IDC ANALYZE THE FUTURE

IDC TECHNOLOGY SPOTLIGHT

Sponsored by: EdgeWave

Traditional email security gateways are a must-have, but they are not enough to answer the increase in advanced and targeted attacks. Managed inbox detection and response (MIDR) is the modern approach to combatting these attacks.

Managed Inbox Detection and Response

December 2018

Written by: Christina Richmond, Program Vice President, Worldwide Security Services, and Curtis Price, Program Vice President, Infrastructure Services

Introduction

Businesses of all sizes use email security gateways to prevent transmission of emails that oppose company policy, send malware, or attempt to exfiltrate company information. Traditional gateways prevent data loss, encrypt emails, protect against known and unknown malware, and can compensate for weak partner security. Delivery models for email security gateways include private cloud, hybrid cloud, hardware appliances, virtual appliances, and email server–based products. They are a must-have in today's security architecture to stop 80–90% of nefarious traffic, but it's apparent from continued rampant phishing attacks that there is still more to do to secure the modern inbox.

Greater visibility at the email attack front and broader capabilities within the inbox are required today. Email security has evolved, and advanced solutions now include predelivery and postdelivery capabilities as well as incident response. In addition, there are options for managed email security that provide these emerging features; hence the title of this IDC paper: *Managed Inbox Detection and Response*.

AT A GLANCE

KEY STATS

Traditional email security gateways are a must-have but miss advanced socially engineered and targeted phishing attacks, making email the number 1 attack vector for cybercriminals.

WHAT'S IMPORTANT

Today's hybrid and cloud-enabled architectures require a more modern approach that includes advanced analytics, machine learning, human expertise, and ease of use.

KEY TAKEAWAY

EdgeWave's next-generation Email Security Platform combines comprehensive predelivery protection, postdelivery detection, and email incident response to effectively address emerging email attack vectors.

Trends

Email is the company lifeblood and a ubiquitous tool across the business, which makes it a very attractive and common attack surface. According to industry research, email delivers over 92% of malware. Adversaries use email to deliver malware, steal user credentials, and exfiltrate sensitive data. But the fact of the matter is that traditional email security gateways do not catch everything. They are terrific at handling mid- to high-volume attacks but often still miss targeted, socially engineered attacks. Email security gateways are proven nearly 100% effective against spam but not nearly as effective against phishing attacks, which continue to be the number 1 threat vector for data and financial breaches.

Spam is a high-volume nuisance, while phishing attacks are often much lower in volume, flying under the monitor-and-alert radar. Often, adversaries change IP address and attack vector in rapid succession, making the attacks hard to combat using traditional solutions. Spam filters have added sandbox features and signature-based defenses, but phishing attacks continue to propagate. Email security gateways are a required tool for the business, but more is needed, and the market is evolving beyond traditional email security capabilities.

A multilayered approach is key to creating a true defense-in-depth strategy for email protection, including traditional email security gateways, advanced analytics such as machine learning to augment human analysis of the threat landscape, and methodology that enables facile identification of and response to suspicious emails. Employee education is increasingly deficient because of workforce fatigue, and many solutions do not tie together the predelivery and postdelivery capabilities, making the defense-in-depth approach difficult to attain. In fact, market movement clearly demonstrates that there is a bifurcation or at least a separation of these two strategies.

Predelivery email security is where the more traditional email security gateways shine as a first layer of defense. They seek known malware and update signature white lists and can function across all workloads. Often they incorporate encryption capabilities as well. Filters identify known criminal IP addresses, authenticate mail, and find spoofed and illegitimate emails, but they do not find targeted phishing emails.

Postdelivery tools find emails that have passed through the gateway undetected. Most postdelivery begins with an employee recognizing that an email is suspicious, and a lot of effort has gone into security awareness and education training of employees to do just that. This is a great start, but employees are not properly skilled or equipped to assess email legitimacy. There must be an easier way.

Immediate action, or incident response, is critical to modern inbox protection. The ability to automatically quarantine, remove, and delete malicious emails without human intervention is critical for protecting an organization from targeted attacks. Eliminating phishing attacks within the inbox breaks the cybersecurity kill chain at the delivery phase, which prevents breaches and other downstream effects. Automation of incident response assists IT organizations by reducing dwell time and accelerating response speeds.

In addition to modern tactics to secure the inbox, emerging managed email security solutions are on the rise. It is difficult to tackle predelivery and postdelivery email security within the organization because resources and budgets are often scant. In addition, not all organizations have the ability to do the threat research or possess the automation capabilities or the advanced analytics to achieve success. Managed email security services offer a subscription-based pricing model that accommodates limited security budgets found within many organizations as an operational expense rather than a capital expense.

Finally, but not at all inconsequential, is the human expertise necessary in a modern approach to email security. Most companies do not possess enough IT resources to manage the day-to-day business let alone thwart crafty adversaries that have all the resources needed to socially engineer and deploy targeted phishing attacks. The human element is not trivial in this battle. Managed inbox detection and response capabilities must tout global 24 x 7 human analysis that can review and categorize email-borne attacks. This expert human layer is essential to successfully thwarting social attacks with the highest levels of accuracy.

Considering EdgeWave

Headquartered in San Diego, California, EdgeWave offers a next-generation Email Security Platform that provides predelivery protection, postdelivery detection, and email incident response. By covering all three elements, EdgeWave follows a defense-in-depth approach applied to email security. EdgeWave has more than a decade of email security experience and today touts more than 2,500 customers and over 3.5 million protected users worldwide. Key components of the EdgeWave Email Security Platform are shown in Figure 1.

FIGURE 1: ***EdgeWave Email Security Platform***

PREDELIVERY PROTECTION

- ePrism Email Security Gateway
- AV and Malware Scanning
- Mail reputation and custom filtering rule sets

POSTDELIVERY DETECTION

- ThreatTest Anti-Phishing Solution
- Digital fingerprinting and threat scoring
- Combination of machine learning and human review

INCIDENT RESPONSE

- ThreatTest global remediation
- Alerting/reporting of phishing and malicious attacks
- Security operation center integration

Source: EdgeWave, 2018

Predelivery Protection

The EdgeWave ePrism email security gateway is central to predelivery protection and provides email defense against internal and external threats such as spam, viruses, spyware, phishing schemes, identity theft, and other dangerous content. ePrism consists of inbound and outbound spam and antivirus filtering, category-based policy, and automated directory integration in an easily provisioned hosted SaaS solution. Additionally, the EdgeWave Threat Detection Center provides proactive threat monitoring and analysis.

Postdelivery Detection

Providing postdelivery detection within the Email Security Platform is ThreatTest, an automated, anti-phishing solution that uses both machine learning and expert human review to quickly analyze and resolve any suspicious email. This patent-pending approach reduces targeted attacks while lowering the amount of time and money spent by IT investigating and recovering from email incidents. EdgeWave ThreatTest enables employees to report suspicious emails for threat investigation with the click of a button. It then processes the email through machine learning and human

expert analysis to check the email's true intent. In minutes, the email is analyzed and removed, if it is malicious. The intent of this service is to remove the guesswork of identifying phishing threats and enable staff to be a part of the organization's security defense. In addition, EdgeWave states that the service optimizes IT resources by automating email investigations and delivering managed phishing remediation. When an employee receives an email impersonation or other suspicious email, ThreatTest provides easy-to-use investigation and incident response.

ThreatTest follows six steps to accomplish identification and remediation:

1. An employee notices a suspicious email in his or her Outlook Inbox and clicks the ThreatTest button to launch a review.
2. The flagged email is automatically quarantined and routed through the EdgeWave Hybrid Threat Detection Center.
3. The EdgeWave automated machine learning engines investigate the suspicious email.
4. Live security experts join the investigation of the suspicious email with multifaceted analysis.
5. Within minutes, the suspicious email is classified and either returned to the submitter or retained in quarantine.
6. Real-time reporting gives IT clear visibility into the incident and its resolution.

Incident Response

EdgeWave's Email Incident Response service provides automatic remediation of detected, malicious email. When malicious email is detected by ThreatTest, a follow-up scan of the mail store can be executed to find the same message in additional inboxes and automatically delete or quarantine the message across the organization.

Challenges

The email security market is mature, and its value is ubiquitous. However, it has evolved to the point that it should no longer be taken at face value. This is a key challenge for both the market at large and EdgeWave because buyers assume that a traditional email security gateway is enough to protect their organization. Education is needed to inform buyers not only that more email security is necessary but also that the market has evolved and key players now include predelivery and postdelivery capabilities. However, there is a strong misperception that training and education are enough — and the lack of knowledge that there is another approach creates a bit of an uphill battle for EdgeWave.

Benefits

For organizations that embrace managed inbox detection and response for securing the inbox, there are many benefits to be realized:

- Minimizes risk of email attacks that include phishing, ransomware, and business email compromise
- Eliminates human factor risk by taking the guesswork out of phishing detection while improving catch rates
- Improves response times that mitigate email-based attacks at the delivery phase of the cybersecurity kill chain
- Reduces burden on internal IT staff by outsourcing email review to email security experts

Conclusion

IDC believes that next-generation inbox protection — that is, postdelivery detection and automated incident response informed by human expertise and machine learning — will be the norm in the future. Additionally, because organizations are overwhelmed with security management, the MIDR market will continue to grow along with increasing enterprise adoption of managed security services.

IDC believes that next-generation inbox protection will be the norm in the future.

EdgeWave is well positioned to answer the market challenges discussed previously because the company is focusing on creating best-in-class, next-generation email security to thwart phishing attacks and address the three required components of MIDR: predelivery protection, postdelivery detection, and automated incident response.

About the analysts:

Christina Richmond, Program Vice President, Worldwide Security Services

Christina Richmond is responsible for IDC's worldwide research and analysis on enterprise and service provider security consulting and integration services. She is responsible for identifying trends and analyzing strategies that are key to the success of security-focused IT suppliers, global system integrators, and service providers and analyzes key issues faced by these suppliers, examining their services strategies, ecosystems, strategic alliances, and partnering strategies in this complex and fast-moving market segment.

Curtis Price, Program Vice President, Infrastructure Services

Curtis Price is the Program Vice President of IDC's Infrastructure Services group. He oversees all research efforts within IDC's Network Life-Cycle Services, Wireless Infrastructure Services, and Software and Hardware Support Services programs. Mr. Price provides expert insight and analysis of the trends and market dynamics impacting the network services market within the enterprise and telecommunications sectors.

IDC Custom Solutions

IDC Corporate USA
5 Speen Street
Framingham, MA 01701, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com