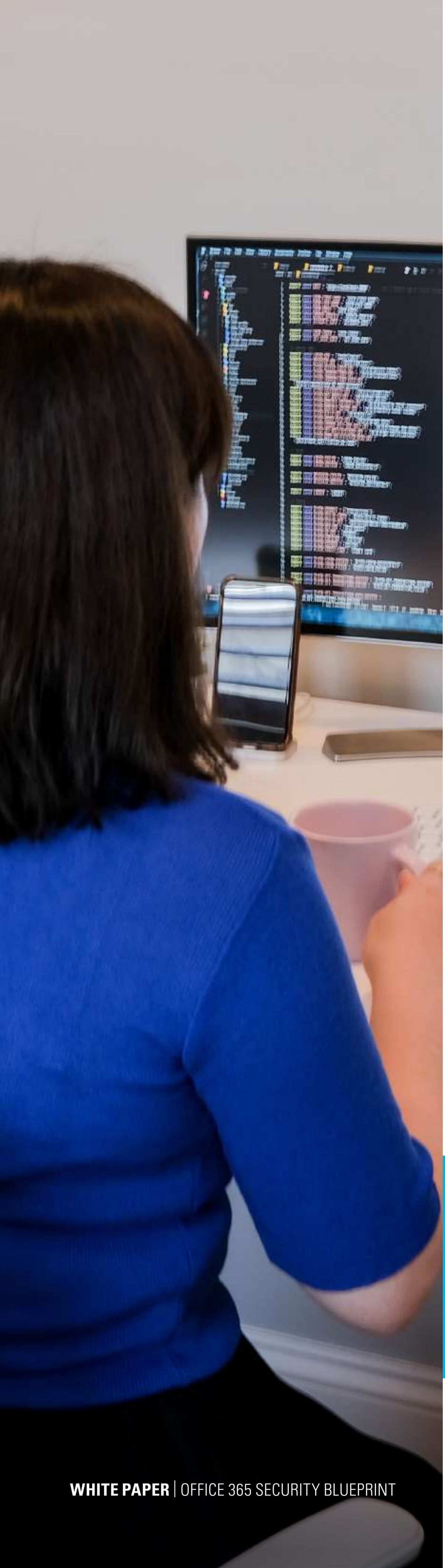
AN OFFICE 365 SECURITY BLUEPRINT FOR MIDSIZED ORGANIZATIONS

MOTOROLA SOLUTIONS



EXECUTIVE SUMMARY

Moving to Microsoft Office 365 is often the first step that midsized organizations take when migrating sensitive business activities to the cloud. Without careful consideration and planning though, adopting Office 365 can complicate security and compliance efforts. In this white paper, we discuss the wealth of security features within Office 365, along with third-party products and services that can enable organizations to achieve a strong security and compliance posture.

INTRODUCTION

Microsoft Office 365 is now the de facto standard for deploying and using Microsoft Exchange and the full suite of Microsoft Office business productivity applications. Midsized organizations, in particular, were early adopters of Office 365. They were driven by its simplicity and operational advantages compared to on-premise Microsoft Exchange and file server management.

The cost and efficiency benefits of Office 365 do come at a price, however. Shifting sensitive business data to the cloud means giving up direct control over where it is stored and how it is secured. It can also complicate compliances efforts, as Microsoft's infrastructure must now be considered as part of any compliance audits and assessments.

However, with the right cloud security systems and processes in place, along with third-party security solutions, most organizations can achieve a stronger security and compliance posture in Office 365 than with traditional on-premises infrastructure.

ACCORDING TO THE CYBERSECURITY INSIDERS 2019 CLOUD SECURITY REPORT:

66% Of survey respondents are using Office 365, leading all other SaaS platforms by a wide margin

41% Report "staff and expertise" as a barrier to cloud security solution adoption

SHARED RESPONSIBILITY MODEL

Like many cloud providers, Microsoft uses a shared responsibility model to define cloud security roles and responsibilities. In its simplest form, this means that:

- Microsoft is responsible for security of the cloud.
- Office 365 customers are responsible for security of their activities in the cloud.

	PRIMARY RESPONSIBILITY	SUPPORTING TECHNOLOGY	SECURITY	REGULATORY
THIRD PARTY'S RESPONSIBILITY	**Global Infrastructure** Uptime of the Cloud Service	**Office Data Replication** DC to DC geo-redundancy	**Infrastructure Level** Physical Security Logical Security App-Level Security User/Admin Controls	**Role As Data Processor** Data Privacy Regulatory Controls Industry certifications HIPAA, Sarbanes-Oxley
		Recycle BIn Limited, short term data loss recovery (no point-in time recovery)		
YOUR RESPONSIBILITY	**Your Office Data** Access and control of your data residing in Office	**Office Backup** Copy of your data stored in a different location	**Data-Level** Internal: Accidental Deletion, Malicious Insiders, Employee Retaliation, Evidence Tampering External: Ransomware, Malware, Hackers, Rogue Apps	**Role As Data Owners** Answer to corporate and Industry regulations Demands from internal legal and compliance officers
		Full Data Retention ST & LT retention filling and/ all policy gaps granular & point-in time recovery options		

IMPLEMENTING A CLOUD SECURITY APPROACH THAT SPANS MULTIPLE PROVIDERS, AS WELL AS ON-PREMISES ENVIRONMENTS, PROVIDES MAXIMUM FLEXIBILITY.

42% Percent of organizations plan to use multiple cloud providers

30% Percent plan to use hybrid cloud/on-premise infrastructure

SECURITY ADVANTAGES FOR MIDSIZE ORGANIZATIONS

For midsized organizations with limited IT staff, migrating to Office 365 alone may deliver immediate security benefits. After all, Microsoft's ability to provide effective infrastructure level security (e.g., network security, encryption, Distributed Denial-of-Service (DDoS) prevention, OS and application patching, etc.) exceeds the in-house capabilities of most midsized organizations. Microsoft's large security team also has direct access to the teams that are responsible for Office 365 application development, giving them the ability to quickly resolve newly-discovered application vulnerabilities.

In addition, even though Microsoft clearly defines where its responsibility for Office 365 security ends, it does provide a wide range of security tools that customers can use to fulfil their own obligations under the shared responsibility model.

The stakes are extremely high for Microsoft when it comes to Office 365 security, and they have historically invested heavily in both in-house feature development and acquisitions of specialized cloud security companies. Office 365 customers benefit from these investments both directly and indirectly.

TOP SECURITY RISKS

An effective Office 365 security strategy must be broad in its scope, as there is a diverse set of possible risks. Even as Office customers' scope of security responsibility is limited to activities in the cloud, there are multiple attack vectors to consider.

ACCOUNT-LEVEL SECURITY

The principle of least privilege – the practice of giving user accounts only those privileges that are needed to perform their designated function – is a longstanding cornerstone of information security. This concept is particularly important when moving to Office 365, which is much more dynamic than traditional on-premise communication and document storage infrastructure.

It's also important to pair identity-centric privilege management with multi-factor authentication, given the Internet-centric nature of Office 365. This can be accomplished using Microsoft's native tools such as Azure Active Directory (Azure AD) or one of the many third-party identity-as-a-service (IaaS) solutions. Either approach should be combined with an effective monitoring strategy, as account misuse and abuse if often detectable early if the right measures are in place.

SPAM AND MALWARE

Microsoft offers baseline anti-spam and anti-malware protection to all commercial Office 365 users. They also offer a paid upgrade option, Office 365 Advanced Threat Protection, that adds more sophisticated attachment sandboxing, link checking and analytics.[1] As with IaaS, there is an extensive collection of third-party spam and malware solutions to choose from as well.

In most instances, spam and malware protection technologies respond to threats as they appear. However, no security measure is 100 percent effective. Therefore, this is another area where a combination of protection and monitoring is most effective. Ideally, this should include correlation of Office 365 event information with alerts from endpoint solutions to provide the most complete view of potential malware impact.

DATA LEAKAGE

One of the most notable benefits of Office 365 is that it makes it easy for users to collaborate and share data. Common data sharing options include standard email attachments, web-based document access and link-based sharing of files and directories. While useful from a productivity standpoint, each one of these sharing mechanisms is a possible path for data leakage.

Data loss prevention (DLP) is another established security practice that has been adapted for the cloud. Once again, organizations can choose between standard integrated capabilities of Office 365 and specialized third-party solutions.[2] Like spam and malware protection capabilities, DLP solutions generally take immediate action if the right policies have been defined upfront. However, it's important to actively monitor sharing activity and review audit reports on a regular basis to catch anything that slips through the cracks and make policy refinements as necessary.

NON-COMPLIANT USAGE

While most Office 365 security measures are focused on external attackers, monitoring for insider threats is also an important component of an effective Office 365 security strategy. Security teams should approach this area with care, as demonstrating trust and respect for employee privacy is important in most organizations. However, targeted monitoring for non-compliant Office 365 usage can be useful for both detecting malicious actions by insiders and unintentional non-compliant usage.

Anomaly detection is one of the most powerful tools that can be applied to this area. It is impossible to codify every type of usage behavior in a security policy. However, most usage patterns are fairly consistent day-to-day. Therefore, surfacing anomalies in areas such as access location, access device and volume of data shared or exported can cue security and compliance teams to perform targeted investigation and validation of how the platform is being used and prevent or reduce the impact of potential insider threats.

A GROWING TARGET FOR BUSINESS EMAIL COMPROMISE

Business email compromise (BEC) is a growing threat that has impacted thousands of Microsoft Office 365 customers. Cybercrime caused $3.5 billion in losses in the U.S. in 2019, with BEC attacks accounting for nearly half of that.[3] Unfortunately, it can be quite difficult for security teams and administrators to uncover what happened without the proper tools — either native-enabled tools or third-party solutions — to investigate.

The BEC incidents vary in how they are executed, but they share a common theme, as this story illustrates. In one example, a finance executive at toymaker Mattel received what appeared to be a legitimate email request from her recently appointed CEO to make $3 million in payments to a Chinese supplier. Mattel does a significant amount of business in China, so this request did not seem out of the ordinary. After verifying that approvals from herself and the CEO were enough from a compliance standpoint, the executive transferred the funds to a bank in China.

When she mentioned the payment to the CEO later, she was shocked to discover that he had never requested it. Mattel had been subjected to a BEC attack. An attacker used a phishing email that was spoofed, appearing to come from the new CEO. It was well-targeted to take advantage of the recent executive changes and the company's growth plans in China.

Mattel was lucky in one respect: the day after the transfer was made was a bank holiday in China. This gave the company time to work with law enforcement to freeze the recipient account and eventually recover the funds.[4] However, many more organizations have been caught off guard by this fast-growing criminal scheme.

Reviewing information in the Office 365 Management Activity API can help security teams determine what happened if an attacker manages to get control over a user's account. However, there are typically too many daily events for administrators to spot inconsistencies unless they use analytics to analyze, detect and highlight anomalies.

The Office 365 edition of Microsoft Cloud App Security (CAS) that is included with Office 365 E5 subscriptions can provide deeper insights into security profiles of Office 365 tenants. Administrators should ensure that they are taking advantage of these tools, as well as consider third-party solutions with additional capabilities to monitor for unauthorized email forwarding rules and enable advanced logging, for example, and to integrate with their organization's security information and event management (SIEM) tool.[5]

GAINING VISIBILITY: OFFICE 365 MANAGEMENT ACTIVITY API

Microsoft offers a wealth of information about Office 365 activity through standard web-based reports with high-level summaries. More detailed information is also available programmatically through the Office 365 Management Activity API.[6] Organizations can use this API to collect extensive information about user and administrator activities, platform operations and security activity through a representational state transfer (REST) web service.[7]

Applied effectively, this information can play a central role in an effective Office 365 security monitoring and response strategy. But the time and resources it takes to acquire, normalize and asses this information isn't practical for many organizations. As a result, high-severity events can get lost in the noise and go undetected.

WHAT ARE CASBs?

As software-as-a-service (SaaS) usage has expanded, a specialized category of security vendors known as cloud access security brokers, or CASBs, developed. The CASB solutions act as a security overlay across an organization's various SaaS platforms.

Gartner describes the four essential capabilities of a CASB as:

- Visibility
- Compliance
- Data security
- Threat protection

CASBs can play a useful role, particularly as organizations adopt SaaS platforms that do not have the same extensive native security capabilities as Office 365. However, they are often an expensive investment. It is also important to consider the human effort that must go into implementing and using a CASB effectively.

In-house skills, expertise and time are required to take advantage of the additional security controls and security alerts that CASBs offer. Midsized organizations are usually better served by a managed services model that combines SaaS security event detection and expert support to complement their in-house security efforts.

AUDITING AND COMPLIANCE

A major concern that many organizations have is the effect that adopting Office 365 will have on their compliance posture. These concerns are valid. After all, giving up direct control over both application delivery and data storage to a third-party makes it impossible for IT and security teams to directly attest to the fact that their infrastructure is being operated and protected in a compliant manner.

Where possible, Microsoft supports its customers' compliance efforts. For example, Microsoft will execute a Business Associate Agreement (BAA) to support healthcare organizations' efforts to comply with the Health Insurance Portability and Accountability Act (HIPAA) in the United States. Microsoft also provides built-in compliance tools to help map Office 365 controls to the requirements of specific regulations, including the European Union's General Data Protection Regulation (GDPR). However, ultimately the responsibility for compliance resides with the organization using Office 365.

It is important for regulated organizations to scrutinize the types of encryption used as part of their Office 365 deployment. Overall, Microsoft delivers stronger data protection than most mid-sized organizations can achieve on-premise. For example, SSL/TLS encryption is used for user sessions. Data at rest is also proactively encrypted on Microsoft systems at both the volume and service levels.

However, it is important to consider that while data is encrypted in Office 365, it is Microsoft — not an organization's in-house IT team — that controls the encryption keys. This is likely acceptable for most midsized organizations. However, organizations with more extensive compliance needs in this area may need to explore Microsoft's more complex Customer Key option for a higher degree of control.[8]

Log retention is another important factor for regulated organizations to consider. While Office 365 generates detailed event log data, the retention period varies based on the Office 365 license purchased. It is as short as 90 days at many licensing levels. Organizations that must retain event log information for more extended periods may wish to implement an external log collection and storage solution.

ALTHOUGH MICROSOFT DELIVERS STRONGER DATA PROTECTION THAN MOST MIDSIZED ORGANIZATIONS CAN ACHIEVE ON PREMISE, ULTIMATELY THE RESPONSIBILITY FOR COMPLIANCE RESIDES WITH THE ORGANIZATION USING OFFICE 365.

SECURITY DOESN'T ALWAYS COME FOR FREE

After learning about the wide range of available native Office 365 security capabilities, many organizations dismiss the idea of using third-party Office 365 security products and services. It is important to note that many native Office 365 security capabilities are only included at the highest Office 365 licensing levels or as paid upgrades, though. Therefore, it is wise for organizations to evaluate combining less expensive Office 365 licenses with third-party security solutions that can meet their needs more effectively and economically.

SECURITY FEATURE	NATIVE MICROSOFT OPTIONS	SAMPLE THIRD-PARTY OPTIONS
Identity-as-a-Service	• Free Basic Azure • AD capabilities • Advanced features require a paid upgrade	• Okta, Ping Identity, Oracle, IBM
Spam and Malware Protection	• Basic features included • Office 365 Advanced Threat Protection requires a premium license or paid Upgrade	• Mimecast, Proofpoint, Cisco
Data Loss Prevention	• Basic features included	• Symantec, Forcepoint, Digital Guardian
Cloud Access Security Broker	• Cloud App Security requires a premium license	• McAfee, Netskope, Symantec

EFFECTIVE SECURITY MONITORING AND RESPONSE

While there is a wide array of Office 365 security tools and information sources available, it is often difficult for in-house security teams to absorb yet another tool to learn and another wave of security alerts to monitor. ActiveEye from Motorola Solutions is a force multiplier for security teams facing this challenge.

ActiveEye collects and analyzes Office 365 activity data alongside information from a broad range of other security data sources, including:

- Other SaaS platforms
- Complementary cloud-based security services
- Infrastructure-as-a-Service (IaaS) platforms like Amazon Web Services and Microsoft Azure
- On-premise security tools such as security information and event management (SIEM) systems and endpoint security products
- Threat intelligence feeds

ActiveEye is more than another security technology. It offers advanced security threat analysis that is supported by both automated machine learning and 24/7 monitoring and analysis by a team of security experts.

Instead of flooding your security team with more noise, ActiveEye surfaces the security incidents that truly matter and provides the expert guidance your team needs to respond quickly and effectively.

CONCLUSION

Developing and implementing an Office 365 security strategy can seem daunting for many midsized organizations. The number of native and third-party security options is seemingly endless, and the last thing that most security teams need is another set of tools to learn or another high-volume feed of unprioritized security events.

The best way for organizations to approach Office 365 security is to break it down into its component parts and address them systematically. In some cases, simply learning and enabling native Office 365 security features is sufficient. In other cases, third-party products and services can be the most effective option.

In either case, it is critical to consider how an organization's in-house team will create new workflows for cloud security management even as on-premise security requirements remain. Adding incremental staff for cloud security is not an option for many companies. However, a blend of advanced technology and expert third-party guidance can help in-house security teams absorb a growing set of security demands by working more efficiently.

TRUSTED CYBERSECURITY SERVICES

Motorola Solutions Cybersecurity Services bring together an integrated portfolio aligned to the National Institute of Standards and Technology (NIST). As a trusted business partner, we help you develop roadmaps to safeguard your information, employees and systems.

With more than 90 years of experience managing mission-critical technologies and more than 20 years of developing cybersecurity solutions, Motorola Solutions is well-positioned to be the 'one service provider' for your cybersecurity needs.

With best-in-class people, process and technology we bring scalable operations that can help organizations manage cyber risk awareness, detection, response and recovery. Our cutting edge security automation and orchestration platform delivers 24/7 insights on security management, system performance and service delivery, enabling a 100 percent co-managed approach to security management.

We provide a purpose-built and integrated approach to end-to-end resilience.

SOURCES:

[1] Office 365 Advanced Threat Protection, Microsoft.
https://docs.microsoft.com/en-us/office365/securitycompliance/office-365-atp

[2] Overview of data loss prevention policies, Microsoft.
https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies

[3] FBI 2019 Internet Crime Report.
https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-internet-crime-complaint-center-2019-internet-crime-report

[4] Chinese Scammers Take Mattel to the Bank, Phishing Them for $3 Million, CSO Online.
https://www.csoonline.com/article/3049392/chinese-scammers-take-mattel-to-the-bank-phishing-them-for-3-million.html

[5] Resisting Business Email Compromise Attacks on Office 365 Users, Petri IT Knowledge Base.
https://www.petri.com/resisting-business-email-compromise-attack-office-365

[6] Office 365 Management Activity API Reference, Microsoft.
https://docs.microsoft.com/en-us/office/office-365-management-api/office-365-management-activity-api-reference

[7] What is REST?, Code Academy.
https://www.codecademy.com/articles/what-is-rest

[8] Office 365 Service Encryption, Microsoft.
https://docs.microsoft.com/en-us/office365/securitycompliance/office-365-service-encryption

Learn more at: motorolasolutions.com/cybersecurity

MOTOROLA SOLUTIONS

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, Il 60661 U.S.A. **motorolasolutions.com**