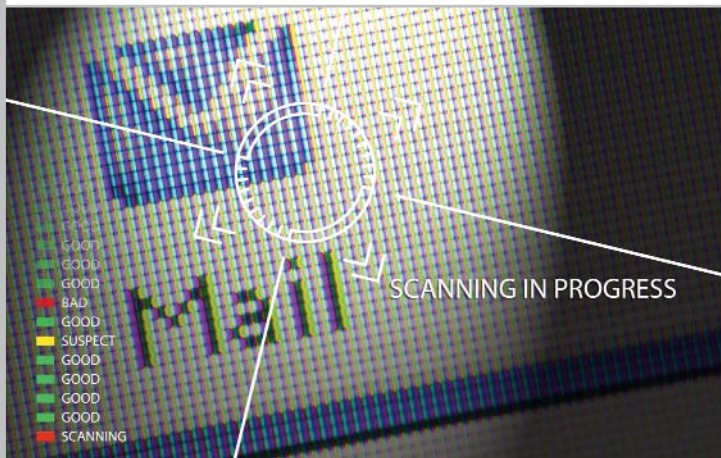


RShield™ Email



Targeting advanced zero-day
email attacks that bypass
conventional security controls

Key Features and Benefits

- Behavior-based detection that can identify advanced zero-day malware that signature-based solutions miss
- Interoperates with existing mail infrastructures
- Scalable to the largest enterprise networks
- Operates in active IPS or passive IDS mode
- Advanced detection methods and algorithms operate in faster than real-time clock speeds
- Extensible detection framework allows end-user extensions to detection methods
- Automated forensics collection for malicious files
- Workflow driven processes decrease malware analysis time

Traditional malware detection approaches, such as signature-based anti-virus, spam gateways and personal firewalls, fail to adequately address sophisticated, socially engineered, polymorphic, zero-day and targeted malware attacks. As a result, these kinds of attacks have proven very effective in eroding the perimeter security of many high-value networks, such as those within the government, defense contractors, the banking industry, and others. RShield Email, a Raytheon solution, addresses these threats.

RShield Email performs behavior-based analysis on attachments and/or embedded URL content by opening/ executing them in a safe sandbox environment as part of the mail delivery process in either an active or passive mode of detection.

This method is more effective in identifying zero-day malware than traditional signature-based anti-virus techniques because many of these attacks utilize custom binaries designed for and deployed to attack a specific target. Such sophisticated attacks usually include advanced packing, encryption and polymorphic techniques to make signature-based detection even more difficult.

Desktop and network level firewalls have proven ineffective because advanced malware is often designed to circumvent them, either by disabling them at the host level or by masquerading as otherwise legitimate traffic at the network level.

RShield Email offers a proactive method of countering this threat.

Complements Existing Mail Controls

RShield Email is intended to enhance existing email filtering technologies such as anti-spam and anti-virus to prevent malicious content. The existing controls act as a noise filter, allowing RShield Email to work on the more advanced threats.

MTA Interoperability

RShield Email is designed to be inserted inline with an existing email infrastructure through insertion of inline commercial Mail Transfer Agent (MTA) or it can be called directly by any MTA that supports the Milter interface.

Enterprise Scalability

RShield Email scales from small mail systems to the needs of large global enterprises including, multi-site, load-balanced, and massively-scaled user environments.

Flexible Operating Modes

RShield Email operates on attachments and/or embedded URLs in either a passive Intrusion Detection System (IDS) mode that passively scans and alerts or in an active Intrusion Prevention System (IPS) mode, which prevents malicious content delivery.

Mail Quarantine Options

As a configurable option, RShield Email either deletes, quarantines or sanitizes malicious emails.

Hypervisor-Level Behavioral Detection

RShield Email core detection capability is based on a proprietary sandbox technology specifically tuned for processing email attachments and analyzing URLs.

Extensible Detection Capabilities

RShield Email core detection capabilities support multiple operating systems and application configuration baselines simultaneously. Additionally, RShield Email provides a generic detection framework that is used to tie in third-party modules and advanced end-users can make use of this framework to add-on their own internally developed detection methods.

Performance Optimizations

RShield Email optimizes performance and scanning of emails with:

- Advanced scheduling and disposition algorithms
- Multiple virtual machines on the same hardware
- Raytheon's TimeWarp capabilities for faster than real-time detection
- Near-instant baseline reverts following detections
- Flexible and scalable hardware

RShield Email is optimized to provide the ability to open and analyze malicious attachments at speeds that allow RShield Email to run inline with minimal impacts to mail delivery timelines, even in IPS mode.

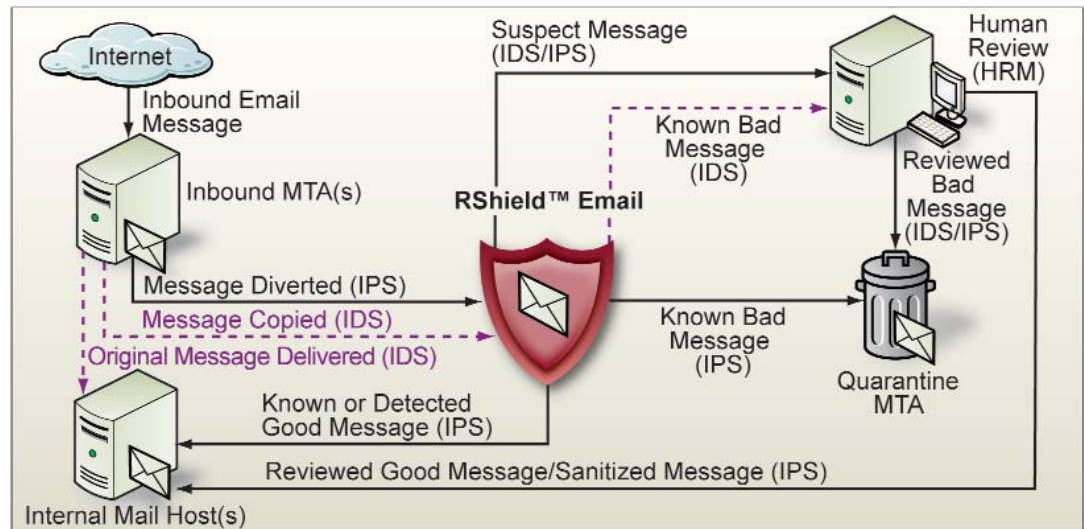
Automated Forensics

RShield Email has a significant advantage over traditional antivirus and signature-based solutions by providing forensic level capture and analysis as part of the detection engine.

Workflow-Driven Incident Handling

RShield Email includes Raytheon's Human Review

Manager (HRM) as a back-end analysis and workflow system. This provides a flexible and completely customizable framework for integrating RShield Email into an organization's existing incident handling process. RShield Email provides the ability to notify appropriate personnel of incidents via email and Simple Network Management Protocol (SNMP). Additionally, custom HRM widgets can be developed to support even the most complex incident handling processes or provide additional post-detection automated malware analysis.



For further information contact:

Intelligence and Information Systems

P.O. Box 660023
Dallas, Texas
75266-0023 USA
iiscommunications@raytheon.com

www.raytheon.com
Keyword: zeroday

Customer Success Is Our Mission is a registered trademark of Raytheon Company.