VIPRE EMAIL SECURITY

Solution Brief

ADVANCED THREAT PROTECTION (ATP)

Layered Security with Sandboxing and Phishing Protection

Cybersecurity threats continue to evolve as attackers employ advanced techniques like zero-hour exploits and customized malware to stay a step ahead. Traditional signature-based solutions are necessary but may lack the modern analytics to prevent all zero-hour and targeted attacks. A more powerful protection is needed. New and emerging threats require a layered email security approach that includes multiple levels of malware detection, and must cover common attack vectors such as malicious attachments and URLs simultaneously.

SMBs Under Attack, Email Attachments Widely Targeted

Often seen as easy targets, criminals prey on small and medium-sized businesses while leveraging advanced techniques to bypass traditional security. Typically, smaller organizations don't have the resources that larger enterprises have, so they need a solution that will provide them with a similar level of advanced protection in a cost-effective, easy to manage package. VIPRE ATP is perfect for SMBs challenged with limited IT resources.

- *"The average company received over 94% of their detected malware through email while over 45% of malware was delivered by email attachments containing common Microsoft Office documents"*
  – Verizon 2019

VIPRE Email Security Advanced Threat Protection (ATP) offers enterprise-grade email protection in an easy to use, out of the box package. VIPRE ATP defends end users against the newest most sophisticated strains of malware, weaponized attachments and phishing techniques that evade traditional detection.

Comprehensive Solution from a Single Vendor

VIPRE is the single source from ordering and provisioning to award-winning support. Get more for less with a single trusted vendor.

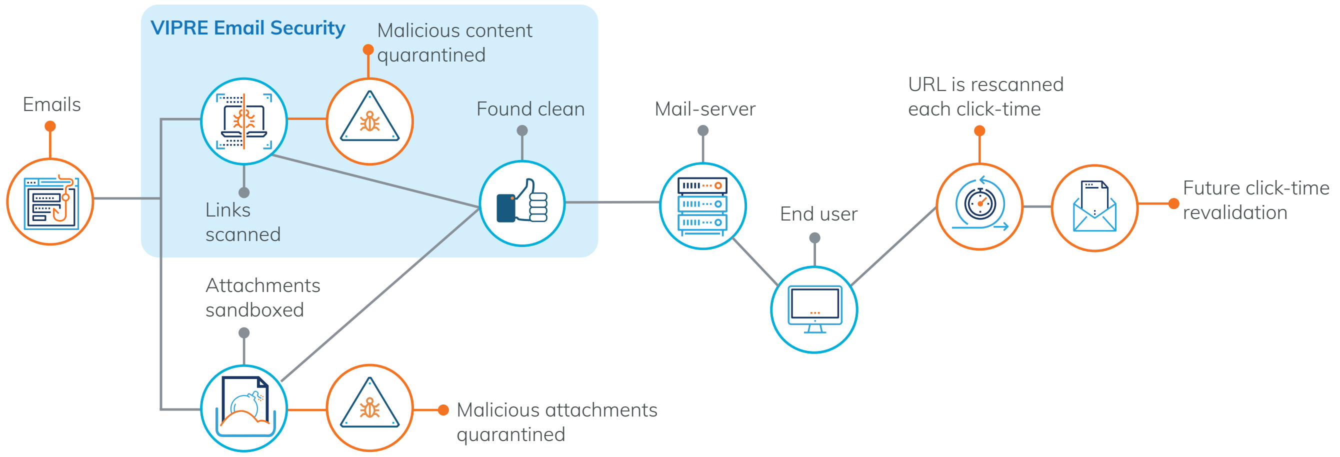
Single Solution for Multiple Attack Types

Protection against malicious attachments and URLs simultaneously.

Zero-hour Protection

Signature-based bulk malware detection combined with sandboxing and machine learning behavioral analysis deliver powerful defense against zero-hour malware.

VIPRE Email Security Cloud: Journey Leveraging ATP



VIPRE Email Security
Malicious content quarantined
Emails
Found clean
Mail-server
URL is rescanned each click-time
Links scanned
End user
Future click-time revalidation
Attachments sandboxed
Malicious attachments quarantined

Powerful Protection with Layered Defense

At the core of VIPRE ATP is VIPRE Email Security Cloud, the platform that provides a solid foundation for email reception, handling, and bulk protection. The base platform includes core anti-spam, anti-malware, and anti-phishing technology, continuity protection against email server downtime, and highly customizable filtering and routing rules.

- Core email reception and routing engine
- Provides tough anti-spam, anti-malware, and anti-phishing protection against bulk malware
- Sophisticated custom routing/filtering rules engine, extensible to meet any business need
- 90-day continuity protection to guard against email server outages
- Extremely reliable having no outages in a decade

Attachment Sandboxing goes a step further than traditional anti-malware by executing extracted attachments in a protected cloud sandbox environment. The behavior of the executed content is observed and compared to past known malware strains using sophisticated machine learning to determine if the content could be malicious.

- Powerful sandboxing technology
- Protects against evasive and sandbox-aware malware
- Dynamic, isolated cloud virtual machine environment that scales easily to handle the load from all clients
- Detailed behavioral analysis output that explains exactly what the attachment tried to do upon execution

Phishing Protection provides another layer of defense against embedded malicious URLs by closing the time gap, often exploited by attackers, between receipt-time scanning (performed by the core platform) and when an end user clicks on the URL. All an attacker has to do is to wait to set up a malicious domain until sometime after an email is sent, and users could be fooled into visiting a phishing site. Phishing Protection closes that gap by rewriting the URLs embedded in emails and re-scanning them at click-time, ensuring that users stay protected.

- Deep scan URLs and block links that can lead to malware infection
- Re-write URL and web links in emails for click-time protection
- Schedule customized messaging, reporting and statistics