



FOR IMMEDIATE RELEASE

MEDIA CONTACTS:

Jennifer Lake
TippingPoint
+1 512-681-8111
jlake@tippingpoint.com

Joyce Wady
Connect2 Communications
919-554-3532, x2
joyce@connect2comm.com

TippingPoint Launches New Services To Secure Web Applications

Specialized Digital Vaccine[®] Filters Virtually Patch Vulnerabilities in Custom Web Applications; Enable PCI DSS Compliance

AUSTIN, TX – April 13, 2009 – [TippingPoint](#), a leader in intrusion prevention, today announced availability of its [Web Application Digital Vaccine](#) (Web App DV) services, a two-part approach to address the security threat posed by Web applications. This new set of services enables TippingPoint customers to maximize their security investments, while reducing the risk of attacks through custom-built Web applications. Further, the deployment of the Web App DV service allows organizations to show Payment Card Industry Data Security Standard (PCI DSS) compliance while avoiding the pitfalls associated with the ambiguous protection offered by today's Web application firewalls.

Today's Web applications are used to support a variety of customer and partner transactions and data exchanges, including inventory management and customer relationship management (CRM). These applications often tie into sensitive data assets such as credit card data or personal information. Prior to being "Webified," these applications were set deep in the confines of the corporate network behind layers of security. Now, these applications are being retrofitted to the Web in order to support a larger audience of customers or partners and have moved closer to the perimeter of the network.

"Companies invest a significant amount of money securing various layers of the organization, including the operating system, the network – even the endpoint. However, Web applications – while productive – are still the Achilles heels of most infrastructures," said Rob Ayoub, global program director for network security at Frost & Sullivan. "Since the components of these applications were not originally designed to work together, there are oftentimes weak points associated with the way these are connected. These weak spots represent a greenfield of opportunity for hackers looking to access sensitive data deep in the network."

Improving Web Application Protection with Intrusion Prevention

Customer feedback indicates that Web application firewalls (WAFs) have had issues with false positives when deployed in-line with the network. Instead of ensuring high

availability of the Web applications they were assigned to protect, the firewalls are causing network outages and performance problems. In addition, the constant tuning required to mitigate these false positives adds unnecessary ambiguity to the vulnerabilities the WAFs will ultimately protect against and creates a drain on IT resources and budget.

With the TippingPoint Web App DV services, vulnerabilities in customers' custom-built Web applications are identified and remediated with a set of custom DV filters working in tandem with the standard DV filters to provide comprehensive network protection. The service begins with a scan of the application and associated URLs to determine weak points in the code and possible areas that could be exploited by malicious attacks such as SQL injection, cross-site scripting or reverse proxy. Once the scan is completed, the customer works with TippingPoint's DV Labs team to categorize the vulnerabilities by severity and create a custom filter or set of filters that will be deployed through the TippingPoint IPS.

"TippingPoint's Web App DV services extend the power of the IPS to capture attacks threatening previously unseen security vulnerabilities," said Rohit Dhamankar, director of TippingPoint's DV Labs. "Adding custom filters to the standard filters already included in the TippingPoint IPS provides our customers with another layer of protection for their corporate assets."

Improved PCI Compliance Through Documented Web Application Protection

It is now mandatory in the PCI DSS standard for every organization to provide proof that its Web-based applications are protected from malicious attacks. TippingPoint's Web App DV services not only scan these Web applications for dangerous vulnerabilities, but also create custom filter sets that protect the organization's critical assets and meet the standard for PCI compliance. Additionally, as part of the follow-up scan, the protection from these filters is documented in a PCI report, providing clear validation that the identified vulnerabilities have been mitigated.

Availability and Pricing

The TippingPoint Web App DV Services will be available to customers in May 2009.

Customers have the option of utilizing their legacy Web application scanning programs or TippingPoint's Web application scanning service. The TippingPoint Web application scanning service will be offered at a fixed price and will include the initial scan as well as a post-filter scan to ensure accurate blocking. Custom filters will be priced according to volume ordered and will be delivered to the customer within 48-72 hours following the application scan.

For more information on the TippingPoint Web App DV Services, visit www.tippingpoint.com/webappdv.

About TippingPoint

[TippingPoint](http://www.tippingpoint.com) is a leading global provider of comprehensive network security solutions that address the security and regulatory compliance needs of complex network environments for enterprises, government agencies, service providers and academic

institutions. With the TippingPoint IPS-Secured Network, which includes the TippingPoint® Intrusion Prevention System (IPS) and Network Access Control (NAC) solution, network infrastructure, applications, and critical data are protected from malicious cyber attacks. TippingPoint's 360° approach to network security enables enterprises to enforce security policies across all users, devices, traffic flows and content; while preserving existing infrastructure and ensuring business continuity to help lower total cost of ownership. TippingPoint's security intelligence is powered by DV Labs, TippingPoint's premier team of expert internal researchers for vulnerability analysis and discovery. DV Labs is supplemented by over 900 external Zero Day Initiative researchers. For more information, please visit www.tippingpoint.com, or the press center at <http://www.tippingpoint.com/press>.

About 3Com Corporation

3Com Corporation (Nasdaq: COMS) is a \$1.3B global converged network infrastructure supplier that helps customers achieve business success by delivering solutions that provide exceptional value. The company's H3C enterprise networking portfolio provides best-in-class performance, efficiency and reliability and delivers unparalleled return on investment. Through its TippingPoint division, 3Com is a leading provider of network-based intrusion prevention systems that deliver in-depth application protection, infrastructure protection, and performance protection. For further information, please visit www.3com.com, or the press site www.3com.com/pressbox.

Copyright © 2009 3Com Corporation. 3Com, the 3Com logo, TippingPoint and H3C are registered trademarks of 3Com Corporation or its wholly owned subsidiaries in various countries throughout the world. All other company and product names may be trademarks of their respective holders.

###