Office 365 Buyers Guide: Best Practices for Securing Office 365

Executive summary

Microsoft Office 365 has become the standard productivity platform for the majority of organizations, large and small, around the world. It's an easy-to-use, cost-effective solution with flexible collaboration features, making it a compelling choice for many organizations. But as its adoption has increased, Office 365 has also become an attractive attack surface for cybercriminals targeting hosted email, user credentials, and valuable personal/organizational data.

More than 90 percent of breaches start with email. According to the Cisco 2017 Midyear Cybersecurity Report, attackers turn to email as the primary vector for spreading ransomware and other malware. This is why no company can afford to skimp on Office 365 security. Exchange Online email is vulnerable to malware from attachments and malicious URLs that can lead to ransomware, business email compromise, phishing, and other attacks.

Best practices for securing Office 365: threat protection and data protection

It's best to view the task of securing Office 365 from both a cloud collaboration tool perspective and an email perspective. It requires two types of defense: threat protection and data protection.

Contents

Security, DevOps, and business leaders need to secure use of Office 365 to improve collaboration and productivity, reduce costs, and protect networks. Organizations using Microsoft services need to:

- Detect anomalous user behavior, including compromised accounts and malicious insiders
- Enforce and demonstrate compliance
- Detect threats in incoming email
- Help ensure the organization is following security best practices
- Identify data exposures resulting from over-sharing

Although Office 365 is a cloud-based service, organizations are fully responsible for their employees' use of the platform. It is important to note that Microsoft's security offerings, those included in Office 365 and those sold through a separate license, are still lacking in many critical security features.

Office 365 administrators often have limited visibility into the activities of their users, such as the files they're accessing, the policies for those files, and whether or not those user accounts have been compromised.

Threat protection: Detect and manage threats

The top five things buyers should consider when securing their Office 365 instances from network threats are:

1. Compromised accounts – "How do I detect account compromises?"
2. Malicious insiders – "Are malicious insiders extracting information?"
3. Privileged account actions – "Are users with sensitive information at risk?"
4. Lack of visibility into threats – "Do I have comprehensive threat intelligence?"
5. Lack of visibility into existing malware – "Do I have retrospective security if a file becomes malicious after the initial point of inspection?"

Contents

1. Compromised accounts

Attackers are compromising cloud application accounts at astonishing rates. Microsoft reported a 300 percent increase in Microsoft cloud-based user accounts attacked year-over-year. Targeted attacks, such as spear phishing, have reached a new level of sophistication; they are virtually indistinguishable from legitimate communications. Many recent cases have no files or malicious URLs involved in an attack. These render traditional security solutions, including anti-malware and anti-phishing tools, incapable of addressing these threats. The traditional security boundary has disappeared, but many end users still feel comfortable using the older authentication methods. At the same time, many cloud offerings make networks vulnerable to entirely new attack schemes, such as the use of employee Office 365 credentials to log into obfuscated, malicious cloud applications.

User and Entity Behavior Analytics (UEBA) can discover and analyze all user activities and identify anomalous user behavior. An example of suspicious behavior would be logging in from different geographical locations in a short amount of time. You need the ability to blacklist and whitelist specific IP addresses to help protect against malicious application logins. Additionally, it's important to have visibility into all connected applications, particularly where Office 365 users can log in to unsanctioned applications with their existing credentials. Your solution needs to give you control over your connected application ecosystem.

2. Malicious insiders

As malicious insiders are unlikely to trigger typical security alerts when performing nefarious tasks, detecting insider threats can be extremely difficult. Given the ease with which malicious individuals can use cloud applications to access, modify, distribute, and exfiltrate sensitive information, it's critical to detect malicious insiders and mitigate the risk they pose.

Since malicious insiders are hard to detect, you need a solution that can understand and establish a baseline for users' typical behavior, compare user actions to that baseline, and alert security administrators when it finds suspicious deviations. The solution should also look for users downloading high volumes of files or accessing Office 365 accounts outside of normal business hours.

Contents

3. Privileged account actions

Privileged users not only have access to a high volume of sensitive data, but also have administrative rights, such as configuration settings and user provisioning within applications. A compromised Office 365 administrator account can lead to extensive damages, with an attacker able to steal, modify, and delete data, remove user accounts, and prevent the entire organization from using the service.

It's important to deploy a solution that can monitor these privileged identities in Office 365 to the same or even a higher standard than regular accounts are monitored. It should offer the capability of separating roles and responsibilities to mitigate the risk of compromise. Implementing a "least privilege" access model promotes the fewest user profile privileges needed on Office 365 accounts, based on users' job responsibilities.

4. Comprehensive threat intelligence

As cyber attacks against Office 365, and particularly Exchange Online email, have become more sophisticated, so must the security layers deployed against them. As with any email security offering, the Office 365 email security solution must protect against spam, viruses, malware, spoof attacks, and other advanced threats. In addition, effective security solutions need to go beyond the basic perimeter tools that inspect email at a single point in time. With this outsourcing of email to Office 365, customers need a solution that provides deeper visibility and control to reduce the Time To Detection (TTD) of an attack, scope the event, and contain malware before it causes damage.

An effective solution to secure Office 365 email should also contain geolocation-based filtering safeguards against sophisticated spear phishing, quickly controlling email content based on the location of the sender. It also needs comprehensive threat intelligence that tracks new and emerging threats. This intelligence needs global threat data from a wide range of sources, and is shared with multiple security products, to quickly correlate, identify, and detect threats in your Office 365 email.

Contents

5. Retrospective security and real-time URL inspection

Today's attacks are becoming more sophisticated and that includes those that target Office 365 users. A file attachment that may look benign when it comes in can transform into malware hours, days, or weeks after entering an environment. Retrospective security alerts administrators when a file turns malicious, making it a critical factor in determining security options for Office 365. In addition, Mailbox Auto-Remediation can automatically remove these malicious attachments, saving teams hours of work and helping them contain threats before they cause more damage.

In conjunction with attachment-based continuous security, real time URL scanning at the point of "click-time" is required. It can tag URLs that look suspicious for scanning every time an end user clicks. As with attachments, attackers know they can evade the scanning of URLs at a point in time by staging their attacks after that period of time.

Your solution should continuously scan attachments and URLs past the initial point in time inspection that is traditionally offered in most email security products. Continuous security is mandatory.

Data protection: Detect and manage data loss

Although threat protection is a critical component in securing Office 365, data loss is just as important. Critical information is stored within Office 365. This is not only sensitive information, like medical records, payroll records, or credit card information, but also emails and email attachments with sensitive data. In the past, this data was controlled and segmented off within the corporate security layers. Now, the data will be exposed to the security layers defined within Office 365. You can counter this loss of visibility by increasing controls and visibility within Office 365.

The top five things buyers should consider when securing their Office 365 instances from data loss are:

1. Unclear user policies – "Are my users clear on best practices?"
2. Lack of visibility into sensitive data – "Do I know what my users are uploading?"
3. Risk of data exfiltration – "Do I know what my users are sharing?"
4. Data loss from outgoing emails – "Do I know what my users are sending through email?"
5. Encryption of email – "Are my users encrypting sensitive data sent via email appropriately?"

Contents

1. Clear user policies

Train Office 365 users to understand that the convenience of cloud-based applications comes with an increased security risk. This training must be mandatory. It's critical to give them clear policies on how to handle content created within Office 365, along with email and email attachments.

2. Visibility into sensitive data

Users often upload sensitive information to Office 365, from credit card numbers to health information to product roadmaps. Traditional on-premises Data Loss Prevention (DLP) systems are limited to on-network traffic. They can't detect sensitive information that users upload to or create in cloud services.

Office 365 needs a cloud DLP engine to identify sensitive information stored in cloud environments in violation of policy. The focus should be on common types of sensitive information, such as credit card numbers and Protected Health Information (PHI), as well as creating custom policies to identify proprietary data, such as intellectual property.

Cloud DLP should continuously monitor Office 365 to detect and secure sensitive information through comprehensive out-of-the-box policies, as well as highly tunable custom policies. At the same time as an organization rolls out DLP capabilities for Office 365, it needs to make certain that DLP policies will be followed in the future, and that retroactive scans will be performed to help ensure full policy compliance.

3. Risk of data exfiltration

Office 365 makes it very easy to share and collaborate, but this also introduces additional risk of data exfiltration. A user, within a few clicks, can make data available from anywhere on the Internet. Cybercriminals and malicious or careless insiders can easily exploit Office 365 to exfiltrate or expose sensitive information.

You need a solution that can identify all sensitive data stored in Office 365. It should highlight information that, based on policies your organization created, is inappropriately shared or exposed. Automated response actions should be capable of remediating risk in the event of a policy violation, including notifying administrators and end-users, removing collaborators, or even revoking the file share and more. These controls are critical to reduce the exposure of sensitive content and risk of data exfiltration.

Contents

4. Data loss via outgoing emails

Email security solutions must detect, block, and manage risks in outbound email. This includes guarding against malicious content sent to customers and business partners and preventing sensitive data from leaving the cloud environment, either intentionally or inadvertently. In addition to losing critical intellectual property, compromised email accounts containing malware can propagate a virus by launching sudden outbound spam bursts. This can lead to a blacklisting of the organization's email domain, even when the emails are signed. Office 365 email is no exception.

You need a solution for Office 365 email that provides security layers for outbound email. This should include behavioral monitoring to detect compromised accounts, rate limiting for outbound traffic, and antispam and antivirus scanning, which can keep compromised machines or accounts from ending up on email blacklists.

It should provide content, context, and destination knowledge to prevent accidental or malicious loss of data, enforce compliance, and protect your brand and reputation. You control who can send what information, along with where and how they can send it. Pre-defined policies should be in place that help prevent data loss and support security and privacy standards for government and private sector regulations.

5. Encrypting sensitive content in outgoing email

Office 365 users should be able to rely on secure communications to conduct their business activities without fear of compromise, especially when sending sensitive content. Encryption is one of the critical security layers for protecting data. It can safeguard sensitive information, such as financial and personal information, competitor intelligence, and intellectual property to protect and achieve compliance.

Office 365 users should look for the most advanced encryption key service available to manage email recipient registration, authentication, and per-message/per-recipient encryption keys. The solution should also give compliance and security officers the control of and visibility into how sensitive data is delivered, including customizable reporting dashboards showing encrypted email traffic.

Summary

Adoption of collaborative cloud tools such as Office 365 has become mainstream. Customers are benefiting from the extensive, ubiquitous access to the data they need to conduct business, as well as the simplicity of using and accessing these offerings. At the same time, customers need to examine, in-depth, the security offerings required to balance that convenience with protection. Cisco embraces these new, cloud technologies and provides the comprehensive security that's essential to achieve their potential benefits. For more information on best practices to secure your Office 365, contact your Cisco Account Manager, or visit www.cisco.com/go/cloudsecurity to learn more.