RevBits

PRODUCT BRIEF

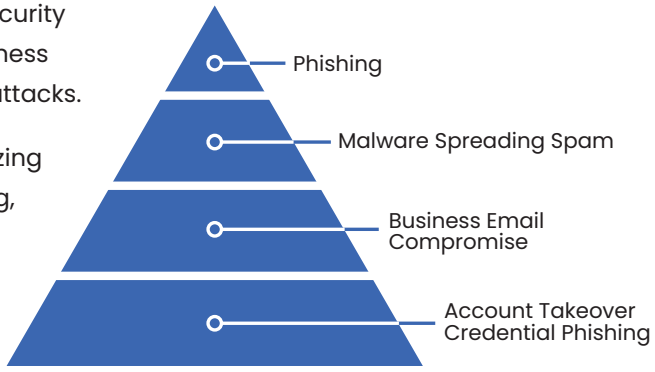
Email Security

End-to-End Email Security Closes Infrastructure to Endpoint Risk Gaps

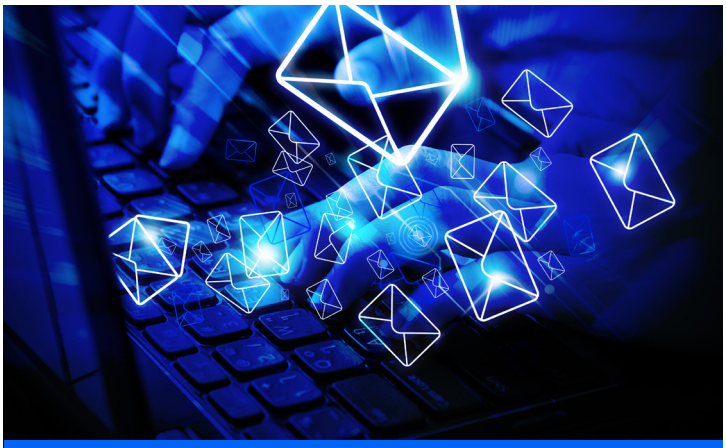
Email security is a foundational requirement, as email is the leading source of malicious attacks and damaging breaches. Robust endpoint email security and secure email gateway (SEG), complemented with security awareness training, are needed to reliably and consistently thwart email-based attacks.

SEG solutions protect against email threats by intercepting and analyzing email before sending it to corporate email servers. SEG blocks phishing, spam, business email compromise (BEC), impersonations, ransomware and other types of malware. While very important, an SEG is but one solution needed to defend against email threats. In addition, organizations must protect user endpoints. This is accomplished with cloud distributed and centrally monitored software deployed on endpoints that detects and blocks sophisticated malicious emails at the network edge.

Email Attack Techniques



Primary email attacks indicating the scale of targets for each type.



"Projections estimate that by 2025, daily email traffic will reach 376 billion, and for the foreseeable future, it will remain the most popular form of digital communication."

Projections estimate that by 2025, daily email traffic will reach 376 billion, and for the foreseeable future, it will remain the most popular form of digital communication. Unfortunately, it is also wrought with vulnerabilities, making it a fertile field for a variety of cyberattacks. Bad actors target and infect email systems inside organizations and across remote edge user devices that can be located anywhere. In addition to technology, a strong and enforceable email security policy and user training must be part of a holistic security strategy to protect this vital business function.

The need for multi-layered email security

Secure email gateways intercept, analyze and block incoming emails, before sending them to the corporate email server for distribution. Because of the massive volumes of traffic, this detection approach leaves little time

for deep analysis, that would cause impractical delays. Because of their limited processing time all secure email gateways will invariably miss some sophisticated threats. Deep analysis of email performed on user endpoints is required to solve the problem and close this security gap. With this distributed processing, superior analysis and better protection can be provided without causing delays. Combining SEG and endpoint email protection within a unified XDR gives IT, security and risk management teams multi-layered security with a 360-degree view and broad coverage of their enterprise-wide cybersecurity ecosystem.

Bad actors understand the inherent limitations of email gateways, and can get around them with impersonations, multi-layer attachments, links to files, link redirects, and many other evasive techniques. No organization is immune to unknown, zero-day multi-layered email attacks. Eventually, very determined bad actors will break through their defense.

Email security capabilities for advanced threats

Some of the most advanced email exploits are impersonations, where hackers discover that an organization uses, say Office 365. They create a fake Office 365 login page with custom emails that are sent to unsuspecting corporate workers. Impersonation attacks take advantage of human errors in judgment. When employees unwittingly open and respond to emails they think are from the CEO or another company executive and unknowingly provide private information or credentials that provide hackers with broad access to the corporate network.

Domain spoofing is another technique used to gain access into a corporate network. There are three standards-based email security protocols that address malicious email authentication methods. These include SPF, DKIM, and DMARC, which work together to help protect against email and domain name spoofing.

To prevent email and domain spoofing, Sender Policy Framework (SPF) hardens DNS servers by restricting who can send emails from a domain. Domain Keys Identified Mail (DKIM) ensures email content is trusted, and not compromised. Domain-based Message Authentication, Reporting, and Conformance (DMARC) integrates SPF and DKIM protocols with consistent policies, links the sender's domain name with the "from header", and provides reporting back from email recipients.

The legitimacy of an email's true owner is critical for communications. In the case of a Business Email Compromise (BEC) cyberattack, the result for the victimized organization can be financial loss, brand erosion, and the loss of customer trust. Email authentication, using SPF, DKIM, and DMARC protocols to verify an organization's email and domain, provides proof that the users and devices sending outbound emails are legitimate. However, implementing, managing, and mitigating email authentication remains a cumbersome and fault-riddled process.

RevBits Multi-Layered Email Security

RevBits Email Security includes endpoint-based email security and SEG. RevBits sophisticated, easy-to-use dashboard receives automated and manually reported emails that are dissected, parsed, analyzed and made ready for investigation. RevBits email security can also be part of the RevBits Cyber Intelligence Platform (CIP).

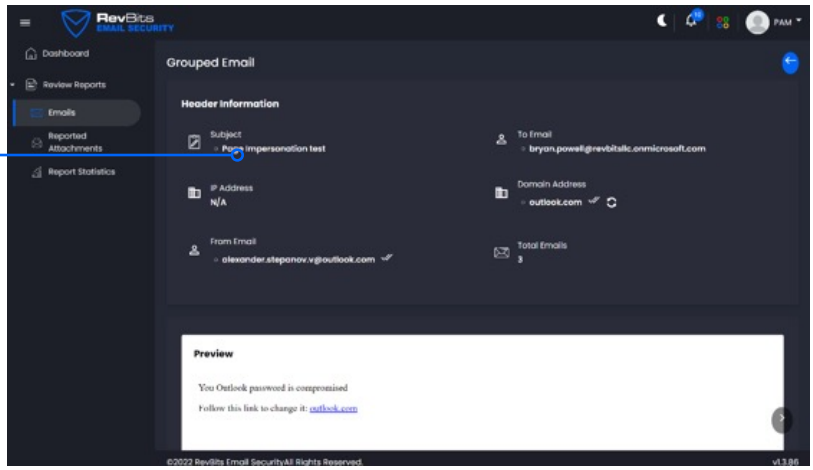
CIP is a unified extended detection and response (XDR) platform that includes best in class email security, endpoint detection and response, privileged access management, zero trust networking, and deception technology. RevBits CIP integrates and unifies telemetry from all attack vector sources to detect, respond and block the broadest range of threats. RevBits unified orchestration increases the overall fidelity of threats and responses to deliver the best outcomes.

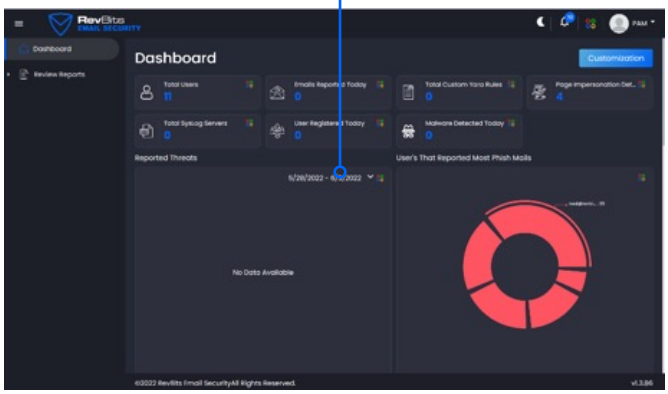
RevBits Email Security's Endpoint-Based Agent (EBA) – is a native SaaS-delivered solution, also referred to as integrated cloud email security (ICES). RevBits Email Security - EBA protects against malicious emails, like phishing campaigns, at the most dangerous point - the endpoint. In some ways it takes over where a secure email gateway leaves off, filling in security gaps by leveraging distributed processing for deep analysis on remote user endpoints to detect and block malicious emails that get past the centralized layer of an organization's security stack. This includes multi-layered attachments, and even password protected attachments. Blocked emails are quarantined and batched for review. They are then transformed into non-actionable states and displayed, with details regarding risk factors and reasons for blockage, for user awareness and training.

RevBits Email Security delivers end-to-end email security and feature-rich administrative reporting.

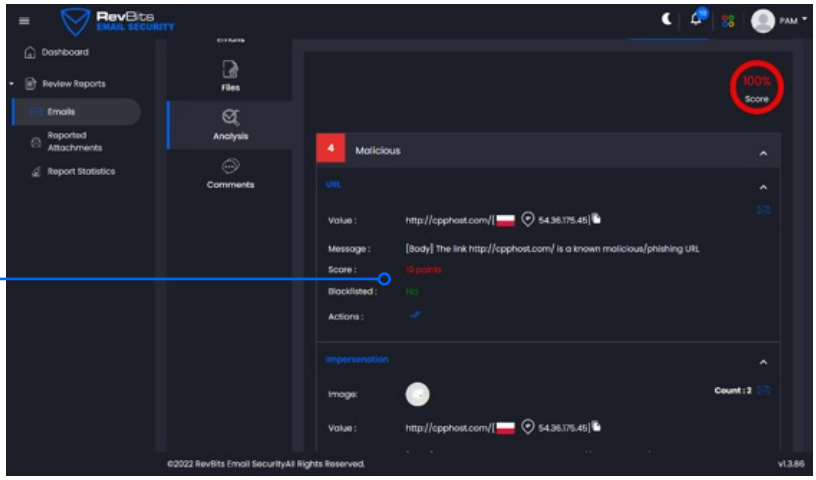
Unique page impersonalization protection

Feature rich dashboard

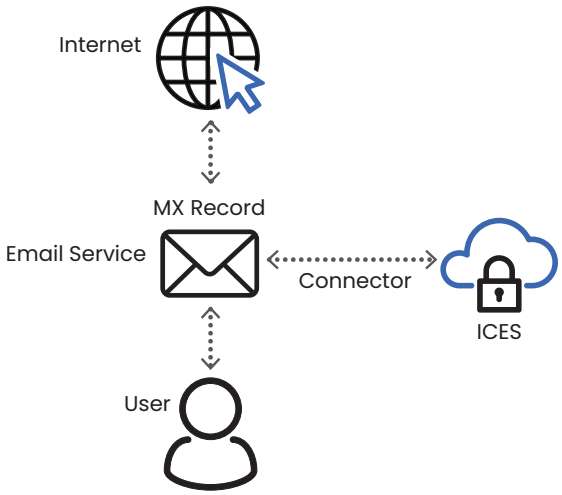




Actionable intelligence



Predelivery or Connector-Based ICES Architecture



RevBits Email Security - EBA deployment scenario

RevBits - EBA performs deep analysis of all email that arrives on endpoint Outlook inboxes, leveraging more than fifty advanced algorithms. This distributed processing offers superior analysis and better protection, without causing delays. Features includes intelligence sharing, page impersonation analysis, custom configuration and deep analysis of password protected attachments.

Employees receive real time email phishing training through RevBits Email Security user inbox interface. This allows users to see real blocked emails and the reasons why they were blocked. This feature provides valuable ongoing email security training for employees.

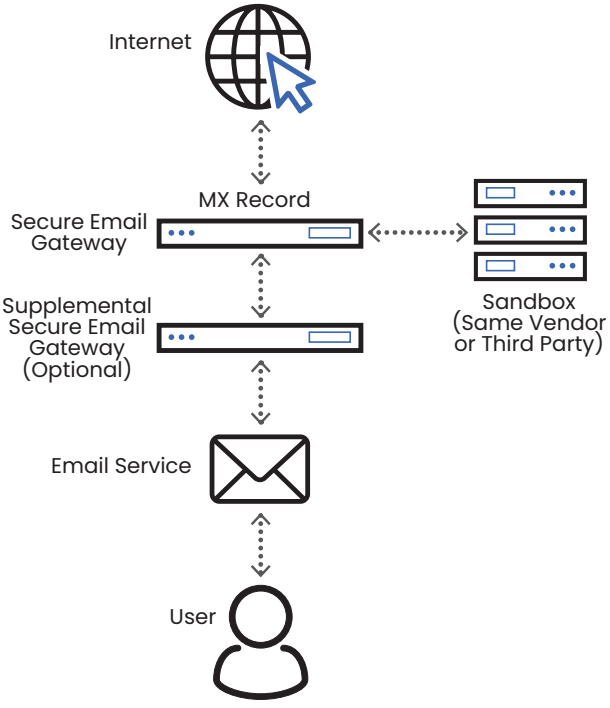
RevBits has removed the complexity and difficulty of enabling DKIM, DMARC, and SPF, reducing risk and enhancing the organization's overall email security posture. RevBits endpoint email security automates workflows and reliably deploys standard email protocols that authenticate out-bound emails. This simplifies the process of controlling domain email addresses to minimize spam and spoofing. It also enables admins to easily authorize third-party email marketing companies to send email campaigns out on their behalf.

While the benefits of RevBits Email Security - EBA are many, here are a few highlights:

- Easy deployment
- Significantly reduce the number of successful phishing attacks
- Reduce the cost of mitigation by blocking credential harvesting campaigns
- Scalable within the organization's existing email security stack

RevBits Secure Email Gateway (SEG) - is cloud-based and globally deployed for dynamic scalability. It is also inherently redundant for reliable and dependable operations – anywhere in the world. RevBits SEG protects against email threats by blocking phishing, business email compromise (BEC), spam, social engineering, ransomware, and other malware. RevBits SEG is positioned as a front-line corporate email defense, inline within the email transportation route, and directly in the path of all traffic going to the corporate email server. All email is processed, scanned, filtered, and analyzed. Clean emails are passed onto the user's inboxes, while questionable emails are quarantined for further inspection.

Secure Email Gateway Architecture



RevBits SEG deployment scenario

End-to-end email security within a single dashboard

A robust multi-layered email security approach, RevBits Email Security's endpoint-based agent and SEG work together at the speed of business. RevBits delivers a unified end-to-end security chain that captures, analyzes and blocks the most sophisticated malicious emails - from on-premise and cloud email servers, to user inboxes at the furthest points of the network edge. All features and functions are unified within a single dashboard, accessed through the secure admin portal. All email threats, attackers, spammers, analysis, policies and rules, blacklists and whitelists and reports are viewed within a single screen. No more swiveling between dashboards. No more logging into, coordinating, and managing multiple vendor products, licenses and reports.

RevBits endpoint and gateway email security centrally monitored and managed, and unified within a single dashboard, provide greater security than disparate email security products working independently. RevBits Email Security is a case where the whole is greater than the sum of its parts.

RevBits®, LLC • 34 Willis Avenue • Mineola, NY 11501 • 844-4REVBIT (844-473-8248)