two complementary High Availability modes of operation—Intrinsic High Availability and Stateful Network Redundancy—that ensure maximum uptime and availability for both the TippingPoint IPS platform and the Security Management System (SMS) devices.

Several built-in features enable Intrinsic High Availability. First, TippingPoint IPS Platforms have dual hot-swappable power supplies. Secondly, watchdog timers continuously monitor the security and management engines. If an internal error is detected, TippingPoint can automatically or manually fall back to a simple Layer 2 device, configurable per segment. Additionally, TippingPoint offers a Zero Power High Availability (ZPHA) option. In the event of full power loss to the IPS Platform, the interfaces can switch over to the internal (where available) or external ZPHA relay allowing all traffic to pass unimpeded.

Two TippingPoint IPS Platforms can be provisioned using redundant links in a transparent High Availability mode. Because the IPS Platform acts as a “bump in the wire,” does not have an IP address nor participates in routing protocols, redundant TippingPoint platforms can be deployed in existing high availability network designs without changing the network configuration. High availability routing protocols such as Virtual Router Redundancy Protocol (VRRP), Open Shortest Path First (OSPF), and Cisco Hot Standby Router

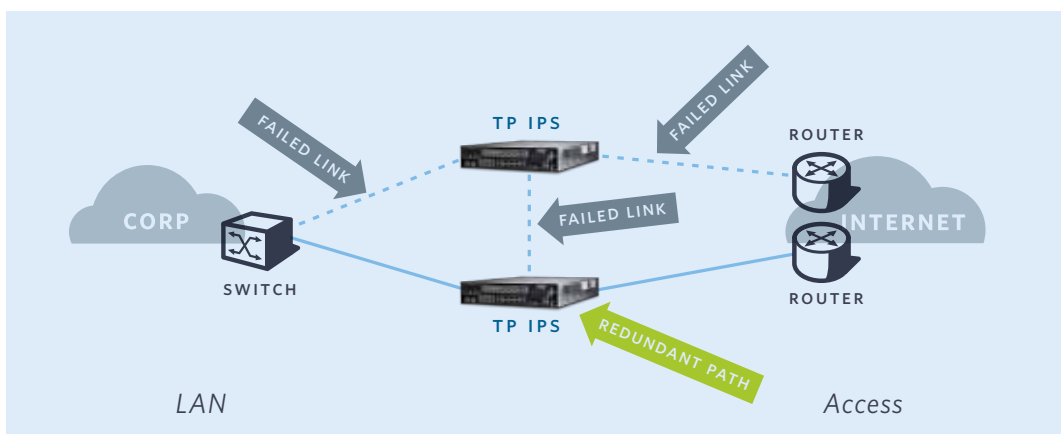
TipingPoint_Intrusion_Prevention_System

Protocol (HSRP) are passed transparently by the TippingPoint IPS and therefore operate equally well with a TippingPoint IPS Platform in-line. The redundant TippingPoint systems can be configured in either Active-Active or Active-Passive modes to appropriately share state information so attack protection is fully maintained during and after network outages.

High_Inspection_Throughput_for_Large_Data_Center_and_Core_Network_Deployments

The TippingPoint Core Controller solution, combined with a pool of IPS Platforms, delivers automated, in-line, 20Gbps inspection to protect network devices, operating systems and applications from attack, with high inspection throughput and sophisticated resource management. The data center or network core are protected,

Redundant_Deployment_with_the_IPS_Platform



without impeding performance, as traffic flows enter the Core Controller and are intelligently managed and then sent to a bank of IPS devices, where traffic inspection and enforcement are performed. Malicious and unwanted traffic is blocked, and clean traffic is returned to the Core Controller for distribution to the appropriate 10Gbps egress link. The solution is designed to manage flows and workloads across the IPS pool and does this in a way that provides 20Gbps of IPS inspection, while also maintaining low latency.

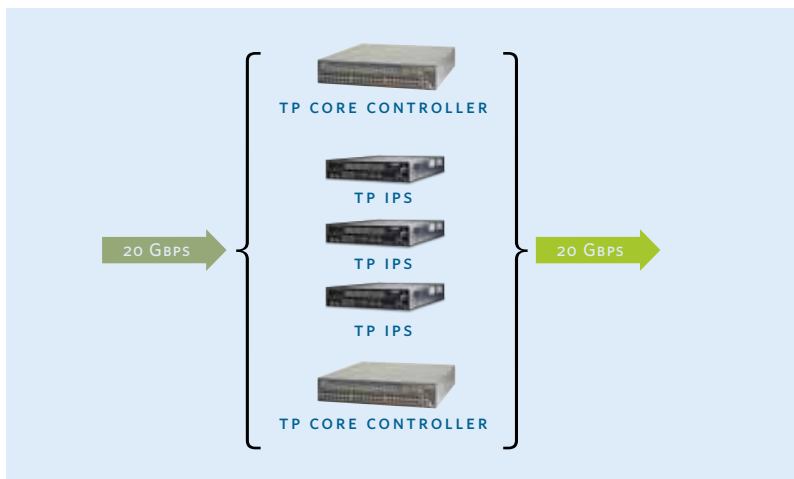
In addition, for customers who would like to grow into the solution, they can start with just the IPS capacity that they need today, and then scale out their inspection capacity over time by expanding the IPS pool as it becomes necessary. Ease of Core Controller deployment and management allow customers to maintain staffing levels and keep overall solution costs low, even for the most demanding data center and network core deployments.

Low_Application_Latency_Ensures_No_Degradation_of_the_End_User_Experience

The IPS platform's unique design ensures that packet flows are fully inspected and move unimpeded through the platform with latency of less than 80 microseconds, independent of the number of filters or security services that are enabled. This eliminates any noticeable application performance impact from an end user perspective.

TippingPoint_Intrusion_Prevention_System

TippingPoint's_High_Performance_Core_Controller_Solution



Unmatched_Filter_Accuracy_Ensures_Legitimate_Traffic_is_Not_Blocked

TippingPoint uses two simple filter writing rules to guarantee filter accuracy. The first is “No False Positives”: Do not block legitimate traffic under any circumstance, and the second is “No False Negatives”: Do not miss any attack on the vulnerability, even when the attacker intentionally tries to evade detection. Achieving these goals is non-trivial. It requires the security knowledge and expertise to write filters to guard the entire vulnerability, not just a known exploit – two very different tasks. TippingPoint creates vulnerability filters that block the various exploits for a given software vulnerability, creating a “Virtual Patch.” This unmatched level of filter accuracy makes the most efficient use of IPS resources and provides customer confidence that a filter will not block legitimate traffic while it is protecting the network from malicious traffic.

Purpose_Built_Hardware_and_Software

Blocking cyber-attacks at multi-gigabit speeds with extremely low latency requires purpose built hardware and software. While others solutions use general purpose hardware and processors that are simply unable to perform without degrading network performance, TippingPoint’s IPS Platform provides thorough threat protection at multi-gigabit speeds, with very low latency.

Real_Time_Comprehensive_Protection

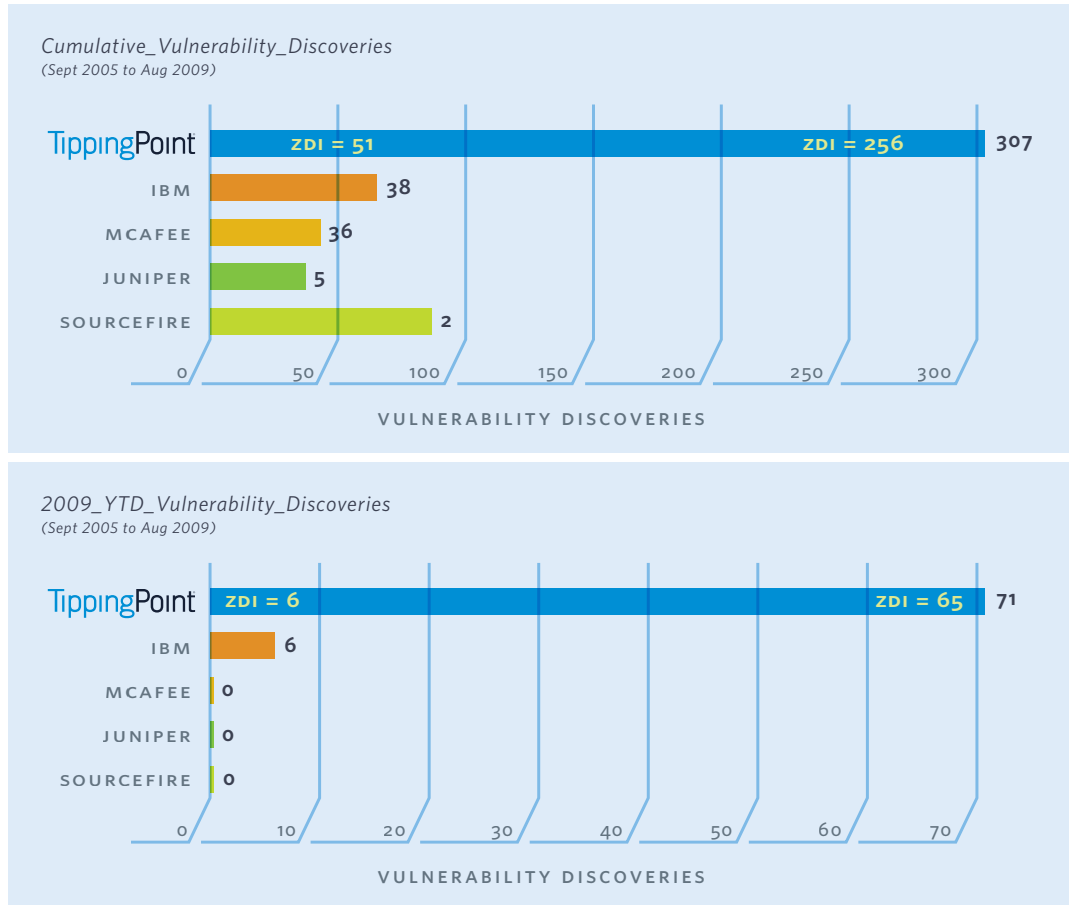
Leading_Security_Research_Team—Digital_Vaccine_Labs_(DVLabs)

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 DVLabs Web site (dvlabs.tippingpoint.com) serves as a portal into the research laboratories headquartered in Austin, Texas. The portal includes upcoming and published advisories as well as blogs, RSS feeds and other security resources. In

TippingPoint_Intrusion_Prevention_System

TippingPoint_Discovers_Eight_Times_More_Software_Vulnerabilities



In addition, DVLabs provides ThreatLinQ, a service that allows TippingPoint IPS customers to view the latest threats across the globe from data that is collected from numerous intrusion prevention systems. ThreatLinQ provides valuable data that can enable enterprises to more effectively hone their network security policy to meet the demands of the latest threat trends. TippingPoint is also the primary author of the SANS Institute @RISK newsletter (<http://www.sans.org/newsletters/risk/>), which contains the latest information on new and existing network security vulnerabilities.

Industry's Fastest Threat Protection Keeps Ahead of the Threats

The Digital Vaccine Service ensures evergreen (always up-to-date) protection against emerging threats. Digital Vaccines are delivered to customers twice a week, or immediately when critical vulnerabilities emerge, and can be deployed automatically with no IT interaction required. Digital Vaccines are created not only to address specific exploits, but also potential attack permutations, protecting customers from zero-day threats.

Zero-Day Initiative Delivers Leading Zero-Day Threat Protection

DVLabs also manages the Zero Day Initiative (ZDI), which is designed to reward worldwide researchers for responsibly disclosing vulnerabilities that they discover. DVLabs passes all vulnerability discoveries and associated research on to affected software vendors so they can develop appropriate patches. In the

TipingPoint_Intrusion_Prevention_System

meantime, TippingPoint creates filters so its IPS customers are protected from potential zero-day attacks. In a 2008 Infonetics IPS Customer Survey, 50 percent of TippingPoint customers reported that TippingPoint provided pre-existing threat coverage (more than twice that of other vendors' customers).

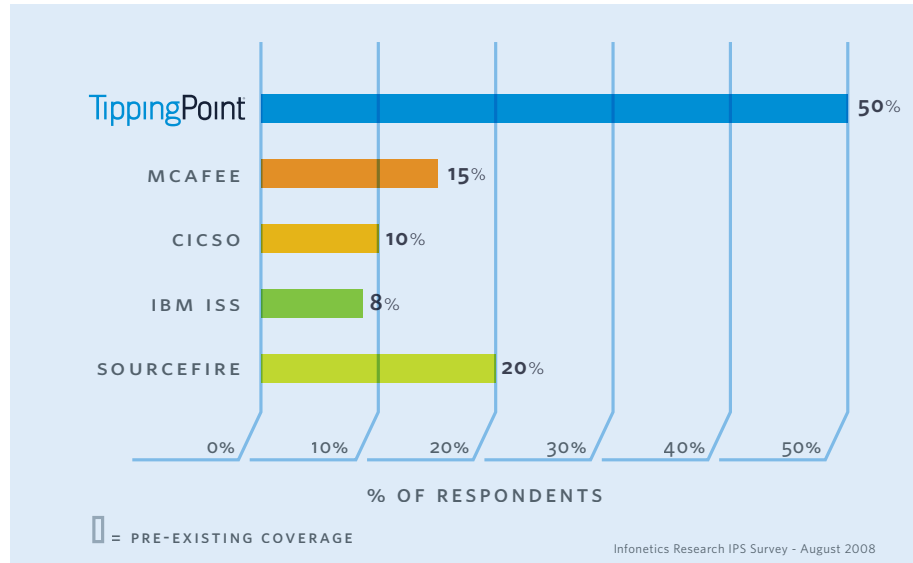
Through TippingPoint's internal vulnerability research and discovery and the Zero-Day Initiative (ZDI), customers are protected against new threats before vulnerabilities are disclosed to the public. For example, in 2008, TippingPoint provided filters for all Microsoft vulnerabilities on average 30 days prior to the public disclosure of those vulnerabilities.

Comprehensive_IPS_Threat_and_Vulnerability_Coverage_for_Best-of-Breed_Protection

The combination of talent, research and security intelligence from TippingPoint's world-class DV Labs research team, over 1,100 researchers in the Zero-Day Initiative (ZDI) program, ThreatLinQ global threat monitoring from thousands of TippingPoint IPS customers (and lighthouses), and security community partners such as the SANS

TipingPoint_Provides_Greater_Zero-Day_Threat_Coverage

Infonetics_2008_"IPS_Customer_Survey"



Institute, CERT, and NIST, and others combine to provide the broadest threat and vulnerability coverage for best-of-breed protection available today.

Network_Operating_System_and_Application_Threat_Protection

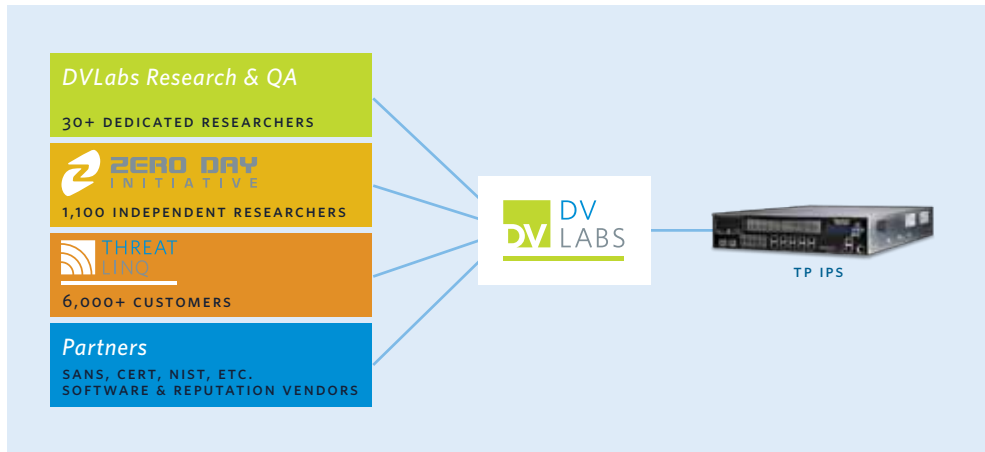
TippingPoint provides the best vulnerability coverage in the IPS industry including protection of network devices, operating systems, enterprise and Web applications, and industrial control system networks. From Microsoft Operating Systems to SCADA and VoIP filters, and many more, TippingPoint provides true network protection for today's complex enterprise IT environments.

Reputation_Service_Eliminates_“Known_Bad”_Traffic

As threats continue to increase, a strategy for eliminating connections to “known bad” Internet sources enables optimal use of IPS resources, and enhances overall network protection. TippingPoint's IPS Platform has a new integrated reputation function. It allows organizations to stop Internet devices known to have malicious code from

TipingPoint_Intrusion_Prevention_System

Broadest_IPS_Threat_and_Vulnerability_Coverage_for_Best_of_Breed_Protection



accessing their internal networks. It can also prohibit access from internal assets to known malware depots, based on DNS or IP address intelligence.

Detailed network security enforcement policy, based on reputation scores and/or “bad” device location or device type is easily configured on the IPS. Through the new Reputation DV service from TippingPoint, automatic updates are sent to the reputation database to reduce or eliminate manual database changes. Customers can also define their own reputation lists to augment the Reputation DV service, or as an alternative to the service.

Minimize_Overall_Security_Costs_and_Complexity

The IPS Platform provides continuous benefits to any network environment: TippingPoint offers organizations the benefits of a comprehensive security solution at a competitive price.

IPS_Automated,_Proactive_Protection_Eliminates_Most_Manual_Event_Follow-up

It is one thing to detect a threat, it is another to detect it accurately and apply policy such as blocking or quarantine without creating false positives. It is no longer necessary to manually respond to myriad alerts (some real and some false), or to clean up after cyber attacks have compromised network servers and workstations. IT security costs are reduced by eliminating ad-hoc patching and alert response, while simultaneously increasing IT productivity and profitability through bandwidth savings and protection of critical applications. These advantages allow IT staff to spend time on strategic IT projects instead of reacting to security breaches.

Eliminate_Emergency_Patching_Processes_and_Protect_Systems_from_Zero-Day_Events

TippingPoint’s vulnerability filters virtually eliminate the need for ad-hoc and emergency patching. By protecting software vulnerabilities, IT staff can implement software patches using a regular, scheduled process instead of costly, disruptive emergency patching. The TippingPoint IPS Platform blocks attacks and allows IT staff to test security patches before deployment.

Most IT teams can’t adequately control all end user desktops. In a recent threat report published by the SANS

TipingPoint_Intrusion_Prevention_System

Institute, TippingPoint and Qualys,² client-side applications are shown to be increasingly more difficult to keep patched due to the growing number of discovered vulnerabilities. In fact, some environments such as service providers or universities have very little control. TippingPoint provides network segmentation to stop the spread of malicious traffic from infected users, while notifying the administrator where attacks originate. This unique and valuable service allows customers to restore efficiency to the security patching process. The burden of emergency and ad-hoc vulnerability patching is alleviated; as IT personnel can apply patches only as required and at regularly scheduled times.

Improve_Current_Network_Performance_by_Recapturing_Misused_Bandwidth

TippingPoint's bandwidth management capabilities stop rogue applications like Peer-to-Peer and Instant Messaging from running rampant throughout the network. By continually cleansing the network of malicious and unwanted traffic, network performance is accelerated for mission critical applications. Blocking malicious traffic and rate shaping rogue applications can increase bandwidth availability, in some cases, by 40-70 percent.

Easy_to_Install_in_Just_Minutes_Minimizing_IT_Burdens

TippingPoint significantly reduces the amount of time and resources needed to maintain a healthy network. The TippingPoint IPS and Security Management System can both be easily installed in the network typically in 30 minutes to one hour. The TippingPoint IPS is designed for network transparency and deployed seamlessly into the network with no IP address or MAC address to immediately begin filtering out malicious and unwanted traffic.

Easy_to_Manage_Solutions_Minimize_IT_Staff_Workload

The TippingPoint IPS solution delivers easy-to-use, best-of-breed management capabilities. The TippingPoint Security Management System (SMS) is a hardened appliance that provides global vision and control of TippingPoint IPS Platforms. The SMS easily discovers, monitors, configures, diagnoses and reports on multiple TippingPoint IPS Platforms. The SMS also features a simple, state-of-the-art secure Java client interface that enables "big picture" analysis with trending reports, correlation and real-time graphs on traffic statistics, filtered attacks, network hosts and services, as well as IPS inventory and health. It also allows integration with third party Network Management Systems, Security Information Management systems (or SIMs), Behavior Anomaly Detection (NBAD) systems, Vulnerability Assessment and Management (VA/VM) systems and other external databases.

The TippingPoint SMS provides a scalable, policy-based operational model that makes even large-scale IPS deployments easy to manage through the TippingPoint SMS dashboard. The SMS dashboard displays an at-a-glance overview of current performance for all TippingPoint IPS systems in the network, including notifications of updates and potential problems that may need attention.

The TippingPoint IPS Platform allows security administrators to manage security policy with fine granularity. Administrators can set specific network security policies by network segment, by VLAN, or by CIDR (Classless Inter-Domain Routing - an expansion the IP addressing system, allowing more efficient address allocation). In addition, by utilizing the IPS Platform's reputation capabilities and the Reputation Digital Vaccine, customers can now incorporate the use of IP addresses and DNS names into their security policy management.

Every IPS also has an embedded Local Security Manager (LSM) and Command Line Interface (CLI). The LSM is a Web GUI management application that provides administration, configuration and reporting capabilities in an easy-to-use, secure Web interface.

TippingPoint_Intrusion_Prevention_System

Automated_Digital_Vaccine_Updates_Minimizes_Staff_Management_Time

The TippingPoint SMS provides automated Digital Vaccine download and distribution capabilities to minimize time required to manage TippingPoint IPS Platform deployments. The SMS allows for manual DV download and distribution, or automated DV download and manual distribution. Since all the DV updates are delivered with Recommended Settings, the majority of TippingPoint customers configure the SMS to automatically download and deploy DV updates to all their IPS Platforms. The result is easy deployment and management of multiple IPS's and Core Controllers for even the most complex network environment.

Demonstrate_Best_Practices_for_Compliance

Automated_Enforcement_of_Internal_Security_Policies

The TippingPoint IPS solutions can be a critical component in any IT compliance program. Today's organizations have to deal with increasingly stringent security policies in the face of an ever changing threat landscape and increasing regulatory requirements. Organizations need solutions that help them enforce security policy on network traffic flows and on network access, ensuring that users and devices have access only to appropriate resources. They also need a way to show auditors how the network is protected from the latest threats.

The TippingPoint IPS solution addresses many compliance program objectives including vulnerability management with the Digital Vaccine service and network monitoring objectives with the TippingPoint Security Management System (SMS). In addition, the TippingPoint IPS may provide a "compensating control" where a requirement is not specifically satisfied with other solutions or processes.

In the face of these stringent security policies and other regulatory demands, TippingPoint IPS provides automated enforcement of network security policies for flows—via the IPS and user, and device-based protection—via an associated network access control (NAC) solution. TippingPoint automates network protection from malicious attacks, provides attack isolation and network discovery of vulnerable devices, and enables traffic shaping to support critical applications and infrastructure.

Robust_Security_Reporting_Provides_Auditor_Details

Reporting from the IPS and SMS allow administrators to show internal and external auditors how the network is protected from the latest threats. In addition to meeting regulatory and internal compliance requirements, organizations can have the best security enforcement available for their networks.

¹ "Customers Show Strong Confidence in TippingPoint IPS Solutions." 22 September 2008.
www.tippingpoint.com. http://www.tippingpoint.com/pdf/press/2008/Infonetics_092208.pdf

² The SANS Institute, TippingPoint and Qualys. "The Top Cyber Security Risks," 15 September 2009.
www.tippingpoint.com. <http://www.tippingpoint.com/toprisks>

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