Technology Alliance: Imperva and ThreatMetrix

Integration of Imperva SecureSphere with ThreatMetrix TrustDefender

Integration Benefits

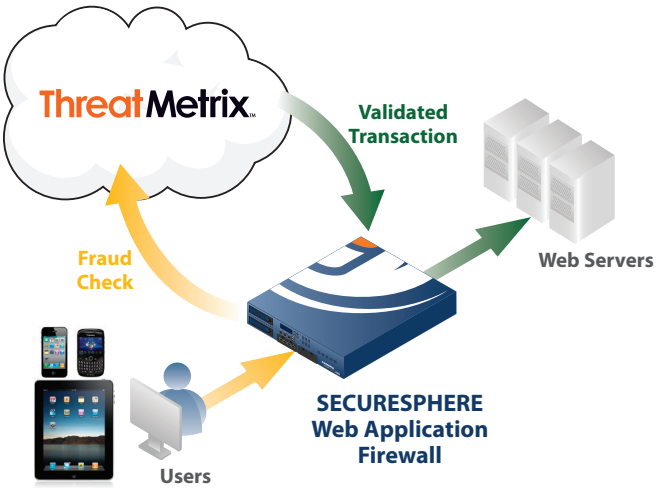
- Protect sensitive transactions like payment authorization, account origination and user authentication
- Reduce fraud investigation costs and chargeback fees and improve reputation
- Correlate fraud and WAF policies for granular detection of fraudulent devices
- Rapidly provision Web fraud security, avoiding manual application integration
- Quickly enforce fraud protection using intuitive Web-based policies
- Allow out-of-the-box integration of malware detection alerts to elevate risk in 3rd party risk engines

Imperva has partnered with ThreatMetrix, the fastest-growing provider of integrated cybercrime security solutions, to help businesses detect and stop fraud. ThreatRadar Fraud Prevention, an add-on service to the SecureSphere Web Application Firewall, empowers businesses to verify payment transactions, new account creation, and online authentication. The integration between ThreatMetrix and Imperva accelerates deployment and eliminates application development costs – not only by streamlining initial fraud prevention deployment, but also by allowing companies to update fraud enforcement policies without modifying Web applications.

Integrated Fraud and Web Application Firewall Management

The SecureSphere Web Application Firewall (WAF) provides powerful custom policies that can correlate multiple attributes for more accurate attack protection. By combining fraud prevention with Web application security policies, organizations can build fraud detection rules that analyze factors such as a suspicious Web request with device identification data provided by ThreatMetrix to accurately detect fraudulent users. In addition, SecureSphere decouples fraud detection from enforcement. It is easy for organizations to create policies that blocked fraudulent devices, monitor devices for a specified period, or redirect users to answer security questions for identity verification.

The Imperva SecureSphere WAF integrates seamlessly with ThreatMetrix's cloud-based fraud detection servers to identify suspicious devices and detect fraud malware. As highlighted in the diagram, when a user accesses a Website protected by SecureSphere, SecureSphere redirects the user's browser to ThreatMetrix's cloud-based servers. The user's browser transparently sends over 250 user and device specific attributes including the IP address, browser and cookie attributes, and packet fingerprint to ThreatMetrix. ThreatMetrix identifies the user's device and determines if it contains any malware that might be used to commit fraud, and then returns a risk score to the SecureSphere WAF, which can then enforce security policies.



Detailed Security Alerts and Reports for Forensics

SecureSphere offers clear, comprehensive security alerts out-of-the-box. These alerts, which capture the full Web request, the Web server response code, source IP address, time and other user details, allow fraud investigators to analyze fraudulent events with ease. More importantly, SecureSphere can track the user name of infected clients, making it easy to follow up with compromised end users. Graphical reports summarize fraudulent activity.

ThreatMetrix TrustDefender

TrustDefender is a cloud-based, real-time solution that combines device identification, identity verification and malware protection capabilities to protect companies from cybercriminals. TrustDefender helps differentiate valuable returning customers from malicious users and determines if customers incur a risk of fraud because of malware on their machines. TrustDefender protects all types of online transactions including account creation, login authentication and payment authorization.

TrustDefender's advanced device identification technology uses multiple methods to expose an individual's intent hidden in the attributes of the user's device. TrustDefender ID is capable of detecting hidden proxies, VPNs, true OS and origin as well as providing satellite, dial-up and mobile wireless detection. With a foundation of intelligent packet and browser fingerprinting, ThreatMetrix TrustDefender ID allows businesses to catch criminal activity with zero false-positives.

TrustDefender's sophisticated malware detection and prevention capability alerts organizations if fraud-enabling malware is present on customers' machines. TrustDefender Cloud detects malicious software like Zeus and its variants, man-in-the-browser, existing and new Trojans that are used to hijack customer sessions. By uniquely combining the ability to identify customer devices with the ability to detect if a customer device has malware, ThreatMetrix helps protect against fraud attempts that are initiated from hackers' machines themselves as well as those that are using bots and infected devices.

ThreatMetrix TrustDefender:

- Slashes chargeback fees and fraud investigation costs and addresses FFIEC compliance
- Offers real-time, non-intrusive fraud prevention
- Analyzes browser, plug-in, and TCP connection attributes to generate a confidence score
- Combines intelligent packet and browser fingerprinting to accurately uncover fraud
- Leverages global intelligence from the ThreatMetrix Cybercrime Control Center, ensuring up-to-date protection

Imperva SecureSphere Web Application Firewall

The SecureSphere Web Application Firewall has transformed the way businesses secure their Web applications and data by automating Web attack protection. With patented Dynamic Profiling technology, SecureSphere automatically builds a model of legitimate behavior and adapts to application changes over time, ensuring that defenses are up to date without manual tuning.

As the market leading Web Application Firewall, thousands of enterprises rely on Imperva SecureSphere to monitor and protect their critical Web applications and data. SecureSphere offers businesses a practical and highly secure solution that stops advanced application threats, automated attacks, and Web fraud. Imperva SecureSphere provides:

- Accurate protection against Web application attacks
- Reputation-based security to stop automated threats
- Web fraud prevention to eliminate malware-based fraud
- Pre-defined and custom correlation rules to block multi-stage attacks
- Transparent deployment and ultra-high performance
- Centralized management and reporting

ThreatMetrix and Imperva provide alert detail and analytics to investigate fraud incidents

About ThreatMetrix

ThreatMetrix is the fastest-growing provider of integrated cybercrime prevention solutions. The ThreatMetrix™ Cybercrime Defender Platform helps companies protect customer data and secure transactions against fraud, malware, data breaches, as well as man-in-the browser (MitB) and Trojan attacks. The Platform consists of advanced cybersecurity technologies, including TrustDefender™ ID, which is cloud-based, real-time device identification, malware protection with TrustDefender™ Cloud and TrustDefender™ Client, as well as TrustDefender™ Mobile for smartphone applications. The company serves a rapidly growing global customer base across a variety of industries, including financial services, e-commerce, payments, social networks, government, and healthcare.

About Imperva

Imperva, pioneering the third pillar of enterprise security, fills the gaps in endpoint and network security by directly protecting high-value applications and data assets in physical and virtual data centers. With an integrated security platform built specifically for modern threats, Imperva data center security provides the visibility and control needed to neutralize attack, theft, and fraud from inside and outside the organization, mitigate risk, and streamline compliance.

IMPERVA®

www.imperva.com