Brief: Five Key Capabilities For Microsoft Office 365 Email Security

Microsoft Takes Steps In The Right Direction, But Microsoft Alone Might Not Be Enough

by Kelley Mak

June 29, 2016

Why Read This Brief

Productivity and collaboration tools are an essential technology component of workforce enablement, and because of its economics, scale, and familiar interfaces, Microsoft's Office 365 online productivity and collaboration suite has become very popular. However, firms don't always understand and prepare for the security considerations of a hosted environment — particularly for hosted email. In this report, we outline five key capabilities that security pros must deliver to secure their Office 365 email environment.

Key Takeaways

Your Email Security Requires Five Key Capabilities

Securing the Office 365 email environment is of paramount importance to the business, yet security pros don't always know where to start. To aid in this effort, we developed a checklist of five key capabilities: 1) comprehensive threat protection; 2) threat visibility and response; 3) encryption; 4) data loss prevention; and 5) privacy.

Microsoft Is Becoming A Security Player

Although Microsoft is taking major leaps in the right direction for providing threat protection and information security and privacy, there are capabilities where security vendors will continue to provide necessary value. However, Microsoft's commitment to a secure experience is evident, and security vendors will need to innovate beyond what Microsoft provides to stay relevant.

Brief: Five Key Capabilities For Microsoft Office 365 Email Security

Microsoft Takes Steps In The Right Direction, But Microsoft Alone Might Not Be Enough

by Kelley Mak
with Stephanie Balaouras, Alexander Spiliotes, and Peggy Dostie

June 29, 2016

Table Of Contents

Notes & Resources

Forrester interviewed 11 vendor and user companies: Area 1 Security, BAE Systems, Cisco, Cloudmark, Forcepoint, HPE, Microsoft, Mimecast, Proofpoint, Symantec, and Trend Micro.

Related Research Documents

Market Overview: Data Loss Prevention

S&R Pros Must Empower Employees To Prevent Phishing Attacks

TechRadar™: Zero Trust Network Threat Mitigation Technology, Q1 2015

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

Office 365 Provides Operational Benefits, Opens Up Security Challenges

Email remains a critical component of day-to-day business activity. Strong interest and adoption of Microsoft's Office 365 online productivity and collaboration suite has pushed email from the classic in-house, on-premises deployment model to a more simplified, hosted cloud solution. The economics, scalability, speed, and mobile-friendly value of the cloud mixed with the familiar interfaces of Microsoft Office products and an ecosystem of broader business technologies make Office 365 a very attractive solution for enterprises. But not so fast. While Office 365 provides many financial and operating benefits, it raises several security challenges. Specifically, S&R pros must now:

- **Evaluate Exchange Online Protection against third-party security solutions.** For an additional fee per user, S&R pros can adopt Microsoft's Exchange Online Protection and its Advanced Threat Protection to gain the kind of security protections third-party email security vendors typically provide, such as antispam and antimalware. However, many S&R pros tell us that after abandoning a third-party security vendor in favor of Exchange Online Protection, they had significant challenges with increasing volumes of spam and malware and reverted to the third-party security solution.
- **Assess the impact to the firm's privacy stance.** In October 2015, EU courts ruled Safe Harbor invalid, making way for the more stringent Privacy Shield agreement in early 2016. In addition, the EU Parliament approved the new General Data Protection Regulation (GDPR) that raises privacy fines up to 4% of a company's global turnover.[1] S&R pros, along with their privacy counterparts, need to understand where Microsoft physically stores data containing personally identifiable information (PII) and what technologies or capabilities they offer to enforce data residency. This is necessary not to comply with just the GDPR but with a global patchwork of privacy laws.[2]

Five Key Capabilities For Office 365 Email Security

The importance of email to the business makes securing Office 365 of paramount importance, yet S&R pros don't know where to start. To aid in this effort, we developed a checklist of five essential capabilities: 1) delivery of comprehensive threat protection; 2) threat visibility and response; 3) encryption; 4) data loss prevention; and 5) privacy. S&R pros should use these considerations to determine if their firm is covered by Microsoft's native email security capabilities or if they need to augment their email security with a third-party email security solution.

No. 1: Comprehensive Email Threat Protection

For complete email threat protection, you must deliver a set of comprehensive threat protection capabilities. This includes the ability to:

- **Provide effective antispam.** The levels of spam have fallen in the past few years.[3] Despite this drop, spam is still a major concern for many organizations due to its drain on productivity and potential for malice; it's also an indication that a company's email filtering solution is faltering. Antispam is a standard feature for Microsoft and email security vendors and uses a combination of heuristic and reputation analysis.
- **Categorize graymail.** Not all spam is necessarily spam. Graymail or bulk email is email traffic that some users want and others do not, such as clothing or electronic stores' advertising emails. How does your email solution handle these types of emails to ensure safety for users? You want a solution that assists with the categorization and dissemination of graymail outside of spam and provides safe unsubscribe options.
- **Protect employees from email attachments containing malware.** Combatting antimalware will typically need more than the signature antivirus (AV) and heuristics present in most email security providers. Signature AV techniques can identify known malware but will suffer against unknown threats. Robust static analysis and dynamic analysis are important tools to mitigate the risk of emails equipped with malicious payloads. By detonating attachments in sandbox environments, email security tools from vendors such as Cisco, Proofpoint, Symantec, and Trend Micro can uncover the behavior of attachments.
- **Protect employees from malicious URLs.** Malicious emails can also employ malicious URLs instead of attachments as the attack vector. In these cases, scanning links initially at the gateway may not identify them as bad, but they can change characteristics at the time of user interaction. URL rewriting protects users to make sure the URL is scanned when clicked and also provides intelligence to email administrators on what happens post-click.
- **Deliver safe emails to employees.** The prevalence of emails with malicious attachments or URLs has ushered in the need for organizations to sanitize emails through document conversion, delivering of the email while holding the attachment in a sandbox, or erasure of any vulnerable element of the email. While not necessary for all organizations, there are targeted use cases where this is helpful, particularly for employees who do not need to interact much with documents. Vendors like Glasswall, Mimecast, and Votiro provide solutions here.
- **Prevent phishing and other fraud.** Not all attacks will include a malicious payload or URL. Email fraud has experienced an uptick in the past year with attacks such as whaling and business email compromise. Criminals aim these attacks at executives or individuals with access to valuable information or processes. Between October 2013 and August 2015, US businesses suffered more than $747 million in losses due to business email compromise where an attacker tricks an employee to initiate a fraudulent wire transfer.[4] Seagate recently was the victim of a whaling attack in which an employee sent the tax information of current and former employees to an email address impersonating Seagate's CEO.[5] Vendors such as Cloudmark, GreatHorn, and Mimecast provide solutions here.

No. 2: Email Security Incident Detection, Analysis, And Response

Despite your best efforts, there will undoubtedly be times when emails make it through your email security gateway. This makes the ability to detect, derive intelligence from, and respond to incidents critical for security teams. Security analysts will need the ability to:

- **Analyze email security incidents and determine the appropriate response.** Security tools in these scenarios need to provide a workbench for analysts to parse emails, analyze and enrich it with both internal and external intelligence, determine its severity, and respond accordingly. S&R pros should seek tools that enable easy investigation through full context, clean visualization, and clear workflows. Additionally, the ability to perform post-delivery actions in cloud-resident inboxes is helpful. Solutions like GreatHorn and Proofpoint have threat response capabilities that can help here.
- **Automate analyst activities.** The security automation and orchestration space is just starting to heat up. One of the most valuable use cases that solutions like Invotas or Swimlane provide is the ability to quickly sift through the contents of the security team's abuse mailbox. S&R pros should expect vendors in the email security space to begin to introduce features of automation and orchestration that enable investigations in speedier formats. Additionally, S&R pros' adoption of email security solutions should build upon an integrated portfolio of tools that helps reduce operational friction.[6]

No. 3: Email Encryption

Employee inboxes are a treasure trove of sensitive information and intellectual property for attackers. Tales from the unencrypted, such as at Sony, have shown the ramifications of exposed data on the brand and consumer privacy.[7] Encryption is a necessary component for business communication because it obfuscates sensitive data from cybercriminals and shields enterprises from the requirements of data breach laws. When choosing an encryption solution, S&R pros must be able to:

- **Keep encryption simple.** Strong cryptography is rarely broken but is often unused or bypassed. If the experience of using encryption tools is overly cumbersome, employees will work around it. It can also be cumbersome for the security pros to manage encryption keys effectively, and poorly managed keys can lead to data unavailability. Solutions such as Cisco, Hewlett Packard Enterprise (HPE), Symantec, and ZixCorp aim to simplify email encryption.
- **Encrypt email end to end.** Data, while in transit or at rest, needs to stay protected. Select an encryption solution that provides full life-cycle data protection, regardless if accessed internally, externally, or through a mobile device. Hosted or on-premises encryption solutions can help with this as well as provide alternatives to often complex and difficult-to-manage OpenPGP or S/MIME implementations. For example, encryption solutions can encrypt emails before they're stored in the Microsoft cloud and give S&R pros control of the encryption keys.

No. 4: Email Data Loss Prevention

Data loss prevention (DLP) technology uses policy to automatically detect and optionally block the transmission or storage of sensitive data. Email gateways from vendors such as BAE Systems, Forcepoint, and Symantec have DLP baked into their product. DLP is an important data security technology, but S&R pros have mixed experiences due to challenges in tuning policy, lackluster solution capability, and difficulty in deployment.[8] However, the value of DLP cannot be overlooked because it will help enforce security policy, such as encrypting all emails with PII, when employees don't think to. For email DLP to be successful, S&R pros need to:

- **Train email DLP to encompass sensitive information.** DLP can be easily applied to certain data types such as social security numbers or credit card numbers because those data strings are standardized and often come with solution templates. However, sensitive information like intellectual property, trade secrets, and risky communication is not as easy to identify. Implement a DLP tool that has a breadth of options and easy tuning capability that encompasses the range of data in your organization. However, DLP is not a silver bullet; it is a process you must continuously improve upon.[9]
- **Train users to be security minded before deploying DLP.** Employees are primarily concerned about doing their jobs, and they won't adopt any technology that adds friction to their day-to-day work. DLP provides timely feedback to employees as an educational feature. Engage with business leaders, corporate training departments, and human resources to help redefine your culture and the importance of adopting a security mindset so that you can effectively support a DLP initiative.
- **Apply DLP policy across the organization.** Email is only one critical channel for data loss; others include endpoint, network, web, and cloud. As data volumes grow and people access data across devices and cloud services, DLP policy must be consistently applied. Email DLP that can integrate with broader enterprise DLP policy can ease administrative headaches across disparate data loss channels.[10]

No. 5: Granular Data Control And Localization To Support Privacy

If you've been ignoring it, you can no longer: Privacy is a part of the global conversation. Concerns from the Apple encryption controversy to the striking down of Safe Harbor show that customers value privacy, and enterprises and businesses must embrace it to win, serve, and retain them. Office 365's role as a cloud solution means that S&R pros need the ability to:

- **Enforce data localization.** Microsoft has data centers dispersed all over the globe, and S&R pros need to know with certainty which data centers store their data. There is a complex patchwork of legal and regulatory requirements that dictate where and how firms collect, use, store, and transmit PII about employees and customers. Firms need to abide by these laws to avoid privacy violations as well as the ire of customers concerned about government surveillance. Microsoft has region-specific servers and commits to aligning data residency requirements to regulations and customer specification. Enterprises should have constant visibility and knowledge of where their data is stored and should know how it's encrypted and protected.

› **Know what data is where.** Aside from knowing where the data is, S&R pros need to know what kind of data is even in their email store. Business users tend to send sensitive information, whether that's PII or IP, without a second thought, and this ends up living in employee inboxes. Enterprises should undergo data discovery and classification efforts to understand what types of sensitive information are buried in email inboxes. Vendors like Identity Finder and Titus provide solutions here. Also, firms should set granular access policies to limit where certain types of data and emails are accessed on employee devices as well as implement data retention policies.

Recommendations

Office 365's Embedded Email Security Is A Starting Point, Not The End

While Microsoft is taking major leaps in the right direction of providing threat protection and information security and privacy, there are capabilities where security vendors will continue to provide necessary value. However, Microsoft's commitment to a secure experience is evident, and security vendors will need to innovate beyond what Microsoft provides to stay relevant. Going forward, S&R pros will need to:

› **Determine what capabilities their email security stack lacks.** Checklist the five key email security considerations to your Office 365 environment to see what your current defenses look like. Microsoft has covered a lot of bases and is continuing to expand its effort, but it is relatively new to fighting advanced threats, providing enhanced DLP, and supporting robust encryption.

› **Determine who the right partners are to help bolster their security forces.** Email security gateways vendors such as BAE Systems, Cisco, Forcepoint, Mimecast, Proofpoint, Symantec, and Trend Micro have seen great adoption of Office 365 among their customer base and have seen continued use of their products due to the advanced threat and information protection features of their solutions. Alternatively, solutions like Area 1 Security, Cloudmark, and GreatHorn provide specific advanced threat protection value that works well with Exchange Online Protection, and HPE and Zixcorp can provide email encryption solutions for Office 365.

› **Maximize security coverage while minimizing expense in depth.** Combatting the email threat vector requires a multilayered approach that addresses the breadth of attack scenarios out there. Yet, this doesn't mean throwing technology at the problem. Redundant technology areas can lead to diminishing returns. With a constrained security budget, carefully evaluate whether or not it makes sense to employ a comprehensive email security gateway either on-premises, in the cloud, or as a hybrid, or if it makes sense to invest in Exchange Online Protection with added support from advanced security technology.

› **Don't approach email security in a vacuum.** Email security is only one part of your entire security portfolio. Implement email security tools that play well with the rest of your security platform to ensure that security threat intelligence can be derived from and applied to the email channel. Additionally, Office 365 is a broad suite of business applications, so S&R pros should approach it as such. Evaluate tools whose current offering and strategy take this into consideration.

Supplemental Material

Companies Interviewed For This Report

Area 1 Security
BAE Systems
Cisco
Cloudmark
Forcepoint
Hewlett Packard Enterprise
Microsoft
Mimecast
Proofpoint
Symantec
Trend Micro

Endnotes

[1] Source: Enza Iannopollo, "The EU General Data Protection Regulation (GDPR) Is Here," Enza Iannopollo's Blog, April 20, 2016 (http://blogs.forrester.com/enza_iannopollo/16-04-20-the_eu_general_data_protection_regulation_gdpr_is_here).

[2] To help security and risk professionals navigate the complex landscape of privacy laws around the world, Forrester created a data privacy heat map that highlights the data protection guidelines and practices for 54 different countries. It also covers other relevant issues like government surveillance, cross-border data transfers, and regulatory enforcement. See the "Forrester's 2015 Data Privacy Heat Map" Forrester report.

[3] Source: "Spam email levels at 12-year low," BBC, July 17, 2015 (http://www.bbc.com/news/technology-33564016).

[4] Source: "Business Email Compromise," Federal Bureau of Investigation, August 27, 2015 (https://www.ic3.gov/media/2015/150827-1.aspx).

[5] Source: Sean Gallagher, "Seagate employees' W-2 forms exposed in another payroll phish," Ars Technica, March 8, 2016 (http://arstechnica.com/security/2016/03/seagate-employees-w-2-forms-exposed-in-another-payroll-phish/).

[6] Targeted attacks continue to plague organizations, and these intrusions damage the brand, customer loyalty, and margins. Preparing for and responding to these attacks requires a focused and resolute strategy. We designed Forrester's Targeted-Attack Hierarchy Of Needs to give S&R professionals a framework to accomplish this. See the "Forrester's Targeted-Attack Hierarchy Of Needs: Assess Your Core Capabilities" Forrester report.

[7] Source: Mark Seal, "An Exclusive Look at Sony's Hacking Saga," Vanity Fair, March 2015, (http://www.vanityfair.com/hollywood/2015/02/sony-hacking-seth-rogen-evan-goldberg).

[8] Data loss prevention (DLP) remains a key technology to help prevent the leakage and exfiltration of the firm's most sensitive data. Using client feedback, survey data, and input from security leaders in Forrester's Security & Risk Council, we looked at DLP with a different lens to address common pitfalls and implementation challenges. In this report, we help S&R pros assess the current state of their DLP efforts against data loss vectors and process maturity. See the "Rethinking Data Loss Prevention With Forrester's DLP Maturity Grid" Forrester report.

[9] Data loss prevention (DLP) remains a key technology to help prevent the leakage and exfiltration of the firm's most sensitive data. Using client feedback, survey data, and input from security leaders in Forrester's Security & Risk Council, we looked at DLP with a different lens to address common pitfalls and implementation challenges. In this report, we help S&R pros assess the current state of their DLP efforts against data loss vectors and process maturity. See the "Rethinking Data Loss Prevention With Forrester's DLP Maturity Grid" Forrester report.

[10] Policies to control data use and movement require enforcement mechanisms. Data loss prevention (DLP) capabilities give security and risk (S&R) professionals the means to enforce those policies and prevent sensitive data exposure. Today, S&R pros can source DLP capabilities in a variety of ways. See the "Market Overview: Data Loss Prevention" Forrester report.

FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

- Core research and tools
- Data and analytics
- Peer collaboration
- Analyst engagement
- Consulting
- Events

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals

CIO
Application Development & Delivery
Enterprise Architecture
Infrastructure & Operations
- Security & Risk

Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

133781