ESG SHOWCASE

Closing the Biggest Security Gap in Cloud-delivered Email Native Security Controls: Stopping Advanced Threats

Date: November 2021 **Author:** Dave Gruber, Senior ESG Analyst

ABSTRACT: The adversary has become quite adept at evading many of the more popular email security controls in use today, making email the perfect path to compromise organizations. Post-breach analysis all too often finds that email is used early in the attack chain, later resulting in substantial breaches. While many organizations expect either the native security controls included within cloud-delivered email solutions or existing secure email gateways (SEG) to protect against today's more advanced threat landscape, more progressive security teams are realizing that additional, layered security controls are needed to stop advanced threats.

Overview

The rapid move to cloud-delivered email, together with a less-than-comprehensive native email security offering from Microsoft, has spawned a new category of email security controls referred to as cloud email security supplement (CESS) solutions. This new category of offerings intends to close gaps that organizations have identified within the native email security controls offered within Microsoft 365 (M365) and controls included within traditional secure email gateways (SEG).

Most CESS products tout their ability to address one or more of these gaps, helping organizations protect against phishing, credential theft, business email compromise, ransomware, data leakage, interruption in business continuity, and other less publicized gaps. These "mini-add-on-platforms" attempt to provide a one-stop-shop approach to closing email security gaps, without overlapping with the native email security capabilities already included with M365.

Stopping Advanced Threats

The adversary has become quite adept at evading many of the more popular email security controls in use today, making email the perfect path to compromise organizations, as an early step in the attack chain. Of the many identified gaps in native email security controls, 58% of organizations report experiencing business email compromise attacks such as payroll fraud, executive impersonation, email account compromise or takeover, wire transfer or payment fraud, or vendor/supply chain fraud within the last 12 months.[1]

Inbound email attacks commonly leverage two highly successful techniques, including the attachment of malicious files and inclusion of malicious URLs. Both typically utilize some amount of "lure" body copy to convince unsuspecting users to either open a malicious file or to click on a malicious URL.

[1] Source: ESG Research Report, *Trends in Email Security*, August 2020.

This ESG Showcase was commissioned by VMRay and is distributed under license from ESG.
© 2021 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Low and Slow Attacks

In more advanced attacks, malicious files and URLs are often used to drop silent spyware on machines, providing a means for attackers to gather reconnaissance that is often used to inform attack strategies and orchestration of low and slow attacks.

Malicious URLs serve a variety of purposes but are commonly used to lead users to impersonated websites where they are asked to enter sensitive information, often including login credentials.

According to the 2021 Verizon Data Breach Report, credentials lead the list for the top variety of data stolen in north American data breaches. Personal data is a prime target as well, since that includes such data elements as Social Security/Insurance numbers paired with other bits of information that allow criminals to commit further financial fraud.[2]

In more advanced attacks, malicious files and URLs are often used to drop silent spyware on machines, providing a means for attackers to gather reconnaissance that is often used to inform attack strategies and orchestration of low and slow attacks.

While the detection of these two types of well-known attack techniques is well understood and supported in many email security solutions, most only recognize them in plain sight. However, attackers have evolved the use of these techniques to disguise them using encryption, obfuscation, and other techniques that enable them to evade typical email security controls. Only advanced email security solutions are able to expose the true behavior of these disguised attacks using anti-evasion mechanisms that can see through and identify malicious tactics.

Broad Adoption of Cloud-delivered Email Opens Up New Threats

With so many organizations now depending on the same, native email security controls provided within M365, attackers are optimizing threats to evade native security controls. These "evasive" threats are often further targeted and customized for specific organizations and even specific people.

While many large organizations continue to depend on secure email gateways (SEG) and expect SEG vendors to strengthen their offerings to protect against today's more advanced threat landscape, more progressive security teams are realizing that additional, layered security controls are needed and are investing in CESS solutions to supplement traditional and native security controls.

And while in the past attackers often focused on larger enterprises with higher-value assets, they now commonly prey on smaller, less-equipped organizations that have vulnerable systems, fewer controls, and smaller IT and security teams to support their infrastructure.

Defense in Depth

Defense-in-depth strategies have long been core to implementing the level of security required by most organizations, with an ongoing convergence from best-of-breed approaches to consolidated platforms. This pendulum swing occurs as the "arms-race," "cat-and-mouse" chase continues, with both defenders and attackers continuously investing to implement new strategies and techniques to keep up with advancements in IT infrastructure.

The recent move to a work-from-anywhere environment together with the rapid acceleration of digital transformation and cloud initiatives have sufficiently disrupted IT infrastructure to a level that is providing the adversary a host of new attack

[2] Source: Verizon, *2021 Data Breach Investigations Report*, 2021.

© 2021 by The Enterprise Strategy Group, Inc. All Rights Reserved.

opportunities. As a result, more than half believe that email security is in a state of transformation and will reevaluate all security controls (including the ones they already own) currently available natively and via third-party solutions.[3]

Further advancements in prevention, detection, and response technologies are swinging the pendulum back towards a defense-in-depth approach, layering new types of security controls on top of modernized infrastructure.

Email Security a Top Priority

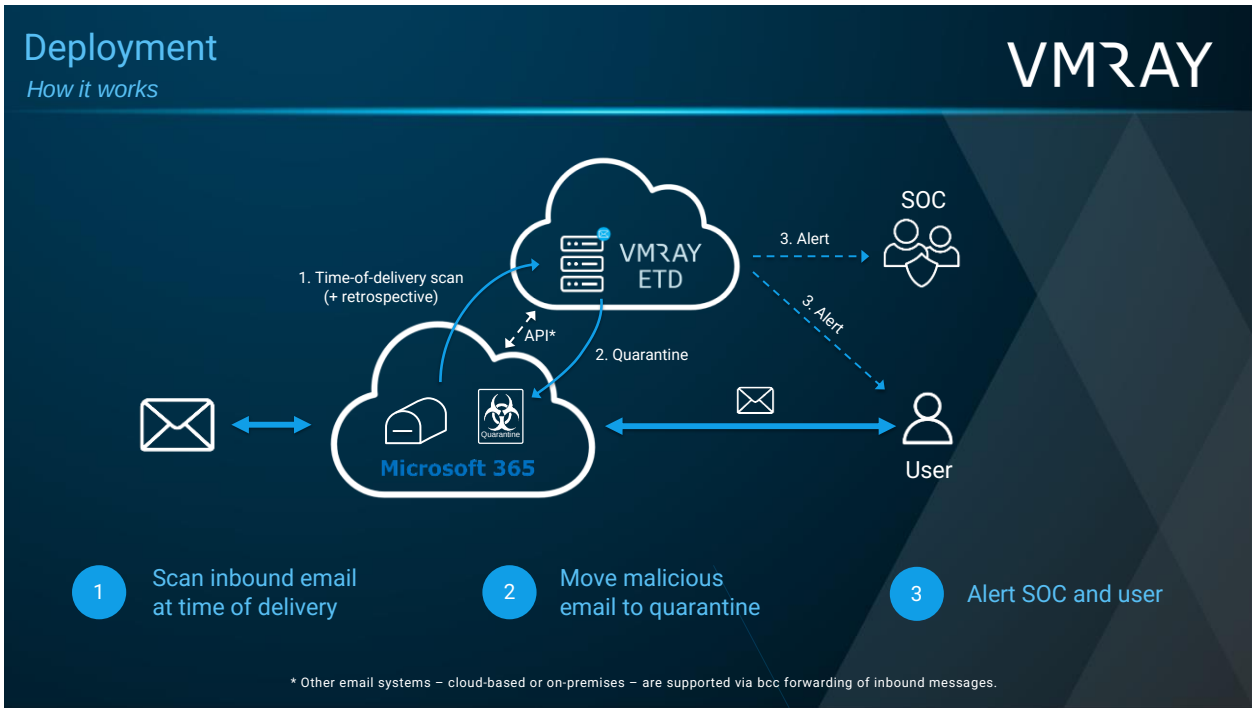
Over two-thirds (69%) of respondents to an ESG research survey report that email security has become one of their top 5 cybersecurity priorities.

With over 1.3M companies depending on Microsoft 365,[4] over two-thirds (69%) of respondents to an ESG research survey report that email security has become one of their top 5 cybersecurity priorities, with 18% citing email security as their most important cybersecurity priority.[5]

Introducing VMRay Email Threat Defender

VMRay Email Threat Defender (ETD) is laser-focused on stopping advanced email threats. Leveraging VMRay's proprietary, evasion-resistant, multi-layered scanning engines and unique sandbox technology, ETD is designed specifically to detect and stop threats that evade SEG and native M365 security controls. Using a multi-layered architecture that combines reputation lookup and static scans with unique dynamic sandboxing technology, ETD is entirely invisible to malware, detecting evasive threats.

Figure 1. VMRAY CESS Deployment Model



Source: VMRay

[3] Source: ESG Research Report, *Trends in Email Security*, August 2020.

[4] Source: Statista, *Number of Office 365 company users worldwide as of June 2021, by leading country*, June 2021.

[5] Source: ESG Research Report, *Trends in Email Security*, August 2020.

© 2021 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Installation and Configuration

- As a cloud-delivered security service, there is no hardware or software to install, and no need to change MX records when integrating with the Microsoft Office 365 email service. Instead, ETD uses a built-in, out-of-the-box API connector. Other email systems—whether cloud-based, on-premises, or hybrid—can also be supported via bcc forwarding.
- ETD sits behind a secure email gateway or built-in cloud email security controls (e.g., Microsoft 365 Defender, Google Workspace) to scan all emails at the time of delivery for advanced threats.

Administration and Management

- ETD features an easy-to-use console for administration and noise-free reporting. Reports vary from high-level dashboard views to actionable verdicts, empowering security teams and other parts of the organization to prioritize and contain email threats without delay.
- ETD further offers the option to automate email quarantine management and incident notification, so users' mailboxes are protected 24/7.

The Bigger Truth

Modern, advanced threats are evading current email security controls, leaving organization at risk of significant business interruption and potential financial losses. Recent focus on the detection and prevention of these advanced threats is creating new layered security offerings, enabling IT and security teams to easily strengthen security posture and reduce the penetration of these attacks. Many solutions are fully cloud-delivered, making the barrier to entry extremely low to add advanced threat protection.

ESG recommends security teams of all sizes explore how these supplemental offerings from vendors like VMRay can strengthen email security controls and close gaps in native email security controls provided by cloud-delivered email solution providers. ESG recommends organizations begin by investigating the efficacy of these layered controls, which can often be easily added to existing controls using simple, out-of-the-box integrations with little to no configuration. Using this approach, organizations who are struggling to stop advanced email-borne attacks can quickly see and understand the types and numbers of threats that can be further detected and stopped using a layered security approach.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188

© 2021 by The Enterprise Strategy Group, Inc. All Rights Reserved.