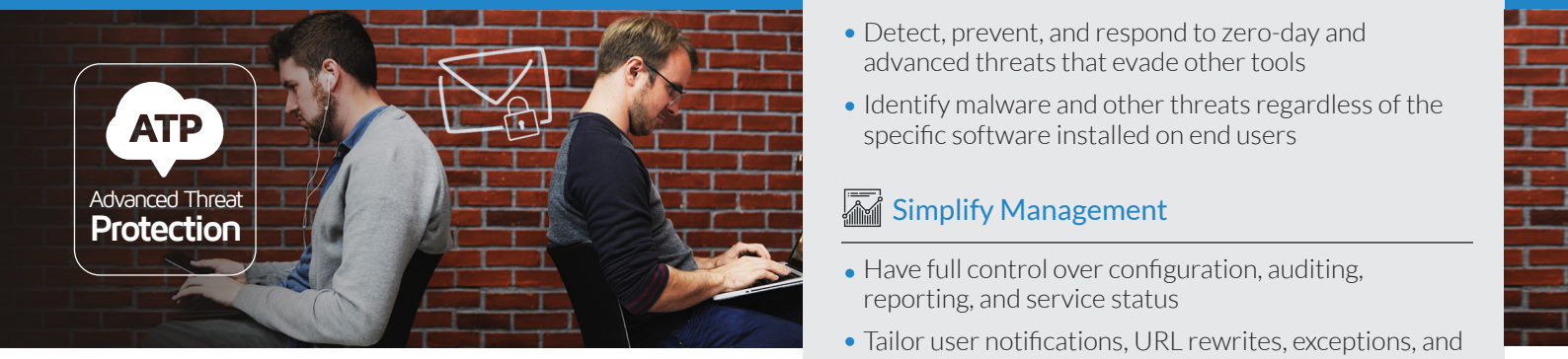
SPAMINA
Securing Digital Communications

ADVANCED THREAT PROTECTION

Stop zero-day, business email compromise, ransomware and other threats before they can reach users



ZERO-DAY > BEC > MALWARE > VIRUS

Spamina Advanced Threat Protection (ATP) is a cloud-based solution that detects, prevents, and responds to zero-day malware, ransomware, business email compromise (BEC), whaling attacks, viruses, and other advanced email-based attacks in real time.

Powered by next-generation sandboxing technology, Spamina ATP dynamically analyzes files and URLs to uncover, quarantine, and identify malicious attachments and links—even those using the most sophisticated evasion techniques. With Spamina ATP, you will deploy powerful defenses against advanced threats that attempt to infect users' systems and gain a foothold in your network.

KEY BENEFITS

Defend the Primary Attack Vector

- Analyze suspicious email file attachments, content and rewrite malicious URLs before they are delivered to users
- Detect, prevent, and respond to zero-day and advanced threats that evade other tools
- Identify malware and other threats regardless of the specific software installed on end users

Simplify Management

- Have full control over configuration, auditing, reporting, and service status
- Tailor user notifications, URL rewrites, exceptions, and analysis reports to your needs
- Achieve comprehensive visibility into email logs and analysis results

Support Regulatory Compliance

- Stop more threats, including those that try to evade detection or disable the sandbox
- Support audits and compliance with at-a-glance reports and detailed analysis
- Maintain a record of all the emails analyzed

Increase User Protection

- Alert users and block access to malicious sites automatically
- Prevent system infections by analyzing suspicious items before they are delivered
- Stop business email compromise (impersonation) attacks
- Notify users when items are being analyzed to increase awareness of potential threats

Dynamic Analysis

Our dynamic analysis technology delivers deep visibility and analysis in real time to identify and stop threats embedded in attachments, header anomalies, domain similarities and malicious links. Spamina ATP even stops threats that try to evade detection or disable sandboxing capabilities.

Detailed Reporting

Instantly view detailed threat activity with Protection Status reports. See the number of emails processed, percentage with malware, domains or users ranked by malware detected, sandbox status, and other data.

Deployment and Management Flexibility

Dry-run mode lets you measure sandboxing effectiveness prior to deployment without disrupting existing workflows. Tailor advanced threat defenses to the needs of individual departments. Deactivate URL analysis for employees in controlled environments and enable user notification as desired to support user awareness campaigns.

Made in Europe

We understand the threat landscape facing European customers and your data requirements. Our data centers have deep knowledge of region-specific risks and operate in areas where your data privacy is legally protected from third parties.

VALIDATE FILE ATTACHMENTS WITH DYNAMIC ANALYSIS

Email attachments are analyzed by Spamina file sandboxing to ensure that they are safe from zero-day threats, ransomware, and viruses before being delivered to users' mailboxes. Spamina ATP analyzes a wide range of executables, documents, archives, scripts, and media files.

Through the Complete Runtime Environment Instrumentation, Spamina ATP has kernel-level visibility into files so that the sandbox is aware of the interactions between the suspicious file and the host operating system. Dynamic analysis technology also interacts with the suspicious attachment to elicit behaviors that verify malicious intent.

DEFEND AGAINST IMPERSONATORS

Some email attacks rely on social engineering techniques, instead of malware, to deceive users into revealing sensitive data. Business email compromise—or spoofed—messages attempt to impersonate the company CEO, CFO, or other executive and request employee payroll data, funds transfers, or bill payments. Spamina ATP scans all inbound email and inspects headers, domain details, and content to identify impersonation attempts and block them.

PILOT THE SOLUTION WITHOUT WORKFLOW DISRUPTION

Our unique dry-run service assessment and deployment tool enables you to pilot Spamina ATP for a subset of users while preserving your existing workflow. In dry-run mode, your security team can assess email sandboxing effectiveness, response time, and other capabilities. During a dry run, a copy of the message is immediately delivered to the recipient's mailbox and a second copy is sent to Spamina ATP. Once the solution finds malicious content, it flags the message in quarantine for review by the security team.

PROTECT AGAINST INFECTED WEBSITES

Spamina ATP URL sandboxing identifies attacks targeting vulnerable websites through malicious Flash, JavaScript, and ActiveX elements. It prevents systems from being infected when users click on malicious links that attempt to install malware or C&C capabilities. When a user clicks on links in an email, URL sandboxing analyzes it to detect any suspicious behavior. If it is malicious, Spamina ATP alerts the user and blocks access to the site. Link rewriting is optional. Your team can activate the URL rewrite feature completely or by company, domain, or user.

KEEP USERS IN THE LOOP

Spamina ATP also gives you control over whether users are notified when emails or URLs are being analyzed. If you activate user notification, they receive a courtesy message that a received email is being analyzed with Spamina ATP.

ASK FOR A FREE TRIAL
spamina.com/en/free-evaluation

About Spamina

Spamina provides innovative enterprise solutions in the areas of Threat Prevention, Data Governance and Secure Collaboration. Our cloud services offer customers a safe communication environment where business continuity, service scalability and cost-effectiveness are ensured. Headquartered in Madrid (Spain), Spamina serves customers in more than 50 countries, supported by a network of authorized partners.

SPAMINA
Securing Digital Communications

For more information:
www.spamina.com
+34 91 368 77 33
info@spamina.com

SIMPLIFY MANAGEMENT AND RESPONSE

Spamina ATP is fully integrated with the Spamina administrative console, giving you control over configuration, auditing, reporting, and service status. Email logs track activity for all sandboxed items, so that you can quickly see which email attachments were sent for advanced threat analysis and whether URLs were rewritten. Download sandbox threat analyses with a click for fast review and information to target your response.

ACCELERATE MALWARE IDENTIFICATION WITH FEWER FALSE POSITIVES

Spamina ATP includes a signature-based Advanced Premium Antivirus Engine, which identifies and stops a wide range of malware hidden in email attachments. It identifies known malware families and their mutations, as well as threats that mutate rapidly. Proactive behavioral monitoring and analysis enables faster detection of threats. The antivirus engine also maintains up-to-date lists of executables that are known to be malware-free to minimize false positives.

SUPPORT COMPLIANCE INITIATIVES

Spamina ATP meets critical data governance requirements for availability, security, usability, and data integrity. Spamina ATP supports your audit and compliance activities for a wide range of regulatory acts, including EU GDPR. Data protection regulations, such as GDPR, require organizations to keep a record of all data that can contain private information, and organizations must update their policies, messaging inventories, and procedures. Spamina makes it simple. Spamina ATP also simplifies compliance with PCI DSS, HIPAA, FINRA, PIPED, and other region-specific regulations.

EXTEND THE BENEFITS

Spamina ATP is a premium option for Spamina Cloud Email Firewall and Parla Mailbox customers. You can subscribe to Spamina ATP for all domains and users, specific domains, or individual users. Integration with the Spamina console enables comprehensive email and instant messaging protection, data leak prevention, encryption, archiving, threat prevention, and compliance reporting in a single pane of glass.

Spamina Trusted Protection for Enterprise Email and Instant Messaging