Cloud-Based Malware Attack Detection & Mitigation Service

Radware's Cloud Malware Protection service protects global enterprises from targeted malware attacks and removes the uncertainty in which IT security teams operate. Delivered via the cloud, the service provides continuous visibility into compromise and risk by automatically detecting active malware attacks inside the network and measuring performance against simulated potential attacks. Cloud Malware Protection delivers answers not questions, supplying accurate actionable information about compromised devices to SOC teams and existing security systems. Organizations worldwide use Radware's Cloud Malware Protection to identify and mitigate known and unknown security threats.

Malware Attack Detection

- Identifies active infections that have evaded perimeter-based prevention systems, reporting exactly which devices and users are infected by which malware
- Reports only "true positive" infections…no chasing false positive alerts. Reduces detection, containment, and remediation time from weeks to 1-2 days per incident
- Utilizes a combination of big data analytics, machine learning and external context to generate unique malware profiles and identify known and unknown threats
- Detects evasive malware behaviors designed to defeat real-time detection solutions
- Leverages crowd-sourced threat data from Radware's global network to allow fast and reliable attack detection and remediation, meaning an infection identified in one domain will benefit others

Figure 1: Malware Attack Detection Dashboard

Proactive Protection

- Constantly enriches Radware's C&C Servers database by gathering, sandboxing and analyzing data from the growing Radware community of enterprise users and multiple other sources
- Provides API to query the C&C Servers database and automatically feed existing security solutions with accurate up-to-date information about known and zero-day C&C servers
- Improves the efficacy of existing prevention layer solutions by analyzing their logs and feeding accurate threat data back
- Provides integrated threat visibility with leading SIEM solutions

Audit

- Provides continuous visibility on prevention systems performance and response to new attacks. Determines how well your secure web gateway (SWG), next-generation firewall (NGFW), or proxy would do at preventing the latest, real world malware attacks from succeeding in communicating with their perpetrator's C&C servers.
- Uses advanced simulation methods to run precisely mimicked sophisticated exfiltration techniques such as Domain Generation Algorithm (DGA), Low and Slow Communications, Spoofed headers and more, all reverse-engineered from actual in-the-wild malware.
- Speedy & Safe: In mere minutes, Radware Cloud Malware Protection's Javelin Test measures if your gateway is vulnerable to, or effective against inside-out attacks without introducing any actual bad actors to your network

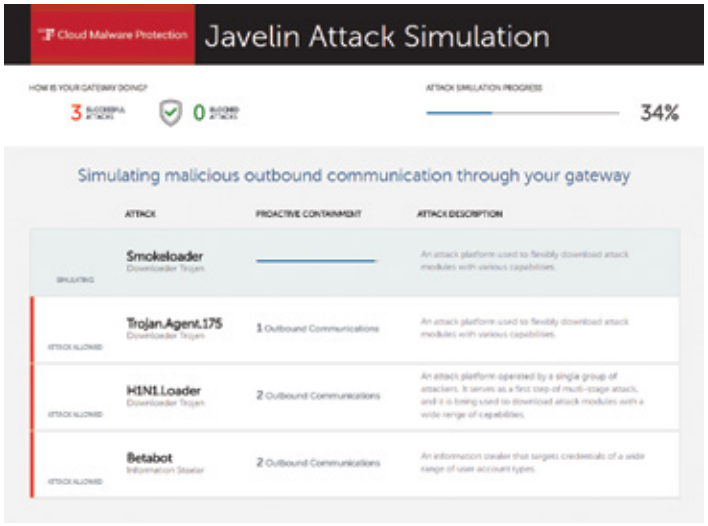

Figure 2: Audit Section – Javelin Attack Simulation

- Provides actionable results your security specialists can use immediately to update existing prevention layer components
- Automated Gateway Update Service resolves the gap between your gateway's prevention capabilities and the latest threats revealed by Javelin Attack Simulator.

About Radware

Radware® (NASDAQ: RDWR), is a global leader of application delivery and cyber security solutions for virtual, cloud and software defined data centers. Its award-winning solutions portfolio delivers service level assurance for business-critical applications, while maximizing IT efficiency. Radware's solutions empower more than 10,000 enterprise and carrier customers worldwide to adapt to market challenges quickly, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com.

Radware encourages you to join our community and follow us on: Facebook, Google+, LinkedIn, Radware Blog, SlideShare, Twitter, YouTube, Radware Connect app for iPhone® and our security center DDoSWarriors.com that provides a comprehensive analysis on DDoS attack tools, trends and threats.

Certainty Support

Radware offers technical support for all of its products through the Certainty Support Program. Each level of the Certainty Support Program consists of four elements: phone support, software updates, hardware maintenance, and on-site support. Radware also has dedicated engineering staff that can assist customers on a professional services basis for advanced project deployments.

Learn More

To learn more about how Radware's integrated application delivery & security solutions can enable you to get the most of your business and IT investments, email us at info@radware.com or go to www.radware.com.