Partner Playbook –Mobile Security

websense®

Elevator Pitch

Websense® TRITON™ Mobile Security is the only cloud security solution that extends your existing security policies to mobile devices while providing a unified web, email, data, and mobile security management console with detailed reporting capabilities. This solution is backed by the Websense® Advanced Classification Engine (ACE) that uniquely analyzes , classifies, and stores mobile apps on the various marketplaces.

The Value Proposition

The enterprise we work in is vastly changing. Workers are becoming more mobile and are starting to adopt newer technologies to conduct business. Many businesses are now allowing employees to bring their own devices to work and access corporate information. In a study conducted by Dasient, researchers found that within 12 to 24 months more than 1 in 20 (5.6%) of Android phones and iPads/iPhones could become infected by mobile malware if fraudsters start integrating zero-day mobile vulnerabilities into leading exploit kits.

Websense® TRITON™ Mobile Security provides:

ACE provides you with ***real-time*** threat and content ratings for protection, productivity and compliance

Contextual Security reduces risk for data theft from mobile devices by encryption and monitoring and controlling information that is sent via email

Websense Mobile App Tracker analyzes, classifies, and stores mobile apps found on various marketplaces.

ThreatSeeker® Network unites over 900***million end points*** for collaborative intelligence by analyzing 3-5 billion requests per day.

Why Websense® TRITON™ Mobile Security?

Integrated Mobile Security

- Single console to create policies and reporting for web, email, and data which can be extended to mobile devices with the click of the mouse

Mobile App Security Intelligence

- Websense Mobile App Tracker has already scanned, classified, and stored 130,000+ apps on the Google marketplace

Websense Security Labs

- Over 100 researchers found in four locations, focusing on four areas of security: web, email, data, and mobile

Product Capabilites

- Combining industry leading web, email, and data security to provide you with a complete mobile security solution with popular MDM security features
- Mining applications from several marketplaces and the web, decompiling them and extracting features, and storing the results
- Single click policy setting capabilities combined with over-the-air device provisioning to allow for a simple installation and integration
- Over 8 years of R&D to provide customers with industry leading, real-time protection from advanced threats and malware on mobile devices

Why Websense?

- 15+ years of web, email, data security experince
- Over 900 million users united through ThreatSeeker intellengice
- Enterprise-class data threat protection to provide containment security
- Real-time monitoring of social content 24/7 for the best possible protection
- Partnership with Facebook, feeding ACE and ThreatSeeker Network from end users around the world
- Worldwide operation centers with mirrored redundancy in the cloud for automatic backup

Sound Bites

"Websense administrative portal is clean and straightforward."
-EMA Radar Report for Message Security Services, June 2011

Leader quadrant for Secure Web Gateway and DLP
–Gartner SWG & DLP MQs, 2011

"All security and reporting features are seamlessly integrated into a single unified management console."
– Binary Test Product Review, Q2 2011

Websense Mobile App Tracker has profiled over 130,000 mobile apps on the market
– Websense Security Labs

Partner Playbook –Mobile Security

websense®

Managing Objections

Websense is late to the MDM market, and I already have a MDM solution

- The Websense® TRITON™ solution is much broader than a simple MDM solution. Websense is a mobile security vendor, providing industry leading web, email, and data security for mobile devices. This level of technology is more sophisticated than a MDM solution, thus taking longer to develop. They also have a Mobile App Tracker built into ACE and ThreatSeeker , further adding to the depth of its' mobile security knowledge.

Websense doesn't have expertise in end point security like McAfee or Symantec.

- Security is evolving as are the devices being leveraged in everyday business. Due to the nature of the emerging mobile devices and the vast variety of operating systems, end point solutions will not scale and will be replaced by cloud solutions. Also, researchers have found that it is not the device that needs to be secured, but the data. Websense is an expert in end point DLP, awarded with the Gartner Content Aware DLP Leader for five years in a row.

Websense is a URL filtering vendor, how can you have cutting-edge mobile security?

- The Websense Security Labs works around the clock, mining mobile apps from several marketplaces and the web, decompiling and extracting their features, and storing the results. Also, ACE and ThreatSeeker Network work in real-time and are equipped with machine learning. To add to this intelligent network, we have partnered with Facebook, giving us the largest threat detection network in the industry.

Customer Pain Points	Discovery and Measurement Questions
Unsecured mobile devices in the work place	▪ Do you allow employees to use personal mobile devices for business use? ▪ How many devices are accessing your corporate network today? ▪ What is your primary concern with allowing non-corporate issued devices in the workplace? ▪ What are you doing to seccure those devices and protect your corporate data?
Malware and infected mobile apps	▪ How are you protecting mobile users against malware, data loss, and loss of device? ▪ What are you currently using to protect from data theft on mobile devices? Is it working? ▪ How are you inventorying mobile apps that are being downloaded to devices on your network? ▪ How do you determine if new or updated apps contain malicious content? ▪ What is your policy around phones or tablets that have been jail broken?
Data Loss Prevention	▪ What concerns do you have about sensitive information leaking from mobile devices beyond the corporate perimeter? ▪ What are you doing to protect confidential information being accessed on mobile devices? ▪ Do you have a way to limit the amount and type of data that is being accessed on mobile devices?

A Changing Environment

- Bring Your Own Device (BYOD) to work is a new trend in the marketplace
- Employees are requesting to access corporate information on personal devices
- Mobile threats are on the rise, malware attacks have risen over 400% in the last year