Web_Application_Digital_Vaccine®_Service_(Web_App_DV)

Addressing_The_Web_Application_Security_Challenge

The "Webification" of critical business applications has created a unique and sometimes daunting security challenge for IT and security administrators. Applications that were once behind a set of protective "defense in depth" security safeguards and close to the core of the network are now Web facing, and are more exposed to malicious attacks. Given the difficult financial position most organizations are finding themselves in with the struggling world economy, the question being asked is "how do we provide the best protection for these critical Web applications with limited budget and staff?"

IPS

In addition to the critical Web applications that need protection, associated data assets are potentially exposed by these Web applications, including credit card data, private customer information and other sensitive internal data. Today's mission-critical Web applications are used for conducting a variety of customer and partner transactions and the exchange of critical data is commonplace. To provide adequate protection for these assets and facilitate continued productivity, organizations seek to ensure the continuity, integrity and availability within the Web application environment. IT and security administrators are looking to:

- Ensure the high availability of critical business Web applications
- Safeguard Web applications against being hijacked for malicious purposes such as redirecting customers to rogue Web sites
- Protect Web application transaction data that is stored on data center resources

Protecting_the_App_Means_Protecting_the_App_Environment

To achieve the goals mentioned above, it's necessary to protect the Web application environment as a whole. The vulnerable systems within the Web application environment include:

- Routing, switching and load balancing infrastructure including the operating systems on each of these devices
- Web server operating systems
- Supporting applications such as database software, patch management software and database back-up software
- The Web applications themselves (both off-the-shelf and custom developed applications)
- Company and customer data used by the Web applications

The first step is typically to install a basic firewall in front of the Web application data center to provide coarse control over the protocols that can route to servers in the data center and the ports those protocols may use.

Next, organizations typically look at solutions that can provide real-time, effective and broad protection and security policy enforcement for Web application infrastructure given a fixed or limited security budget. The first choice of is usually a dedicated, in-line network intrusion prevention system (IPS) to protect the network, operating system (OS), and application vulnerabilities that may be associated with malicious Web application threats.

Web_Application_Digital_Vaccine®_Service_(Web_App_DV)

Addressing_The_Web_Application_Security_Challenge

TippingPoint_IPS – Security_Enforcement_for_the_Web_Application_Environment

Many organizations today have standard Web applications as well as unique custom-built applications. The use of a vulnerability assessment tool to determine weakness in each Web application may be used. The combination of the prioritization and vulnerability assessment allows companies to develop risk ratings for the different Web applications to prioritize protection efforts. Finally, security enforcement solutions must be identified to address these Web application vulnerabilities. This is where TippingPoint's network IPS becomes even more valuable. The same in-line TippingPoint network IPS that is used to protect the network infrastructure, server operating systems and supporting applications can also provide very broad coverage for standard Web application vulnerabilities, including protection from SQL Injection attacks, PHP File Include attacks, and Cross Site Scripting attacks which account for over 80 percent of all Web application vulnerability attacks today. Unfortunately, many standard filters cannot fully protect custom Web applications because each one comes with its own set of custom vulnerabilities.

Custom_Apps_Need_Custom_Protection

TippingPoint's Web App DV services provide for the creation of custom Web application filters that will block attacks that are directed at the unique vulnerabilities of custom Web applications. The service takes the vulnerability insight provided by a Web application scan, develops specific filters, and enforces protection through the TippingPoint IPS. The combination of standard Web application filters and filters written specifically for one-of-a-kind custom applications closes the gap on Web application security and alleviates the ambiguity, constant tuning and staffing drain that can be associated with standard Web application firewalls. TippingPoint customers report that Web application firewalls have problems with many false positives when deployed in-line to block malicious traffic, causing outages or performance problems instead of ensuring the high availability of the Web applications. As a result, these Web application firewalls are not considered for in-line Web application protection.

Many organizations are coming to the realization that the starting place for Web application infrastructure protection is a network IPS. This is the most effective use of their limited security budget for protecting Web applications and demonstrating the protection of those Web applications for compliance purposes.

Once the in-line network IPS solution is deployed to provide broad protection for the Web application infrastructure, companies may evaluate other security products that can be used in addition to the network IPS to provide further layered security for Web applications, including ongoing application code reviews with associated internal patching processes and/or patch management systems. Companies will always want to patch Web applications where appropriate patches are available or can be developed, but TippingPoint customers report that internal patch development for custom Web applications can take months to develop, test and deploy, and can cost upwards of hundreds of thousands of dollars per vulnerability for large enterprise Web applications. Therefore, patching can be a slow and costly solution. Fortunately TippingPoint network IPS vulnerability filters provide a "virtual patch" for Web applications for either short-term or permanent protection for the vulnerable Web applications.

Comprehensive_Application_Scan_with_Precision_Accuracy

To determine the vulnerabilities that need coverage by the IPS, Web applications need to be thoroughly scanned and assessed for vulnerabilities. TippingPoint's Web application scanning service provides an automated, comprehensive vulnerability assessment with unmatched accuracy and the ability to quickly scan and analyze large complex Web sites and their associated applications. The scan uncovers application vulnerabilities as well as site exposure risk. It ranks threat priority and produces graphical, intuitive reports that indicate site security posture by vulnerability and threat exposure.

The assessment engine automates a proven assessment methodology. The outcome is a vulnerability assessment that is focused on a case-by-case approach. Instead of attempting to check

Web_Application_Digital_Vaccine®_Service_(Web_App_DV)

Addressing_The_Web_Application_Security_Challenge

the same way every time for networks that may have very different requirements, the scan determines the best way to evaluate an application for vulnerabilities like input validation, poor coding practices, weak configuration management and more. By attempting context-sensitive vulnerability checking, the scan can offer complete assessment coverage with outstanding accuracy.

Since all vulnerabilities are not alike, the TippingPoint scan employs a sophisticated intelligence engine to make sure the right priorities are communicated. By analyzing the content, structure and nature of each vulnerability, the resulting reports can focus on the most important threats. From files and resources discovered to source code to scripts, comments, and directory contents, the intelligence engine will analyze all of scan findings to ensure you see the real problems that need remediation.

- Comprehensive site coverage
- Automated scan and assessment
- Detailed vulnerability detection
- Dynamically Identifies and evaluates site content
- High accuracy avoids false positives and negatives
- Complete JavaScript assessment for dynamic content
- Built for safe scanning on production networks
- HTML Report with flexible XML Data
- PCI-DSS Report (Optional)

In addition to assessing application vulnerabilities, the TippingPoint Web App Scan performs an advanced site analysis on the site structure, content and configuration to identify possible exposure risks to emerging threats. This can be critical in determining future security requirements and site architecture planning to mitigate future threats. Exposure is communicated via a security posture rating and qualitative analysis of findings, including a complete catalog of all site resources and their attributes (e.g. forms, cookies, scripts, SQL strings and ODBC connectors, authentication, applets/objects, hidden fields, etc.).

With industry leading reports and flexible data, the scan provides a clear picture of the current Web application security status, so appropriate risk decisions and proper remediation can follow.

Scan/Assessment Features

- SQL Injection
- Cross-site scripting
- Session Strength Analysis
- Parameter Analysis
- SSL Analysis
- Java Analysis
- Authentication Testing
- Source Code Disclosure
- Cross-site Tracing
- Directory Browsing
- Reverse Proxy
- Site Architecture Exposure

Web_App DV – Custom_Filter_Creation_by_TippingPoint_DVLabs

After an organization has completed a Web application scan from TippingPoint, or alternatively through another detailed Web application scanner, the filter creation phase begins. In this phase, as the customer reviews the vulnerability scan results, they have access to the expert guidance of the TippingPoint DVLabs security research team. This expert consultation will enable the customer to set priorities relative to the vulnerabilities uncovered in the scan, and together with the DVLabs team they will determine the vulnerabilities that require special filters. Subsequently, they will receive a proposal from DVLabs for the creation of a custom filter set. Upon approval, the DVLabs team will write accurate IPS filters for the specific vulnerabilities in the customer's application infrastructure. These filters will be deployed to the TippingPoint IPS and will work in concert with the standard Digital Vaccine filters to provide comprehensive coverage – a virtual patch for the customer's Web applications and Web application environment.

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

TippingPoint
www.tippingpoint.com