cirius

Product Briefing: Enhancing and Securing Microsoft Office 365 Email

Contents

According to Gartner, the adoption of cloud-based email will grow by more than 30% per year through 2022, to almost 700 million users, a more than 6x increase from today[1].

Microsoft Office 365 is leading the way in deployments of cloud-based email in the enterprise with 80% of the Fortune 500 already using Office 365 and an estimated 50,000 new small and midsize businesses signing up for Office 365 every month[2].

Many enterprise deployments of Office 365 have been driven by the need for organizations to upgrade from a previous generation Microsoft Office productivity suite. However, some organizations have initially been hesitant to adopt some of Office 365 functions, including moving their legacy email systems to cloud-based email. One of the primary reasons for this slower adoption has been lingering concerns about security including data privacy, regulatory compliance, and doubts whether cloud-based email security could effectively replicate the needs fulfilled by legacy on-premises systems.

Organizations are now realizing more and more that the productivity gains and benefits of moving to Office 365 outweigh security concerns. In many cases, organizations are discovering that third-party tools can alleviate security concerns, as well as enhance the productivity benefits of Office 365. Gartner projects that by 2018, 40% of organizations adopting Office 365 will rely on third-party tools to fill gaps in Office 365 security, moving to 50% by 2020[3].

Office 365 represents an opportunity for organizations to gain efficiencies in their IT costs as well as enable their workforce to be more productive, mobile and agile. This document, developed by Cirius in conjunction with Gartner highlights the potential needs and options for Office 365 security, and sheds light on how organizations can enhance their security and productivity as they transition to Office 365. We hope you find the information in this briefing helpful as you consider how to enhance the security of Office 365 for your organization.

Bob Spina
Chief Revenue Officer
Cirius

Gartner

[1]How to Evaluate Google Apps for Work Versus Microsoft Office 365, Gartner Research, January 2015
[2]Microsoft's Cloud Bets Pay Off as Office 365 Sees Big Growth, July 23, 2015
[3]How to Enhance the Security of Office 365, Gartner Research, November 2015

Cloud Adoption Becomes Mainstream

In recent years, organizations have increasingly adopted cloud-based email suites in an effort to lower IT costs and administrative overhead, better manage mobile and remote workers, and increase scale capacity. Originally purchased for its productivity suite, Microsoft Office 365 has been adopted in enterprises and small and midsize businesses.

Many IT organizations' concerns about the security of cloud-based services have prevented them from otherwise benefiting from those services. In particular, data privacy, data jurisdiction and regulatory compliance issues have troubled CIOs concerned about what information is being shared and stored outside their network via email and file sharing.

A new view on Office 365

A new view from IT organizations that recognizes the extensive benefits of moving to the cloud has caused a significant shift in the adoption of Office 365. Cloud-based applications such as Office 365 have typically appealed to enterprises due to transfer of costs from capital expenditures to operating expenditures and the ability to incrementally scale with growing needs. This has permitted organizations to adopt solutions without significant upfront commitment of resources and avoid a large step function in expenses to accommodate expanding needs. New innovations from Microsoft such as unlimited email storage options will continue to make Office 365 more scalable and incrementally more cost-effective and attractive vs. on-premesis solutions.

Recently however, a new emerging driver for the adoption of Office 365 is the increasing number of enhancements and new features that are being rolled out for the Office 365 platform. A shift to a "cloud only" and "cloud first" approach to rolling out new features by Microsoft and other vendors developing enhancements for Office 365 has meant that enterprises not adopting Office 365 may miss out on new features.

While Microsoft continues to support on-premises solutions, there is a significant shift to a "cloud-first" model of new feature releases and, in some situations, a cloud-only approach in which new features may not migrate to legacy on-premises solutions.

Current examples of features that are being rolled out in Office 365 indicate the attractiveness of these new features, which includes smart inboxes, smart virtual assistants, and content visualization and discovery. These and other innovations have the potential for significant productivity benefits that would be missed if organizations decide to stay with on-premises email systems.

Taking this into account, organizations more and more may opt to move to cloud-based Office 365 in order to gain from new cloud-based innovations and features. As a result, senior executives are increasingly asking IT leaders to consider and plan for a move to cloud-based systems. IT organizations, in turn, need to be prepared for the possible pitfalls that come from cloud-based deployment of email, including data security, data jurisdictions of data, and ensuring regulatory compliance.

Enabling the New Workforce

Organizations of all types today are driven by the need to respond nimbly to new innovations and increased competition, as well as the requirement of offering better services while simultaneously lowering costs. This, in turn, has increased the need to better communicate and share information internally, as well as with customers and business partners. The use of outsourcing, new business partnerships, and faster, more effective customer communication have made organizations more interdependent and reliant on technology to collaborate and share information efficiently across multiple organizations and locations. In addition, much of this communication is now happening over mobile devices.

The result is the increase in sharing of often confidential, private and proprietary information over multiple organizations and devices. Organizations that need to communicate and collaborate more easily with employees, customers and partners, while protecting intellectual property and maintaining regulatory compliance need to look for solutions that enhance productive sharing of information, rather than impede it. They require tools that support productive information workflows while simultaneously securing information. This allows them to take advantage of cost effective and easy-to-use cloud-

based messaging applications such as Office 365 and use them as productivity enhancing tools while maintaining security of messages, documents, and application-generated information workflows.

Requirements for Office 365

IT leaders need to understand the security, compliance, and data privacy implications for their organization when moving to a cloud-based deployment such as Office 365 for email. Among primary concerns is the need to assess the transition of existing on-premises email security, including email anti-virus/anti-malware, anti-spam, and email encryption solutions.

IT organizations also need to look for solutions that can easily integrate into Office 365 in order to minimize the switching between applications, and maximize the use of secure solutions. Solutions that require separate authentication, or that require another distinct application or user interface, are counterproductive to the productivity enhancements the organizations seek.

While doing this, IT leaders should focus on those applications that are easy to use for both internal as well as external users, and that are seamless across all devices, to maximize adoption.

Finally, with the move to cloud-based email with Office 365, IT organizations should assess the needs of the organization and the ability to support existing information workflows. In fact, the transition to Office 365 provides an opportunity to look at streamlining existing workflows and transitioning existing non-digital workflows to secure digital ones. For example, the ability to integrate an e-signature functionality directly into Office 365 would facilitate the transformation and streamlining of approvals and authorizations that already exist within an organization as well as with customers or partners.

By facilitating existing workflows, IT organizations can also reduce the risk of data breaches and exposure. For example, supporting secure large file transfer capability limits the use of unauthorized and potentially insecure file sharing services, facilitates and supports workflows such as the sharing of medical files or other large images, documents and files.

In summary, by reviewing and understanding existing information workflows within the organization, IT leaders can look for ways to lower cost as well as support and enhance productivity and information security.

About The Cirius Secure Productivity Suite

The Cirius Secure Productivity Suite is a cloud-based solution that helps organizations securely and productively use Office 365 email. Cirius makes it easy for organizations to support their existing workflows by securely sending and receiving email, files, and e-signature documents from Office 365 through Outlook or the OWA interface. In addition, Cirius provides an integrated, patented delivery slip which allows users to track and control messages, files, and e-signature documents internally, and with customers and partners. By delivering one-click encryption, large file sharing capabilities, advanced message tracking and control, and secure electronic signatures, Cirius helps organizations save time and cut costs while protecting private data and complying with company policies and industry regulations.

Cirius runs in Microsoft Azure as a cloud-based application with a client that integrates directly into Microsoft Office 365 so that users can securely send, track and control messages and files in Outlook, Outlook Web Access (OWA), or on a mobile iOS, Android, Windows 10, or Blackberry device. It goes beyond encryption to control messages (true recall, opened or unopened messages, prevent forwarding, etc.) and delivers real-time activity notifications the moment a secure message is received, opened, answered or forwarded.

The Cirius Secure Productivity Suite integrates into third-party applications, including Salesforce and Microsoft Dynamics, to secure existing information workflows from these and other applications. Cirius also integrates with Microsoft DLP to provide a rules-based alternative to simply blocking messages, as well as support for e-discovery and third-party archiving.

The ability to approve and e-sign documents in Outlook and on mobile devices, safely receive information via secure web forms, and share large files securely, improves efficiency for organizations. Additionally, organizations can use Cirius to reduce the volume of paper used and wasted by switching to a faster, more secure method to secure their information workflows.

Key Features:

- **Encrypted Messaging:** Send, receive, and track corporate email securely on any device, including smart phones and tablets, with enterprise-level encryption.
- **Secure Large File Sharing:** Share large files up to 5 GB quickly, and know in real time when and how information was received. Large files sent through Cirius will not clog the recipients inbox and they are unaffected by email bandwidth limitations.

- **Secure E-Signatures:** The Cirius Secure E-Signature solution makes it simple for users to electronically sign documents directly within email without any additional apps or workflow, saving substantial time and money. Unlike other e-signature solutions, Cirius protects sensitive information by authenticating users and securing e-signed documents throughout transmission and storage, ensuring data integrity, regulatory compliance, and non-repudiation.

- **Single Sign On (SSO) Support:** Cirius supports existing single sign-on solutions, including OAuth and SAML, to facilitate integration into the organization's infrastructure.

- **Delivery Slip Control Panel:** The Cirius patented delivery slip embeds into Outlook, Office 365 OWA, and other email clients to provide easy, one-click access to the robust feature set.

- **Advanced Message Control:** Control emails via patented functionality such as Forward freeze, Reply freeze, FYEO ("For your eyes only") and total message recall.

- **API connection to other applications** In addition to Office 365, the Cirius Secure Productivity Suite can be integrated into other third-party applications including Salesforce and Microsoft Dynamics though the Cirius API.

- **Mobile Client:** The Cirius mobile client supports full functionality including secure messaging, large file transfers, e-signatures, and message tracking and control for iOS, Android, Windows 10, and Blackberry devices.

- **Secure Web Forms.** Organizations may use Cirius to receive and manage information submitted through secure web forms which are sent directly to the users' inbox.

- **Five Minute Integration:** The Cirius Secure Productivity Suite easily integrates into existing networks with no MX record changes.

- **Simple Guest Registration:** Guest registration is a simple two-step process, facilitating the use of B2B and B2C collaboration.

It is no longer required for organizations to accept a trade-off between security and productivity. Cirius delivers the perfect complement to Office 365 and other email and cloud-based applications by delivering a highly-secure business communications and collaboration solution that integrates quickly, improves workflows, protects confidential information, intellectual property and other sensitive data. Many organizations have adopted the Cirius Secure Productivity Suite because the solution:

- Enables users to stay in Outlook, Office 365 or OWA, without switching to webmail or creating a separate account

- Extends productivity features such as secure e-signature and large file transfer to the entire organization through the Outlook or OWA interface

- Provides extensive message tracking, including real-time activity notifications the moment a secure message is received, opened, answered or forwarded

- Enables users to control messages, files, and e-signature documents, including recall opened; prevent forwarding, and additional security

- Integrates easily into existing infrastructure, supporting common Single Sign On (SSO) methods and without changes to MX records

- Connects with Office 365 DLP to provide a rules-based alternative to simply blocking messages containing confidential information

Source: Cirius

Research from Gartner

How to Enhance the Security of Office 365

Office 365's security continues to improve, offering native capabilities beyond what enterprises have had in previous on-premises deployments. Security and risk management leaders should use the Gartner SaaS security framework to pursue opportunities for future enhancements with third-party tools.

Key Challenges

- Organizations must contend with a proliferation of disparate devices that access Office 365, many of which are unmanaged.
- Traditional security tools, designed for protecting on-premises systems, can't offer visibility and control when enterprises move email, content creation, file sharing and collaboration to the cloud, making the detection of inappropriate behaviors difficult.
- Although Microsoft has simplified administering Office 365 security, certain controls require higher-priced licensing options. In some cases, third-party tools compete with lower prices and enhanced capabilities.
- Some Gartner clients report that Microsoft's more-sophisticated controls perform poorly or lack necessary capabilities.

Recommendations

Security and risk management leaders responsible for cloud security should:

- Examine whether Microsoft's native capabilities are sufficient and for which use cases.
- Evaluate third-party alternatives when gaps prevent them from implementing their policies.
- Begin with an identity, access and privilege management strategy, on which all other controls rely.
- Implement appropriate visibility, data security, threat protection and device management controls using native Office 365 capabilities, enhanced with third-party products, where necessary.
- Use a cloud access security broker to achieve the most consistent security policies across all Office 365 services and other non-Microsoft SaaS applications.

Strategic Planning Assumptions

By 2018, 40% of Office 365 deployments will rely on third-party tools to fill gaps in security and compliance, which is a major increase from less than 15% in 2016.

By 2020, 50% of organizations using Office 365 will rely on non-Microsoft security tools to maintain consistent security policies across their multivendor "SaaSscape."

Introduction

Once an umbrella brand that encompassed multiple, cloud-based, Microsoft enterprise productivity services, Office 365 is now coming together as a cohesive product that consists of several SaaS workloads. Although different product teams manage these services, Microsoft has consolidated many of the security controls into fewer consoles and fewer, more comprehensive APIs, which simplifies security administration. Microsoft has improved native Office 365 security controls to the point where an Office 365 tenant can be more secure than an on-premises deployment of the same services.

Not all security controls are available in every subscription plan. Security and risk management leaders will need to carefully evaluate their security requirements to select the appropriate plan and any required or optional add-ons. Furthermore, some organizations might have security requirements sufficiently stringent that they still require additional spending on third-party tools. Where necessary, security and risk management leaders responsible for cloud security should consider additional security processes and products to achieve the required visibility into Office 365, as well as across an organization's SaaSscape. In this regard, most organizations are likely to adopt third-party tools.

To use Office 365 securely, develop a framework for a discussion of the required security controls. Figure 1 illustrates Gartner's SaaS security framework. (See Figure 1 on Page 6) This framework has two primary security dimensions:

- Secure access
- Threat protection

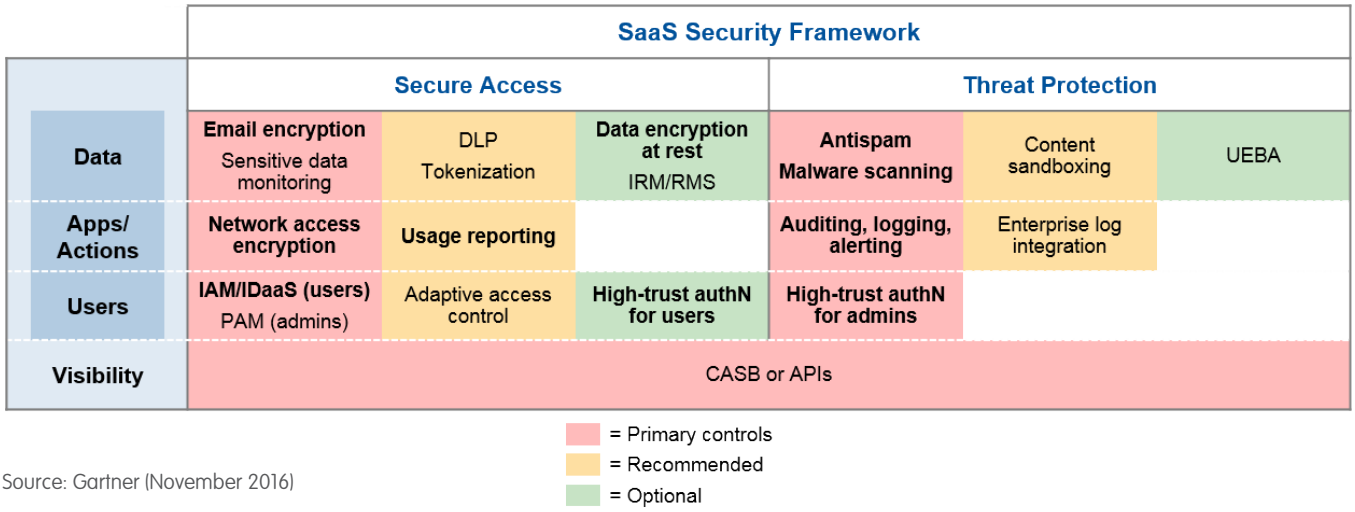
Visibility and control are required for users, actions, applications and data across both dimensions. This research describes Microsoft's native controls in each category in the diagram and includes third-party alternatives with additional functionality. If Microsoft's native capabilities in each category are sufficient for your needs, use them. If they're insufficient, evaluate third-party choices.

The shading indicates our suggested prioritization for securing Office 365. In Figure 1, the **bolded items** are included with all Office 365 plans and are enabled by default or can be enabled by a configuration setting.

- **Pink:** Deployments *must* address these required capabilities.
- **Yellow:** Deployments *should* address these recommended capabilities.
- **Green:** Deployments *could* address these optional capabilities.

Because Microsoft's cloud-based services provide little to no capability for enterprises to use their on-premises agents, network probes, firewalls and similar equipment to secure their Office 365 data and activities, enterprises should be prepared to shift their

FIGURE 1
Gartner Framework for SaaS Security Controls



Source: Gartner (November 2016)

mindsets. Traditional perimeter protection gives way to an information-centric strategy, which is focused on secure access and usage and has threat protection via native capabilities, APIs or other mechanisms.

Gartner's framework doesn't reference multitenant platform security. Microsoft's internal security controls are sufficient for protecting subscribers from each other. Customers shouldn't worry about information "bleed" among subscribers. Nor should they be overly concerned about infrastructure-level attacks, such as a denial of service (DoS). Microsoft has demonstrated proper due diligence and has achieved numerous control attestations.

Analysis

Begin With Identity, Access, and Privilege Management

Securing Office 365 begins with an identity and access management (IAM) strategy. The easiest approach would be for an enterprise to federate its on-premises Active Directory (AD) with Office 365 via Azure AD, which is included at no extra cost. Federation enables single sign-on (SSO) for Office 365 and other SaaS applications. Most of the controls described in the framework work best with or require federation. Federation is needed to support login policies, such as domain join requirements, smart cards and third-party multifactor authentication.

If you don't have an AD forest, or if you have a complex directory configuration and prefer to avoid federation, create cloud identities within Office 365 itself or synchronize identities (and, optionally, passwords) with Azure AD. An alternative is to use a third-party IAM as a service (IDaaS) provider. As with Azure AD, these typically satisfy the same requirements that federation does, and offer SSO across multiple SaaS applications (see Table 1).

Adaptive access controls bring context awareness (such as location and time of day) into access control decisions. They balance the level of trust against risk at the moment of access, using a combination of trust elevation and other dynamic risk mitigation techniques. Azure AD Identity Protection, available in the extra-cost Azure AD Premium P2 plan, provides this capability for Office 365 and other SaaS applications, as do third-party tools and several cloud access security brokers (CASBs).

Administrator accounts are rich targets for attack and require additional protection through higher trust authentication, typically involving multiple factors. All Office 365 editions include a basic two-step authentication capability (available for all account types, not just administrators). A more feature-rich option that works for Office 365 and other SaaS applications is Azure Multifactor Authentication (MFA), available separately (priced pay-as-you-go) and included in Azure AD Premium P1 and P2 plans and in Enterprise Mobility Suite. A number of third-party MFA products are also supported.

Simply adding more factors can give a false impression of security, especially if those factors (e.g., hardware tokens) are easily shareable. One-time soft tokens and privileged access management (PAM) tools enable higher trust authentication. PAM tools provide a greater separation of duties than is possible natively in Office 365. Microsoft's PAM capability, Azure AD Privileged Identity Management, is available in the Azure AD

Table 1. IAM Capabilities and Vendors

Capabilities	Descriptions/Vendors
Native Capabilities	On-premises AD federated with Azure AD Cloud identities in Azure AD Role-based access control (RBAC) Support for user and administrator two-step authentication MFA for multiple SaaS applications (extra cost) Adaptive access control for multiple SaaS applications (extra cost) PAM for multiple SaaS applications (extra cost)
Example MFA Tools	Duo Security Gemalto (SafeNet) RSA SecurID Symantec VIP
Example PAM Tools	Centrify CyberArk Xceedium
Example Adaptive Access Control Tools	Entrust IdentityGuard Oracle Adaptive Access Manager RSA Adaptive Authentication
Example IDaaS Providers	Centrify Okta Ping Identity

Source: Gartner (November 2016)

Premium P2 plan; some third-party PAM tools also work with Office 365. Many PAM tools integrate with MFA products and support various SaaS applications, making them viable candidates if you subscribe to multiple services.

Recommendations:

- Use Azure AD Connect to simplify the work required to enable federation and consider Azure AD Premium or a third-party IDaaS.
- Ensure that the provider supports all necessary access types (e.g., desktop clients, native mobile clients and web browsers), as well as the locations (such as corporate networks and the public internet) and installed versions of Office clients, if considering IDaaS.
- Use Microsoft's predefined roles for each service in Office 365 as a starting point and design an RBAC policy that grants users and administrators the minimum set of permissions required to perform their jobs.
- Implement an adaptive access control if you wish to relax restrictions when risk is low and tighten restrictions when risk is high (executives visiting so-called dangerous places, for instance).
- Require higher trust authentication for all administrator accounts. If the included Office 365 two-step authentication doesn't meet your security requirements, consider Azure AD Identity Protection or look for a third-party tool that indicates membership in the "Works with Office 365" program.
- Evaluate the applicability of PAM tools. If required for audit purposes, select a tool that records all administrator activity.
- Safeguard against phishing attacks by extending higher trust authentication requirements to the accounts of users handling sensitive information as well. Phishing attacks frequently attempt to impersonate corporate officers.

Restore Visibility to User, Application and Data Behavior

Migration from an on-premises Microsoft 3CS deployment to Office 365 requires new approaches for achieving visibility into user, application and data behavior. All services provide activity reports that cover metrics such as service usage and user and application transactions. This information is

available in reports through the Office 365 Admin Center, downloadable spreadsheets and PowerShell scripts.

Audit reports for Exchange Online, SharePoint Online, OneDrive for Business and Azure AD are available in the Office 365 Security and Compliance Center. Audit reports show user and admin activity within an Office 365 tenant and can be searched for specific users or actions.

Two APIs offer programmatic views into Office 365 behavior. The Management Activity API provides a RESTful interface into all user and administrator transactions in Exchange Online, SharePoint Online, Sway and Azure AD. This API exposes a consistent schema across the services and simplifies integration with security information and event management (SIEM) tools, which is a common request from many Gartner clients. The Service Communications API provides information about tenant health, service incidents and maintenance events.

Office 365 Advanced Security Management (ASM), which is included in E5 plans and is available at extra cost for other plans, supplies a discovery dashboard that visualizes usage of Office 365 and other SaaS productivity applications with functionality similar to Office 365. Uploaded logs from on-premises firewalls and proxy servers provide the information that populates the dashboard. ASM is derived from Cloud App Security, Microsoft's CASB.

The rapid adoption of Office 365 has spurred the growth of a variety of third-party tools that increase visibility in one aspect or another, including such areas as:

- Activity and administration auditing
- Event collection and correlation
- Permissions monitoring
- User behavior analytics
- Anomaly detection
- Discovery of sensitive content

However, acquiring and managing a collection of tools from different vendors is likely to be expensive, time-consuming and prone to the risk of misconfiguration. CASBs offer a depth of visibility beyond native Office 365 capabilities and extend this with several important security controls (see Table 2).

Recommendations:

- Use activity reports to generate high-level dashboard views of activity within your tenant.
- Use audit reports to investigate specific user or administrator behavior.
- Evaluate the suitability and complexity of the Management Activity API and the Service Communications API, as well as third-party products for integration with SIEM resources.
- Evaluate whether ASM's discovery dashboard provides sufficient visibility for SaaS usage. If not, investigate using a CASB.

Secure Office 365 Content in Motion and at Rest

Securing connectivity to your tenant is straightforward, as Transport Layer Security (TLS) protects connections to all services when using native clients and browsers, ensuring that data in motion is protected from eavesdropping. Some on-premises, in-line devices that are common in enterprise networks, such as forward proxies and WAN optimization controllers (WOCs), will introduce additional certificate-handling procedures to keep TLS sessions intact.

Office 365 services use various means to encrypt data at rest. Although this sounds attractive at first glance, in reality, it principally mitigates the risk of physical storage devices leaving Microsoft data centers, which is an extremely unlikely event.

Two mechanisms are available for protecting email. Secure Multipurpose Internet Messaging Extensions (S/MIME) can encrypt or digitally sign email. S/MIME offers no predefined policies; users must remember to sign and/or encrypt email. An alternative to S/MIME is Office 365 Message Encryption, based on Azure RMS, which automatically encrypts email without user intervention. No public-key infrastructure (PKI) is necessary.

Table 2. Visibility Capabilities and Vendors

Capability	Descriptions/Vendors
Native Capabilities	Per-service activity reports Detailed audit reports APIs for management activity and service communications SaaS visibility (included in E5; extra cost otherwise)
Example Third-Party Visibility Tools	Alert Logic Cogmotive EventTracker Logentries Savyint Varonis

Source: Gartner (November 2016)

Recipients can be outside your organization and can send encrypted replies.

Office 365 Information Rights Management (IRM) uses Azure Rights Management Services (RMS) to apply per-file encryption, access control, usage policies and auditing that persist regardless of where a file is stored. IRM works with Exchange, SharePoint and OneDrive for Business, and is included with E3 and E5 plans. Authorized users can open files, but only when their identities can be verified and only on devices with software that can enforce the policies. (Recipients who lack an Office 365 or Azure AD identity will need to sign up for the free RMS for individual service.)

Azure Information Protection P1 and P2, available at extra cost, offer additional levels of control, including automated data classification, tracking and revocation, custom templates, and support for bring your own key (BYOK) and hold your own key (HYOK) requirements.

Third-party tools can provide application layer encryption for Office 365 services. Available either as on-premises virtual appliances or as cloud-delivered services, these tools encrypt data before delivering it to your tenant, providing additional protection for enterprises that don't fully trust Microsoft. Microsoft has no access to the keys used to encrypt the data. In most cases, encrypting information outside your tenant will reduce overall functionality. A small number of third-party encryption products claim to work around this limitation by performing "encryption in use."

Exchange Online, SharePoint Online, and OneDrive for Business include mechanisms for identifying sensitive data and controlling its spread. They are evolving into a more comprehensive data loss prevention (DLP) capability, included in E3 and E5 plans. DLP conditions perform deep content analysis through predefined sensitive information formats, custom keyword and dictionary matches, regular expression evaluation, document fingerprinting and other examinations to detect sensitive information in content that should be flagged.

DLP actions include raising policy tips for end users, notifying compliance officers, encrypting the content or completely blocking transfer. Policies can permit a user to override a decision by supplying a business justification or by reporting a false positive. Policies can also indicate exceptions (location-based exceptions can be particularly useful). Microsoft supplies a number of predefined DLP templates for common protection scenarios, such as Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI-DSS) and locale-specific personally identifiable information (PII). A logging mechanism records all DLP incidents. The parts of DLP that interact with users require native desktop applications, native mobile applications or the web app versions of Office.

If your organization subscribes to multiple SaaS applications, an alternative to enabling native Office 365 data security features would be to select a CASB that includes these capabilities. With a CASB, you can create centralized encryption, rights management and DLP policies across most popular SaaS applications (see Table 3).

Recommendations:

- Investigate the suitability of Office 365 platform-level protections or additional data security capabilities based on your risk tolerance, compliance requirements, and content storage and transmission requirements.
- Deploy an on-premises certificate authority if it's necessary for communicating with customers, partners or governments that require S/MIME signed and/or encrypted email. Office 365 does not include a certificate server or PKI.
- Configure Office 365 Message Encryption policies to automatically apply encryption when defined conditions are met.
- If you don't yet have a data classification process in place, evaluate whether Azure Information Protection is sufficient for starting one.

Table 3. Content Security Capabilities and Vendors

Capabilities	**Descriptions/Vendors**
Native Capabilities	Transport encryption and authentication Drive- and file-level platform encryption Email encryption IRM (with certain plans) Automatic classification (extra cost) DLP (with certain plans)
Example Third-Party Data Security Tools	BitTitan CipherPoint Proofpoint Vaultive
Example Data Classification Vendors	Titus Boldon James

Source: Gartner (November 2016)

- Evaluate and test third-party encryption products to determine whether the features are compatible with your environment and are sufficient for regulatory requirements.

- Use DLP conditions to establish a rudimentary type of document classification and to help meet compliance requirements. Use DLP policy tips to alert users to the presence of sensitive information, and begin teaching them how to properly handle such data.

Protect Your Office 365 Deployment From Threats

Several options can protect your subscription from external and internal threats. Generally, they address the threats posed by devices and their users or owners, although content-level threat protection is also an important element.

Exchange Online Protection, included with all plans, is a multiengine, anti-malware/anti-spam service with enterprisewide-allowed/blocked sender lists. Advanced Threat Protection (ATP), which is included in E5 plans and is available for others as an extra cost option, adds more capabilities. ATP offers message sandboxing, link reputation checking, URL reporting and tracing, and phishing protection. ATP sandboxing can delay delivery of the attachment by 15 to 30 minutes and, as with any network sandbox, sophisticated attackers can find ways to evade it.

Typically much faster than sandbox mechanisms, third-party tools can convert incoming attachments to less-dangerous reading formats for initial delivery. If the recipient needs the attachment in its original format, then a sandbox can process the contents.

SharePoint Online and OneDrive for Business use the same anti-malware technology as Exchange Online to scan files as they are uploaded. Infected files are quarantined and can't be downloaded. The service works only on files smaller than 25MB. On-demand scanning is unavailable.

Office 365 ASM, included in E5 plans and available at extra cost for other plans, offers user and entity behavior analytics (UEBA) across all Office 365 services. The service continuously scans user behavior for indicators of threat and other risky activity based on Microsoft's enormous global telemetry. ASM is derived from Cloud App Security, Microsoft's CASB (see Table 4).

Targeted attacks remain a challenge for many enterprises. Low-volume, high-value targeted attacks usually originate with spoofed email. Skilled attackers can penetrate even the best anti-phishing campaigns. From there, attackers find additional ways to spread inside an organization, following wherever the stolen credentials might lead. SSO adds convenience for organizations using multiple SaaS applications; however, it also adds convenience for attackers. An effective SaaS security strategy protects users as well as data. Devise procedures and deploy tools that encourage users to be careful with their IDs and passwords and to protect credentials from theft.

Recommendations:

- Continue to use a sender policy framework (SPF); DomainKeys identified mail (DKIM); and domain-based message authentication, reporting, and conformance (DMARC) to reduce the amount of spoofed inbound email. If not already in use, the migration to Office 365 presents a good opportunity to enable them.

- Use ATP's URL reporting and tracing to determine whether attackers are targeting specific individuals or business units.

- Substitute a third-party message hygiene service if Microsoft's content sandboxing (and its delay) is unsuitable for your organization.

- Evaluate whether ASM's UEBA provides sufficient anomaly detection for your Office 365 requirements. If you're using multiple SaaS applications, a CASB might be a better choice.

Extend Your Strategy to Managed/Unmanaged Devices

The coarsest level of device control is to limit all extranet access to your subscription and to force connections via a virtual private network (VPN) into your corporate network.

Table 4. Threat Protection Capabilities and Vendors

Capabilities	Vendors
Native Capabilities	Anti-malware/anti-spam Content sandboxing UEBA (included in E5, extra cost otherwise)
Example Third-Party Anti-Spam/Anti-Malware and Content Inspection	Fidelis Mimecast McAfee DLP and Email Protection Proofpoint Trend Micro
Example credential protection for SaaS	GreatHorn

Source: Gartner (November 2016)

Certain exceptions are possible for Exchange Online and SharePoint Online and for members of enterprise-defined AD groups. To enable these policies, you must federate your on-premises AD.

All commercial plans include free mobile device management (MDM) for Office 365. Office 365 MDM allows you to apply security policies to devices that connect to your tenant. A log records access from all devices. Office 365 MDM works with native Microsoft productivity apps installed on devices, rather than third-party PIM clients. Users self-enroll with devices running iOS, Android, Samsung Knox, Windows Phone, Windows 8.1 (ActiveSync only) and Windows 10 (requires Azure AD).

Capabilities vary, depending on the OS; however, there are some drawbacks. For example, you might already be using a third-party MDM product, none of which are capable of using the native Office 365 MDM APIs to manage apps or devices. Office 365 MDM also doesn't support non-Microsoft desktop operating systems (e.g., Mac OS and Linux). You can configure a policy to block unsupported devices and operating systems if you want to limit access to your tenant to managed devices only. However, even in this scenario, web browser access to your tenant bypasses Office 365 MDM.

For additional priced capabilities, you can add the full Intune service to your subscription. Among other controls, Intune includes policies that deploy certificates, Wi-Fi, VPN and email configurations. Users can self-enroll and install managed corporate mobile apps from a company portal app. Intune also can perform bulk enrollment to silently enroll all devices without user intervention. Intune can apply mobile application management (MAM) policies to apps even without device enrollment. Intune supports mobile and desktop OSs. Notably, to block movement of data between managed and unmanaged apps, you need the full Intune. Office 365 MDM lacks this capability.

Many Gartner clients have reported that Intune is challenging to configure and contains bugs that affect functionality. Third-party enterprise mobility management (EMM) suites are more popular in large organizations (see Table 5); however, they have some significant drawbacks. Microsoft's native apps don't use device-standard MDM hooks. Thus, they aren't manageable by third-party EMM suites, but this could change in the future.

In addition to providing improved visibility and consistent data security, CASBs offer a variety of threat protection capabilities, including content inspection/conversion, device management and adaptive access based on device parameters (such as OS and app versions, user behavior, and location). If your organization subscribes to multiple SaaS services, a CASB might be a better approach — you can create uniform threat protection policies across all services.

Recommendations:

- If you want to completely prohibit access from unmanaged devices, require that all access to your subscription be over a VPN into your corporate network.
- Determine whether to allow Active Sync over the internet for devices to receive email without a VPN connection.
- Determine whether to allow browser access for on-demand (but not synchronized) access to Exchange and SharePoint.
- Use the included Office 365 MDM to determine whether to permit or block noncompliant devices — if this is the only level of device control you need.
- Create MDM access controls that vary according to group membership — define stricter policies for users who work with sensitive data and relaxed policies for users who don't.
- Deploy Intune to apply additional restrictions (including application-level PIN locks) to managed apps, managed browsers, managed document and media viewers, and line-of-business apps placed in a wrapper.
- Evaluate a third-party EMM suite for broader device control and to include coverage beyond Office apps and content.
- Deploy Intune or third-party content creation apps that an EMM suite can manage to control data movement among applications. These apps might not be able to process rights-protected content or might require an add-on to do so.

Table 5. Device Security Capabilities and Vendors

Capabilities	Descriptions/Vendors
Native Capabilities	Client-based access control MDM Intune (at additional cost)
Example Third-Party Device Management and Policy Enforcement	AirWatch Good Technology MobileIron

Source: Gartner (November 2016)

Consider a CASB for Consistent Visibility, Control and Protection

Microsoft has made significant progress in building more security into Office 365 by broadening native capabilities across more of the various services. For some organizations, especially those for which Office is their only SaaS usage, Microsoft's native capabilities are likely to be sufficient.

Organizations that use multiple SaaS applications will experience challenges when trying to create coherent security policies using each application's native capabilities. CASBs overcome these challenges by providing a suite of controls that enable you to create consistent security policies across several popular SaaS applications. The most effective CASBs are multimodal, combining API-based data discovery, policy configuration, and auditing/logging with proxy-based, real-time inspection and control. CASBs support a wider range of managed and unmanaged devices and access methods, offering differentiated services that are unavailable in traditional security controls, such as web application firewalls (WAFs) and secure web gateways (SWGs). CASBs help you consolidate your security controls into a single management plane, avoiding the interoperability issues that arise when using multiple vendors for different controls.

CASBs deliver functionality around four pillars of equal importance (see Table 6).

Gartner is tracking approximately a dozen CASB vendors, most of which feature prominent support for Office 365.

Table 6. CASB Functionality

Functionality	Description
Visibility	CASBs provide shadow and sanctioned IT discovery, as well as a consolidated view of an organization's cloud service utilization and the users who access data from any device or location.
Compliance	CASBs assist with data residency and compliance regulations and standards, as well as identify cloud usage and the risks of specific cloud services.
Data Security	CASBs provide the ability to enforce data-centric security policies to prevent unwanted activity based on data classification, discovery and user activity monitoring of access to sensitive data or privilege escalation.
Threat Prevention	CASBs prevent unwanted devices, users and versions of applications from accessing cloud services by providing adaptive access controls.

Source: Gartner (November 2016)

Source: Gartner Research Note G00317721, Steve Riley, 15 November 2016

About Cirius

Cirius offers cloud-based solutions that help innovative organizations transform and secure their information workflows. Cirius makes it easy to secure, track, and control email messages, share large files and e-signature documents, and other cloud-based application information. Cirius integrates easily with Office 365, Outlook, and other email and cloud-based applications solutions to improve user productivity and facilitate information sharing and control, while maintaining industry and data privacy requirements from any application, on any device. Used by more than 8,000 organizations worldwide, Cirius can be used by any department to protect their information without changes to existing infrastructure. Cirius is the simplest, most secure way to share, track, and manage information workflows in the digital enterprise.

To learn more about the Cirius Secure Productivity Suite, please contact us today at sales@Cirius.com or call us at 1.888.362.4520 to learn more, and receive a 30-day free trial.