SIRIUS
A CDW COMPANY

WHITEPAPER

Solving the challenge of cloud security with Microsoft 365

Contents

Executive summary

Security is a top priority for organizations of all sizes in every industry. It has to be. Companies rely on their data to do just about everything. Data can provide the direction for strategic decisions that might make or break the bottom line. The right information can help improve relationships with customers and business partners. Companies often hold sensitive information about clients or customers, about strategies, financial information and other private data. Some organizations hold state secrets. And with the emergence of cloud computing the volume of important data is skyrocketing.

The global cloud computing market itself is booming. In fact, the market size is expected to grow from SD 371.4 billion in 2020 to USD 832.1 billion by 2025, at a Compound Annual Growth Rate (CAGR) of 17.5% during the forecast period. The emergence of cloud computing has made covering all security bases more complicated for businesses and most need to revisit their strategy to ensure they keep their vital data safe.

Whether you are considering implementing cloud computing, or have already, it's essential that your cloud investment is as secure as possible. This whitepaper will act as guidance and advice on how to make the best decisions when it comes to your organization's IT security.

We will explain and discuss:

- The multiple threats organizations face
- How IT systems administrators can use Microsoft 365 security technology to help secure their cloud environment
- The role an experienced Microsoft partner can play in an organization's cloud security strategy

Key takeaways

1. In a cloud-first, hybrid working world, IT security needs a new strategy
2. How Microsoft 365 security solutions can be best utilized
3. Why it's important to have a Managed Security partner to support your Microsoft Security program

Staying secure in a cloud-first world

Staying secure in a cloud-first world

Cloud computing has transformed how we work, shop, communicate and everything else in between. It has facilitated remote and hybrid working and it's led to more of a reliance on mobile solutions, on employees working in disparate locations, and perhaps a more detached base of operations.

It has also changed the landscape for many businesses when it comes to securing their data. Today, organizations need to put in place a structure that keeps information secure without limiting the power and flexibility of their cloud-based solutions.

The Catch-22 of the cloud

In a cloud-based, hybrid working world, information can be stored and accessed from anywhere, making it easier for employees to work flexibly and more productively. But, at the same time, this makes protecting data more difficult. Many businesses are struggling with the complexity of regulating information stored on remote devices, and the balance of ensuring employees can work as flexibility as possible.

When organizations struggle to organize their data and information flows, they can leave themselves more open to cybersecurity threats. And cyberthreats are on the up. As organizations have shifted to a new way of working, thanks to the pandemic, cybercriminals have seen new angle for attack.

It pays to be aware of what type of threats are out there. In the next section we'll look at some of the specific threats that companies typically face.

Cloud security threats and issues

Cloud security threats and issues

According to IDG, the media and research company, 92% of organizations' IT is in the cloud. And in a recent study from IDC, the market research company, 79% of companies have experienced a least one cloud data breach in the last 18 months. Together, it's clear that security threats in the cloud for organizations is high. But what do these threats look like?

In an effort to help you avoid becoming another security statistic, we'll look at some of the current threats organizations face. These include:

- Insider threats
- Insecure APIs and interfaces
- Cloud misconfiguration
- Denial of service attacks
- Lack of visibility

Let's look into these threats in more detail.

Insider threats

An insider threat is a malicious threat to an organization coming from employees, former staff, contractors, or business associates. They usually have information around an organization's security practices or even direct access to company data.

According to an Insider Threat report from Nucleus Cyber in 2019, 70% of organizations were seeing more frequent insider attacks. What's more, in the same report, over half of respondents said that, since migrating the cloud, detecting attacks has become significantly more difficult.
It's important to note that there are several different types of insider threats and the motivations behind these threats differ depending on circumstances.

Malicious insider

An employee (or contractor) who is knowingly stealing information for financial gain or to disrupt operations. They may be a disgruntled current employee or a former member of staff who still has access to sensitive data.

Negligent insider

This threat is usually down to human error. An admin who has failed to change a default password, left a computer still logged into their account, or an employee who leaves a laptop in the back of a taxi.

Compromised insider

A computer that has been infected with malware, usually from a phishing scam, which can be used by cyber criminals to scan files, infect other systems or raise their level of privileges and permissions.

Insecure APIs and interfaces

Application programming interfaces (APIs) are the great drivers of digital transformation. But they also come with a threat if organizations fail to secure them correctly. Insecure APIs have long been seen as a potential source of threat – back in 2017 Gartner predicted that by 2022 APIs will be the vector most used in enterprise data attacks and, three years later, Forrester agreed, identifying some major security concerns around API use and warning of an increase in API breaches.

Why are APIs sometimes insecure?

In some cases, developers create APIs without authentication, leaving them open to the internet. This means that anyone can use them to access organization systems and data. The use of open-source software that is potentially tainted with corrupted code is another reason APIs can be left insecure, leaving apps open to attacks.

Cloud misconfiguration

Cloud misconfiguration is another major issue. This is because cloud environments can be extremely complex places and mistakes can be difficult to detect and fix. In fact, according to Gartner, a majority of cloud security breaches have been down to misconfiguration mistakes which were preventable.

These mistakes and delays in rectifying are often down to:

- A skills gap – a lack of cloud architects and engineers
- Prioritizing legacy apps over cloud security
- High volume of API and interfaces to govern
- Lack of controls and oversight

Denial of service attacks

Digital denial of service attacks increased by over 150% in the first half of 2020. Experts predict that there could be up to 15.4 million recorded attacks in the next two years. And costs for small businesses could reach $120K and as high as $2m for larger organizations.

There are several types of DDoS but the most prevalent over the last couple of years has been SYN flooding – where an attacker sends a massive number of SYN requests to a server to overwhelm it with open connections, and thus blocking legitimate traffic.

Lack of visibility

When an organization doesn't own the infrastructure that its environment is built on, the traditional tools for achieving network visibility are not as effective. And if the business lacks cloud-focused security tools it may be limited in its ability to monitor its environment and protect it from threats.

These threats are out there and affect organizations of all sizes every day. So, it's vital that every business has the means to protect itself. In the next section we'll look at the positive impact that Microsoft 365 can have on an organization's cloud security strategy.

All round protection with Microsoft 365

All round protection with Microsoft 365

In the old days, an organization operating with on-premises servers had full control over the security of their IT environment. They were responsible for setting appropriate user access policies, installing firewalls and antivirus software, installing security patches and guarding against cyberattacks. It meant they didn't need to trust another company with their data, or to worry whether their servers were fully protected.

But it also meant they were fully responsible for their own security and the need for IT support (depending on their size could be a very large IT team) to maintain servers' operability and security.

As cloud computing has evolved, the security technology to protect data has evolved alongside it. Big cloud services providers, like Microsoft, understand that security in the cloud has been a divisive point in the past and have taken steps to reassure customers of the cloud's safety. Microsoft 365, for example, has prioritized security across its platform and is one of the best choices for a business that stores its data in the cloud and must navigate a new hybrid way of operating.

Let's look at the positive impact that Microsoft 365 can have on an organization's cloud security strategy. We will look at:

- Identity access management
- Cloud mobility
- Data protection and encryption
- Threat detection and protection
- Zero Trust policy

Identity access management

Thanks to the cloud, users can access information and software from any device and any location. But this can also make it more difficult to ensure that the right users can access the right information they need to do their jobs. This is a balancing act between ensuring good permissions practice and not stifling employees' flexibility.

It's important to balance strong user authentication with the requirements of a great user interface (UI). When people sign into their company systems, for example, they expect all their apps and software to be waiting for them. But there's a lot of disconnected technology in a modern digital workspace, and not all of it may be directly connected to a user's Microsoft 365 account. For admins, an important challenge is managing user access and easily configuring single sign-on – avoiding the need for employees to repeatedly sign-in, while maintaining security. They also need the ability to quickly tailor access permissions to users, preferably at scale.

The Azure Active Directory (AAD) is designed to give users the tools they need to better manage these difficulties in the cloud. It includes information about users, groups, devices and contacts in a cloud environment. AAD includes four main services that can help solve the challenges of cloud-based identity and access management.

Active Directory Domain Services

Active Directory Domain Services, or ADDS, is designed to enable effective and compliant user authentication. It creates a single managed directory that can unite software across an IT environment, including Microsoft 365 apps, SaaS applications, and more traditional directory-based apps. Crucially, it ensures that authentication is fully compliant with LDAP and Kerberos guidelines.

Active Directory Federation Services

The Azure Active Directory Federation Services (ADFS) is a web-based single sign-on service for Azure. It enables users to access all the resources they need, including from third party applications, and on-premises, using a single set of credentials. This is a good way of creating a secure authentication policy in the cloud without sacrificing accessibility.

Active Directory Certificate Services

The Azure Active Directory Certificate Services (ADCS) allow administrators to provide digital certificates to devices and smartcards that can automatically identify users without the use of a password. It removes the need to enter manual credentials into mail and Office applications on remote devices. In practice, this means users don't need to log into specific software (such as Microsoft 365 apps) on their machines because the certificate allows the software to associate that device with a set of pre-determined login credentials.

Active Directory Rights Management Services

This service uses encryption, identity, and authorization policies to help secure files and emails in an IT environment. It allows you to bake security protections into a file or document itself, rather than the folder, site, or list that it's saved in. This means that sensitive information can be protected wherever it moves around your IT environment.

With these four AAD services, IT administrators are armed with the tools they need to effectively manage the challenges of identity and access management in the cloud.

Cloud mobility

In today's hybrid-working world, users work remotely on mobile devices. The challenge for IT departments is to find ways of seamlessly enabling this without compromising security.

When remote working first became a possibility, IT administrators were often hesitant to implement policies, because of the risk that remote devices could find their way around existing security controls. As well as this, when files are stored on remote devices, they can't be encrypted or secured in the same way as you would in an on-premises IT environment. Effectively, all access permissions are void and the file becomes a free for all. There's also the danger those devices aren't properly updated with cybersecurity and malware protections – leaving your environment at risk from malicious attacks via devices you have no control over. So how do you solve this problem?

Mobile Device Management

Mobile Device Management (MDM) allows organizations to govern remote devices that access and interact with their IT environment. IT administrators can create and manage device security policies and view detailed device reports.

There are a range of ways that MDM allows admins to govern how mobile devices interact with the wider IT environment:

- Require that all users enroll their devices before being able to access information – This ensures that you have a clear and comprehensive understanding of the devices that are accessing your information, including some important details, and the accounts those devices are associated with.
- Automatically identify whether a device is compliant with a range of pre-defined factors, including security and malware protections, and grant access only if these are met.
- Enable multi-factor authentication for access via remote devices. This means users must provide an extra level of accreditation to prove their credentials, which significantly reduces the danger of information becoming exposed to hacks and malicious threats.
- Wipe information stored on remote devices. This is particularly helpful if the devices are lost, stolen or hacked.

Taking advantage of Mobile Device Management and Multi-Factor Authentication allows IT administrators to gain full governance over the various remote devices that access their environment.

Data protection and encryption

The passage of the General Data Protection Regulation (GDPR) has meant that data protection is more of a concern than it ever has been. This is because law mandates that if an organization processes personal information of any kind (which most do) then that information must be protected. As well as this, contractual obligations often require a certain level of data protection.

Historically, there have been three predominant ways that organizations have sought to govern data protection via encryption:

- Encryption at rest
- Encryption in transit
- Encryption in use

The problem with these models of encryption is that they're all fundamentally tied to the hardware that the document or file is stored on. This applies whether that's a physical datacenter, server or a portable drive like a disc or USB stick. The problem today is that the relationship between files and hardware has been virtually eliminated with the introduction of cloud technology.

The distinction between a file being at rest, in transit, and in use is less clearly defined than before. If you access a file stored in OneDrive via a remote device – is that file then in transit or in use? It's been accessed remotely but it's still saved in the same place. What if you then email it to someone else? The hardware and location-based relationship between data and encryption is now largely redundant.

Retention and sensitivity labels

This lack of solid encryption technology was a problem for some time. How could you introduce a fundamentally cloud-based encryption technology, that existed in files rather than hardware, that was both easy to use and worked without causing unnecessary friction for users? Not an easy feat by any measurement. After a few years of wrangling, Microsoft came up with the basis for a solution: retention and sensitivity labels.

These functions allow users to 'tag' documents and files with labels that dictate who should be allowed to access them, and how long the file should be kept for. The system is easy to use – and Microsoft 365 does most of the hard work of enforcing these policies for you. It's simple for users to add relevant labels if, for example, they receive personal data that must be kept for several years then deleted or perhaps only seen by certain people.

The vital factor is that this encryption is stored in the file, not in the folder or hardware that it's stored on. That means that the protections are maintained wherever the file moves and from wherever it's accessed, solving the most crucial difficulty of cloud encryption.

Using these labels also allows you to demonstrate a certain level of both contractual and legal data protection compliance.

Threat detection and data protection

Detecting cybersecurity threats has always been a chief concern for IT administrators – whether they're in the cloud or on-premises. The relationship between hackers and those trying to stop them has often been described as a game of cat and mouse. In fact, the relationship resembles something closer to whack-a-mole. As soon as a new threat rears its head, technology must develop an intelligent response before the problem gets out of hand. This is why it's vital to be up to date on the latest developments.

Microsoft Advanced Threat Prevention

Microsoft Advanced Threat Prevention uses intelligent technology, powered by AI and machine learning, to automatically detect and prevent malicious threats from entering your IT environment. It provides comprehensive protections across a range of platforms. Most importantly, the cloud-based nature of the technology means that it's constantly updated. This is vital in providing the most comprehensive and modern protection.

Here's a look at the technology at play in Microsoft 365 Advanced Threat Prevention.

Safe attachments and links

This uses intelligent security to monitor the documents links that arrive via email for malicious threats and security risks.

ATP for SharePoint, OneDrive & Teams

If documents arrive in your IT environment via OneDrive, SharePoint or Teams, this function ensures that the documents are safe, and blocks files that don't pass through the filter.

Spoof intelligence

Spoof attacks occur when harmful parties' emails pose as a legitimate person, a colleague or boss, asking the recipient to hand over sensitive information, such as a password or bank details. Here, ATP uses AI and machine learning to automatically detect these scams and protect them from ever reaching the recipient's inbox.

Anti-phishing

Phishing scams generally involve fraudulent attempts to obtain sensitive information like usernames, passwords, and credit cards. Using intelligent AI technology, AP can check all your incoming messages for any indication that phishing has occurred.

With these protections, organizations are armed with cutting-edge technology that can protect their IT environment without causing unnecessary user friction.

Zero trust

Zero trust is a security model designed for a cloud-first world. The key principle for Zero Trust is the idea of "least privileged" access which assumes that no application or user should be trusted and instead based on strict user authentication.

Microsoft has adopted a Zero Trust strategy to secure corporate and customer data. The implementation centers on strong user identity, device health verification, validation of app health, and least-privilege access to resources and services.

Most organizations should explore how to implement zero trust into their environments as part of a long-term cloud security strategy. But it's important to remember that zero trust is an approach and not something that you can just switch on.

Here are three steps to help begin to implement a zero trust culture:

Step 1: Self-assess

It's important to understand where your data lives and the usual flow of information around your company – if you don't know where your data is you can't protect it. Understanding how information flows in your organization can help you enforce how the data is managed.

Step 2: Start slow

You should try a zero-trust policy on a low-risk area of the business where if you make mistakes, it's not going to upset the everyday operations of the organization. Here you can implement granular controls to see what works and what doesn't. And once you get a feel for the process you can scale to the rest of the company.

Step 3: Scale

As you experiment with implementing your policy you can begin to trial centrally managed zero-trust systems to help enforce changes across specific areas of the business.

Team up with an experienced partner for better protection

Team up with an experienced partner for better protection

Depending on the size of an organization or the available resources it has, teaming with a technology partner who knows cloud security (and Microsoft 365) is the most efficient way of ensuring that critical data is protected.

The right partner is an excellent resource for an organization looking to build a robust cloud security set-up to meet the challenges posed by complex cybersecurity threats. These technology providers have teams of security experts that can help organizations plan, configure, and deploy the right strategy specific to the needs of the business or its industry.

Balancing productivity with security is key to modern collaboration. The best technology partners will work closely with your teams to understand how they operate and make security suggestions and process improvements based on their observations, experience, and expertise.

MessageOps are Microsoft security experts who design and build security strategies for their customers. They offer multiple services, including implementing Microsoft 365, to make sure customer data is continuously kept safe, and security protocols are regularly updated. They include:

- Identity and authentication services
- Threat protection services
- Information protection services
- Endpoint device management services
- Azure security assessments and services

Efficient and cost effective

Updating security strategies is not easy work. Nor is it cheap. So, it's important that when an organization is putting together a plan to become more secure in the cloud that they do it right the first time. This is where an expert tech partner can really help make a security investment go much further. Because they have experience putting these strategies in place, they can make sure that their customer is taking the right steps, saving time, money, and a whole lot of frustration.

Don’t just be another statistic.

More than ever, it’s essential for organizations of all sizes to actively think about their cloud security setup—whether they are planning a migration or are already in the cloud.

A reminder for organizations:

- Assess your current security setup
- Add the right security solutions
- Plan the right upgrades

Get in touch with MessageOps to make sure your environment is as secure as it can be.

877–788–1617
info@messageops.com
www.messageops.com

SIRIUS
A CDW COMPANY