RETARUS E-MAIL SECURITY

Protecting your business one email at a time

Challenges

Organizations must protect themselves against known and unknown malware, advanced threats, and targeted attacks that use email to gain access to their IT infrastructure.

Answer

Retarus and Palo Alto Networks have teamed up to deliver an end-to-end email security service that includes customizable defense mechanisms to meet your organization's security needs.

Benefit

- Protects your entire email infrastructure.
- Sends warnings for fraudulent emails.
- Stops attacks in action before they do harm.
- Complies with regulations for encryption and archiving.
- Prevents the loss of confidential information from your network.

Introduction

Email attacks are becoming more precise and intelligent, surpassing the capabilities of conventional defense mechanisms and posing a continuous risk to companies. To protect themselves against intelligently executed attacks, organizations need equally intelligent protection.

Powered by Palo Alto Networks®, the Retarus E-Mail Security service blocks sophisticated malware, such as viruses, ransomware and other threats. The innovative Retarus® queue-less design analyzes incoming emails without temporarily storing them. Unwanted emails, including spam and phishing messages, are filtered while other emails are received without delay. To ensure maximum security, virus scanners and filter methods are continuously updated. You receive detailed information, enabling you to stay in control of your electronic communications. Data is processed in Retarus' data centers in accordance with local privacy policies.

Stop Attackers Before They Stop Your Business

The more targeted the attack, the more targeted the course of action against the attacker must be. Retarus has developed defense mechanisms that are perfectly harmonized to protect you from attacks:

- **Advanced protection against advanced threats:** Retarus offers four virus scanners as well as deferred delivery scanning, sandboxing, time-of-click protection and CxO fraud protection.
- **Targeted protection from targeted attacks:** Retarus checks each incoming email for criminal content. For example, spear phishing attacks utilize fake sender addresses, which Retarus calls CxO fraud. Retarus prevents phishing by checking links the moment users click and obstructing access to untrustworthy sites.
- **Identify unidentified threats with Postdelivery Protection:** Retarus' patent-pending Patient Zero Detection technology can identify malware in emails that have already been delivered and warn recipients as soon as the matching patterns exist.

The Industry's Most Advanced Analysis and Prevention Engine

Retarus E-Mail Security is powered by Palo Alto Networks WildFire® cloud-based threat analysis service, the industry's most advanced threat analysis and prevention engine. As a key component of the Palo Alto Networks Security Operating Platform, WildFire delivers on-premise analysis, detonation and automated orchestration to prevent zero-day exploits and malware. The private cloud architecture of WildFire allows you to meet privacy and regulatory requirements while still benefiting from the shared threat intelligence of more than 24,000 WildFire cloud subscribers.

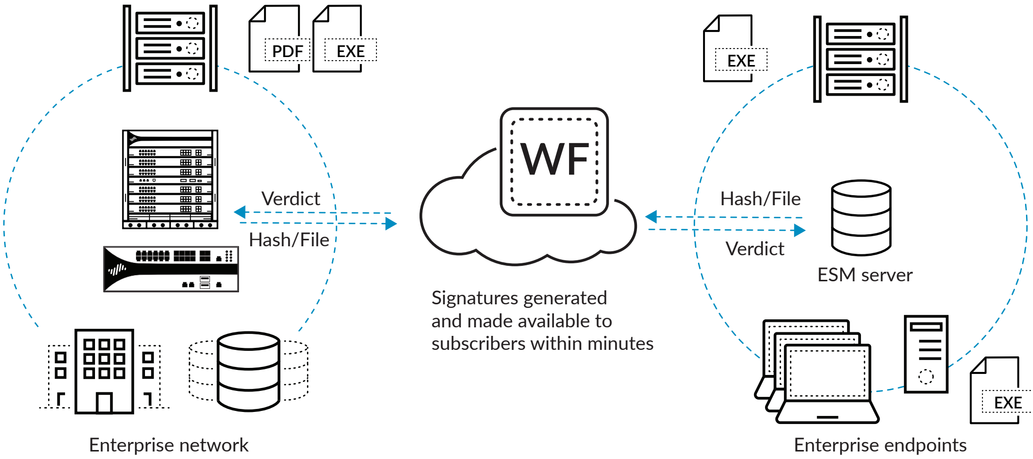


Figure 1: Wildfire schema

Turn the Unknown Into Known

WildFire detects unknown threats through a combination of complementary analysis techniques, including:

- **Static analysis** – inspects thousands of characteristics of a file to determine maliciousness quickly and effectively.
- **Local analysis** – conducts all threat analysis and generates protections on-premise, sending no content outside the boundaries of your network unless configured to do so.
- **Dynamic analysis** – automatically detonates files in a virtual environment to uncover never-before-seen malware based on conclusive behavioral attributes.
- **Shared threat intelligence** – leverages the collective threat intelligence and protections from more than 24,000 WildFire subscribers through manual updates from the global WildFire ecosystem.

WildFire executes suspicious content, with full visibility into commonly exploited file formats, including EXE, DLL, ZIP and PDF, as well as Microsoft® Office documents, Java files, Adobe® Flash® applets and links in email messages.

Using WildFire, Retarus E-Mail Security blocks sophisticated malware, such as viruses, ransomware and other threats.

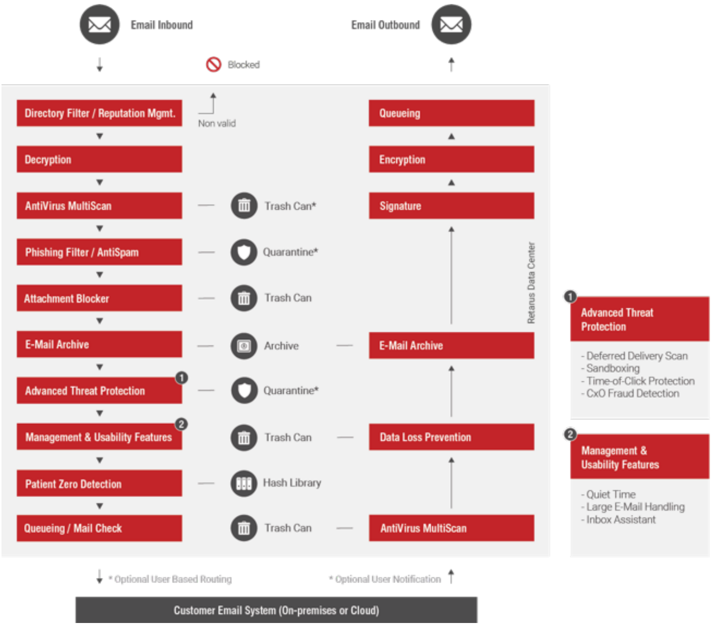


Figure 2: Retarus E-Mail Security

Attachments, such as files and active elements, that contain potentially malicious code are exported to a virtual machine and checked for unusual behavior. Emails identified as infected are deleted or quarantined, and intended recipients are notified.

Customized Email Security for Your Unique Needs

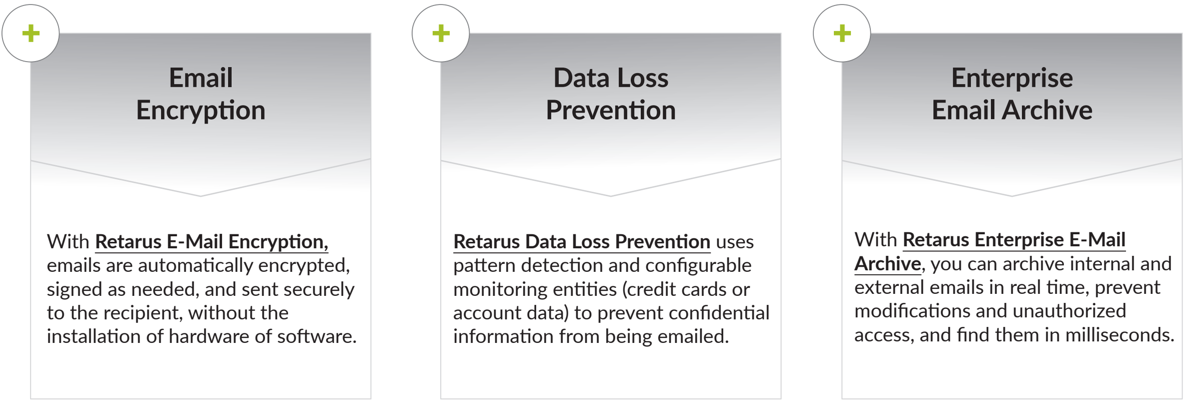
Email security services from Retarus can be customized to meet your company's security needs. With three packages to choose from, including administration and analysis features as well as additional options, you can create an effective defense system that will increase your company's security in the long term.

Double AntiVirus MultiScan	Essential Protection	–	–
Phishing Filter	Essential Protection	–	–
AntiSpam Management	Essential Protection	–	–
Attachment Blocker	Essential Protection	–	–
Directory Filter	Essential Protection	–	–
Large E-Mail Handling	Essential Protection	–	–
Quadruple AntiVirus MultiScan	Optional	Advanced Threat Protection*	Postdelivery Protection*
Deferred Delivery Scan	–	Advanced Threat Protection*	–
Sandboxing	–	Advanced Threat Protection*	–
Time-of-Click Protection	–	Advanced Threat Protection*	–
CxO Fraud Detection	–	Advanced Threat Protection*	–
Patient Zero Protection	–	–	Postdelivery Protection*
PZD Reacting Process	–	–	Postdelivery Protection*
Quiet Time	Optional	Optional	Optional
Inbox Assist	Optional	Optional	Optional
E-Mail Signature	Optional	Optional	Optional
Administration, Monitoring & Reporting	Included in all bundles	Included in all bundles	Included in all bundles

* Requires "Essential Protection"

Figure 3: Customizable protection

In addition to the tiered service offerings, Retarus E-Mail Security and Compliances Services provide gateway-based encryption, data processing in Retarus data centers according to local data protection regulations, innovative email management and tamper-proof archiving.



Email Encryption

With **Retarus E-Mail Encryption,** emails are automatically encrypted, signed as needed, and sent securely to the recipient, without the installation of hardware of software.

Data Loss Prevention

Retarus Data Loss Prevention uses pattern detection and configurable monitoring entities (credit cards or account data) to prevent confidential information from being emailed.

Enterprise Email Archive

With **Retarus Enterprise E-Mail Archive**, you can archive internal and external emails in real time, prevent modifications and unauthorized access, and find them in milliseconds.

Figure 4: Information protection and compliance

Retarus E-Mail Security service ensures that prevention, early detection of unknown threats, accelerated response processes, monitoring and analysis work together perfectly in compliance with regulations and international data protection guidelines, such as the EU General Data Protection Regulation, or GDPR.

Benefits at a Glance

- **Maximum usability:** Take the load off your help desk and make daily emailing easier for your users.
- **Maximum identification rates:** Retarus AntiVirus MultiScans run with up to four harmonized virus scanners.

- **Innovative technology:** From Quiet Time to Inbox Assist to the patent-pending Patient Zero Detection, Retarus innovations go beyond state of the art.
- **Real-time monitoring:** With E-Mail LiveSearch, your support team can track each email quickly, clearly and in detail.
- **Easy integration:** Retarus seamlessly integrates into today's most widely used email systems and cloud services.
- **Global availability:** Worldwide availability, with data centers in Europe, Asia and the U.S., provides maximum reliability and security 24/7.
- **Compliance with stringent regulations:** Global Retarus data centers help you comply with data protection and compliance guidelines relevant to your company.
- **Well-informed monitoring:** The web-based Retarus Enterprise Administration Services Portal allows you to monitor the effectiveness of your Email Security Service with easy-to-use dashboards and detailed reports, either in real time or user-defined periods.
- **Enterprise-level SLAs:** Customized SLAs can meet your needs in terms of quality, support and response time.
- **Direct delivery:** Retarus incorporates user-based routing from your local email server and gateway.
- **Service and support:** The Retarus Support team is available anywhere in the world.

Let one of Retarus' security specialists help you find the right approach:

https://www.retarus.com/contact

For more information about Palo Alto Networks-powered Retarus E-Mail Security, see these resources:

Retarus E-Mail Security & Compliance Services
https://www.retarus.com/services/email-security/tech-specs

WildFire Datasheet
https://www.paloaltonetworks.com/resources/datasheets/wildfire

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com