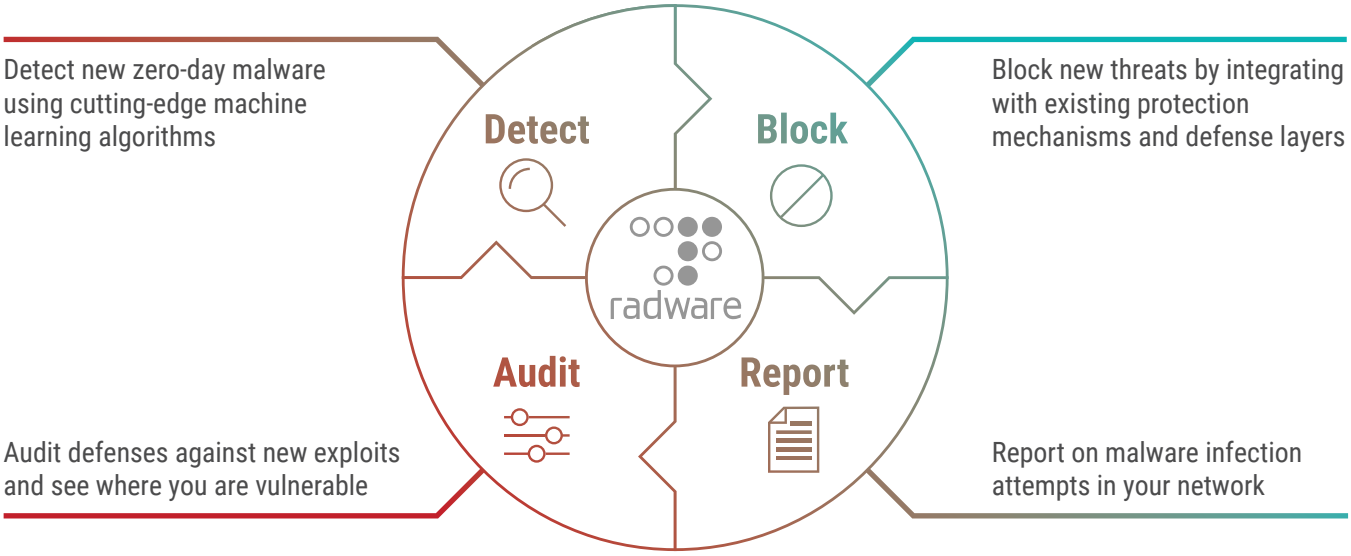
Zero-Day Malware Protection for the Enterprise Network

Every day is zero-day when it comes to malware. Nearly 50% of malware targeting enterprises are zero-day exploits that are not recognized by existing signature-based defenses. With malware being used in the majority of data breaches, organizations are increasingly exposed to the risk of information theft and financial loss.

Radware Cloud Malware Protection Service defends against zero-day malware by analyzing Internet communication data collected from a global community of 2 million users, using patented machine-learning algorithms, as well as unique sandboxing technology examining over 100,000 malware samples a day, to detect previously unknown malware based on their unique communication behavior patterns.



How Radware Detects Zero-Day Malware That Evades Other Defenses

Technology

Designed by a team of data-science experts, 70+ unique machine-learning behavior analysis algorithms detect zero-day malware by analyzing their communication patterns

Community

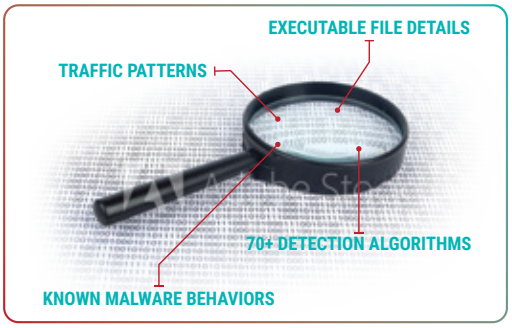
A global community of 2 million enterprise users worldwide collects live intelligence, analyzing over 2 billion communications each day and more than 500 TB of data every week

Data

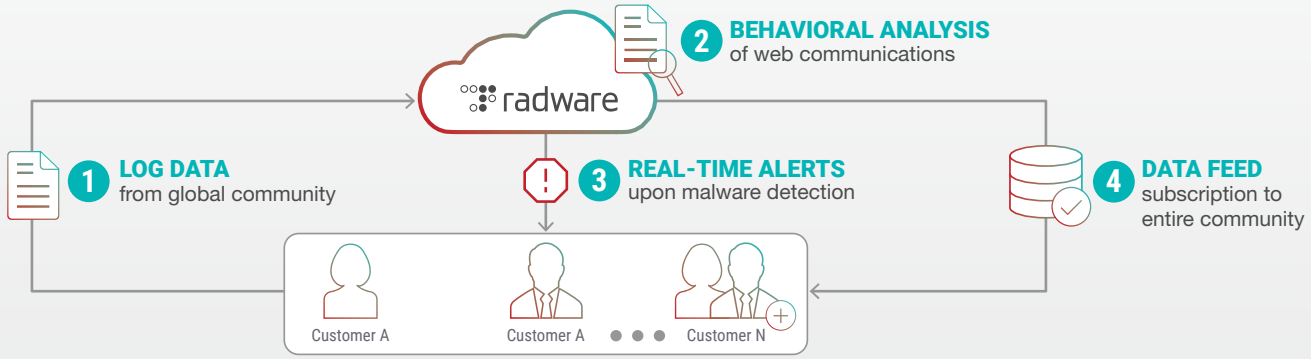
Ground-breaking technology and massive community gives unparalleled breadth and depth of data, aggregated over extended periods of time, to detect new malware quickly and consistently

Case Study: Beating the Nymaim Zero-Day Malware

Nymaim is an example of fast-adapting next-generation malware. It uses multiple advanced evasion techniques such as host spoofing, payload encryption, domain generation algorithms and randomized request paths, which make it immune to detection by all traditional signature-based secure web gateways, IDS/IPS systems and next-gen firewalls (NGFW). By leveraging its community, data, and technology to detect traffic anomalies and identify similarities to existing malicious malware, Radware is able to continuously identify new Nymaim variants infecting customer networks in real time.



Radware Cloud Malware Protection Service Flow



Service Features of Radware Cloud Malware Protection

Proactive Protection from Zero-Day Malware

- Subscription to a continuously updated database of malicious Command & Control (C&C) domains and IP addresses, drawn from global community
- Real-time alerting when zero-day malware is detected in your network, with specific incident details such as identity of infected endpoints, incident history, malware risks and capabilities and supportive forensic information
- Notification on infection attempts, providing threat visibility for identifying points of vulnerability and sources of attack

Powerful Auditing Tool

- Continuously simulates attacks by latest malware currently in the wild without introducing bad actors into the network, and with immediate results
- Measures existing infrastructure resilience to attempted malicious outbound communications and compares gateway performance to global benchmarks
- Verifies the integrity of zero-day C&C data feed integration into existing defense layers

Integration with Existing Defenses

- Vendor-agnostic solution providing integrated threat visibility with existing Secure Web Gateway, NGFW and SIEM solutions
- Provides API to query the C&C server database and automatically feed existing security solutions with updated information about known and zero-day C&C servers
- Improves the efficienty of existing prevention layer solutions by analyzing their logs and feeding accurate threat data back

Easy to Use Management Interface

- 100% cloud solution, no installation of software or hardware required at any level
- Rich centralized dashboard to display new threats, analyze results, and gain visibility across the spectrum
- Easy-to-read executive reports with concise details on infection incidents, malware activity, and actionable steps to prevent data breaches