Microsoft

# 6 Steps

## to Build a Holistic Security Strategy with Microsoft 365

## Introduction

# Meeting the challenge

Securing data and systems is a top priority for organizations. But meeting this challenge gets more difficult every day as attacks grow more sophisticated, employees use a wider array of devices and applications, and data flows into and out of your business in more ways.

Leaders have to balance these challenges with the need to collaborate, innovate, and grow a business. You need a multi-faceted security approach that constantly protects all endpoints, detects early signs of a breach, and responds before damage occurs. And no matter how strong your defenses are, preventive measures are no longer sufficient—you also need to adopt an “assume breach” posture that includes detection and response measures.

Risk management is now an obligation for many Chief Information Security Officers (CISOs). It includes minimizing the potential impact of increasingly sophisticated attacks by more effectively protecting a growing footprint of users, devices, applications, data, and infrastructure with fewer people.

Today's CISOs need agile security frameworks that enable digital transformation, supported by holistic strategies embedded into technologies, processes, and training programs. This e-book shares the strategies and best practices of CISOs who have made security the cornerstone of business success.

> **Every hour of the day you need to be prepared. And so that means you have to exercise this operational security posture on a continuous basis.**
>
> **Satya Nadella,**
> *CEO,*
> *Microsoft*

Microsoft 365 Enterprise is the world's productivity cloud, including Office 365, Windows 10 Enterprise, and Enterprise Mobility + Security, that empowers everyone to be creative and work together, securely.

### Solve

Microsoft 365 has built in security solutions for third-party antispam, encryption, mobile device management, and more.

### Shield

This level of security is woven across all layers of Microsoft 365 — physical, network, infrastructure, and applications.

### Detect

The Microsoft Intelligent Security Graph is the cornerstone of Microsoft's $1 billion yearly investment in security research and development. It assesses more than 6.5 trillion threat signals per day to proactively defend organizations and their end users.

### Protect

Safeguard your people, data, and devices without disrupting productivity.

# Table of contents

01

## Step 01

# Planning for rapid response

Threat actors have evolved from “smash-and-grab” attacks to those that compromise systems in hopes of maintaining a persistent, long-term presence. Attackers now use a variety of vectors and an increasingly advanced array of tools and techniques: stealing credentials, installing malware that erases itself to avoid detection, modifying internal processes and rerouting network data, social engineering scams, and even targeting employee mobile phones and home devices.

Of course, organizations are deploying more and more security tools against this rapidly evolving landscape. While meant to address specific issues, these solutions rarely work together. Many use proprietary dashboards, consoles, and logs. Difficulty of integration makes it hard to have an overarching view and prioritize threats quickly, and is an even greater challenge when dealing with both cloud and on-premises resources. As a result, attacks can go undetected for around 140 days.[1]

> **The average large organization has 7w5 security products.[2]**

## Best practices

The traditional approach is to correlate information from a variety of tools using Security Information and Event Management (SIEM) solutions. But detection still requires security teams to do out-of-band processing of logs and data, then prioritize and investigate incidents. Data gathering and reconciliation are difficult, and the lack of a unified view complicates response and management. As rapid detection and response become more important, these best practices have emerged:

- ✓ Gain a holistic view of your entire network, including cloud and hybrid environments.
- ✓ Streamline and simplify the ecosystem of security products for better visibility, management, and protection.
- ✓ Partner with technology vendors that collaborate and share information across the security industry.
- ✓ Combine data insights with human intelligence from security analysts, researchers, and threat hunters to further enhance the ability to quickly assess and prioritize events.

## Microsoft's security management capabilities

To gain visibility and control over your security, Microsoft 365 provides a holistic approach to security from protecting at the front door to protecting your data anywhere to detecting and remediating attacks. This helps you consolidate tools while ensuring that your security specialist teams have the flexibility and freedom to address their specific workloads.

## Key takeaways

- ✓ The lack of integration between security products makes it hard for security teams to quickly see and combat threats holistically.
- ✓ Seek out products designed to integrate with others.

02

Step 02

# Protecting identity

Enterprises know that a data breach can have enormous costs, and they still face the very real challenge of establishing sufficient security controls to gain the visibility they need into threats and attacks. They also have to support consumerized IT, where employees no longer work exclusively on tightly controlled, corporate-issued devices, and expect to work anywhere, on any device or any platform, regardless of whether it has been sanctioned by corporate IT.

In this world, identity-driven security strategies tie access to identity so the organization can transcend devices and apply controls based on role and need—no matter how the user connects. This focus on authenticating and managing users as they access corporate assets also lets organizations protect their data regardless of where it's stored, how it's accessed, or with whom it's shared.

Two other technologies bear mention: identity and access management (IAM) solutions and mobile application management with data loss prevention (DLP) solutions. Both help reduce risk by protecting access to applications and data in corporate resources and in the cloud. IAM can eliminate the need for multiple credentials by giving employees a single identity to access cloud and on-premises resources. Cloud-based IAM systems can also leverage threat intelligence and analysis from the technology provider to better detect abnormal logon behavior and automatically respond appropriately.

Multi-factor authentication (MFA) offers another layer of protection, requiring that a user present something they know (their password) and something they have (secondary authentication through a device, fingerprint, or facial recognition). Other robust tactics include basing access on user risk, device risk, application risk, and even location risk. These capabilities can automatically allow, block, or require MFA of a user in real time based on the policies you set, essentially letting organizations increase protection at their own front door.

**Organizations can protect their data regardless of where it’s stored, how it’s accessed, or with whom it’s shared**

These modern tools also provide pre-breach endpoint security. The best solutions help encrypt devices at all levels from hardware to application, and provide enterprise-wide visibility into attack dynamics. More advanced tools provide a post-breach layer of protection including insight into adversary techniques and similarity to known attacks with built-in tools to quickly block, quarantine, or wipe company data.

Microsoft 365 works with existing infrastructure — unifying IT management across users, devices, apps, data, and services — so your IT team can consolidate and simplify solutions and save money. It also supports hybrid environments, giving you the flexibility to integrate cloud and on-premises solutions.

## Simplified and intelligent security management helps you gain visibility and control over security

The key for a CISO's success is not a single console for everything, but integration where it makes the most sense. You don't need all the point solutions to manage, data points to sift through to help secure your end user devices and expanding networks. Microsoft 365 provides intelligent security management with specialized controls based on your security teams' needs, visibility where you need it, and guidance on how to harden your organization's security posture based on unmatched intelligence. This lets you benefit from the flexibility and freedom to easily manage security with built-in controls, plus take advantage of security intelligence and guidance to enhance your security posture and defend against threats.

Understand your security posture: Get insight into your security state and the risks across resources in your organization to deliver effective detection and response.

Define the data protection you need: Create and customize consistent security policies and enable controls, crucial to intelligent security management.

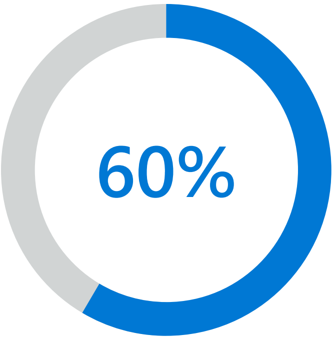
Keep current with security intelligence: Use built-in intelligence, recommendations, and guidance to elevate your organization's security.

## Increasing security through identity and access controls

Microsoft's identity and access management solutions help you protect user identities and control access to valuable resources based on user risk level. Microsoft 365 Enterprise offers protection across identity (Windows Hello, Touch ID, Credential Guard, Conditional Access, Azure Active Directory), apps and data (Office DLP, Azure Information Protection, Cloud App Security), and devices (Device Guard, Intune).

## Microsoft's identity and information protection solutions

Refocus your efforts to protecting identities and information. Microsoft's identity and access management solutions help protect user's identities and secure access to apps and data, while our information protection solutions help ensure information is protected wherever it is, even in motion.



**60 percent of breaches stem from a compromised endpoint.**[3]

## Key takeaways

- ✓ Establish identity and access management control.
- ✓ 60 percent of breaches stem from a compromised endpoint.[3]
- ✓ An identity-driven security strategy turns focus from tracking an ever-growing number of endpoints to managing users accessing corporate data.
- ✓ More robust endpoint protection provides post-breach insight into adversary techniques.

03

## Step 03

# Defending against threats

Identity protection is an important step in securing data. But that's only a start. In an increasingly connected world, any Internet-connected device is an entry point for bad actors who are highly motivated to find their way in. Hackers know that every organization has multiple entry points. They use phishing scams, malware and spyware attacks, browser and software exploits, access through lost and stolen devices, social engineering, and other tactics to breach your security. It takes constant vigilance to maintain visibility across the threats you know and to become aware of emerging vulnerabilities.

Some tools can help maintain an always-on security approach, but a broader approach makes more sense. Traditional tools focus on prevention, but that's no longer sufficient. Organizations must assume that a breach has either already occurred or that one will occur soon, then find ways to significantly reduce the time required

> **The average large organization has to sift through 17,000 malware alerts each week.[4]**

Many security applications use built-in analytics and machine learning capabilities to produce insights into incidents, activities, and steps that attackers took. This is still a look at the past that may not speed up reaction and recovery. More security and advanced analytics solutions leverage those insights, automatically acting to prevent and respond to similar breaches, which helps significantly reduce the time to mitigation. Tremendous breadth and depth of signal and intelligence are behind these solutions, and when combined with the experience and knowledge of human experts, these solutions can be powerful tools against fast-moving threat actors.

Security leaders should work with the C-suite and the board to understand and maintain an acceptable level of risk and to balance it with the security budget. There is no one-size-fits-all solution for every organization, but a risk-management approach can help you decide where and how to invest in light of what's right for your organization.

## Microsoft’s threat protection solutions

Protect against advanced threats and recover quickly when attacked. Microsoft believes threat protection should enable organizations to protect themselves from advanced cyberattacks. It should also provide solutions that can help detect suspicious behavior within the organization. Finally, since no security solution is ever 100% effective, there must be processes and tools to quickly respond to threats, enable damage control, and limit the effects from an attack.

Microsoft threat protection solutions offer a combination of traditional approaches such as anti-malware and new innovations such as user and entity behavior analytics (UEBA) and endpoint detection and response (EDR). Microsoft is investing in both the prevention of attacks and post-breach detection and response.

## Key takeaways

- ✓ Adopt an “assume breach” approach to your security.
- ✓ Choose solutions that reduce the time it takes to detect and recover from a breach.
- ✓ Take a risk management approach to security to help decide where to invest.

04

Step 04

# Protecting information end-to-end

Data leaves your control now more than ever as your employees, partners, and customers share it. This drives productivity and innovation, but it can have significant consequences if highly sensitive data falls into the wrong hands. Security leaders must manage and secure data stored in multiple locations and shared across international borders. Organizations doing business in the EU must prioritize data protection before General Data Protection Regulation (GDPR) enforcement starts on May 25, 2018. GDPR will have a significant impact on how companies store and manage customer data, report breaches, communicate policies, and invest in internal resources.

Employees will tolerate only so much inconvenience before finding security requirement workarounds. Classifying and encrypting data are the best ways to keep it safe while still allowing productive use and sharing of information. Expecting employees to remember which data needs protecting and how to classify it properly introduces errors and delays, so it’s best to classify and label data as it’s created. You can sidestep human error by automating data classification. Tools can understand the context of data, such as credit card numbers within a file, or the sensitivity of data based on data origination. Once labeled, visual markings like headers, footers, and watermarks, and protection like encryption, authentication, and use rights can be automatically applied to sensitive data.

Security teams should also be able to track activity on highly confidential or high business impact shared files and revoke access if needed. This persistent protection travels with the data and protects it at all times—regardless of where it's stored or with whom it's shared.

> **We have to reconsider how we're going to protect data in this mobile-first, cloud-first world. The reality is, nobody has the expertise, the time, and the resources to do this on their own.**

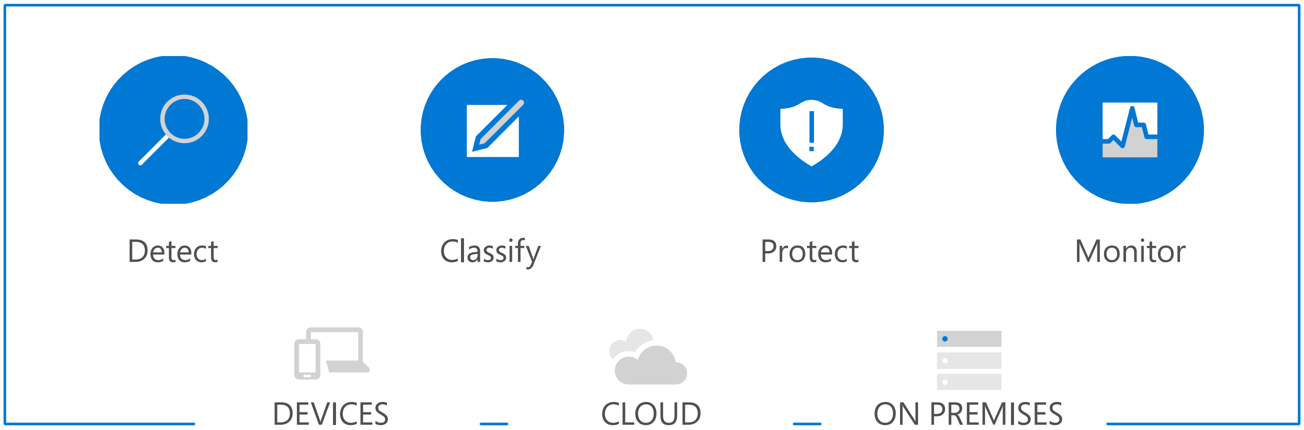
**Brad Anderson,**
*Microsoft Corporate Vice President,*
*Enterprise Mobility*

## Microsoft's information protection solutions

Protect against data leaks and accidental mishandling by securing information no matter where it is.

Microsoft's information protection solutions help you protect sensitive data throughout the lifecycle – across devices, apps, cloud services and on-premises.

Microsoft's approach to comprehensive protection of sensitive data throughout the lifecycle – inside and outside the organization, is to identify, classify, protect, and monitor critical data, no matter where it lives or travels. Microsoft 365 provides a more consistent and integrated approach to classification, labeling, and protection across our core information protection technologies.



## Key takeaways

- Security leaders need to focus on security at the data level.
- Data classification and encryption are becoming increasingly important. Data classification and labeling should occur at the time of creation, and security teams should be able to monitor activities on files and take rapid action.

05

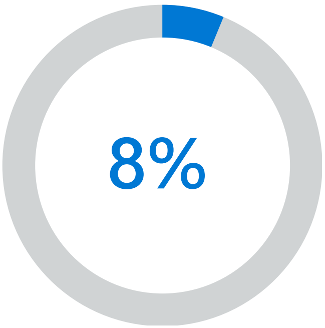
## Step 05

# Managing cloud use

Even if your organization doesn’t use cloud-based solutions, your employees probably do. This trend, known as shadow IT, is far bigger than most people know. In fact, only 8 percent of companies know the scope of shadow IT within their organizations, and the number of cloud services used by corporate employees is rapidly outpacing internal IT estimates.[5]

End users often accept terms and conditions without reading them and without fully understanding what they’re granting access to. Traditional network security solutions aren’t designed to protect data in SaaS apps and can’t give IT visibility into how employees are using the cloud. At the same time, blocking shadow IT is a poor solution—employees always find ways around restrictions. Overly rigid control deters innovation, conflicts with unplanned and demanding technology requirements, stifles productivity, and can decrease engagement and increase turnover among high-caliber talent.

Ultimately, we all have to accept that shadow IT is the new normal. Allowing end users and teams to use the cloud applications that are best suited for their type of work helps drive productivity and innovation. Gaining visibility, control, and threat protection of shadow SaaS apps are the first steps in managing risk and facilitating the digital transformation that has already started at your company.



**Only 8 percent of companies know the scope of shadow IT within their organizations.[6]**

**By 2020, a third of successful attacks experienced by enterprises will be on their shadow IT resources.[6]**

*Gartner's Top 10 Security Predictions 2016*

## Find out how employees are using the cloud

Cloud access security brokers (CASBs) provide organizations with a detailed picture of how their employees are using the cloud.

01 **Which cloud apps are employees using?**

02 **What risk do these apps pose to the organization?**

03 **How are these applications being accessed?**

04 **What sort of data is being sent to and shared from these applications?**

05 **What does the upload/download traffic look like?**

06 **Are there any anomalies in user behavior like impossible travel, failed logon attempts, or suspicious IPs?**

Better visibility and control over these apps and services lets security leaders develop and enforce reasonable, effective SaaS policies without sacrificing the security and compliance that the organization demands.

## Microsoft’s information protection solutions

Your organization can use the cloud without putting sensitive data at risk. Microsoft’s information protection solutions can give you visibility and extend your security policies into the cloud. Microsoft Cloud App Security helps you:

- ✓ Discover and assess risks: Identify cloud apps on your network, gain visibility into shadow IT, and get risk assessments and ongoing analytics.
- ✓ Control access in real time: Manage and limit cloud app access based on conditions and session context, including user identity, device, and location.
- ✓ Protect your information: Get granular control over data and use built-in or custom policies for data sharing and data loss prevention.
- ✓ Detect and protect against threats: Identify high-risk usage and detect unusual user activities with Microsoft behavioral analytics and anomaly detection capabilities.

Users frequently access apps where sensitive business or customer data may be stored. The ability to control what happens after the data is accessed is critical, and to bring the security of your on-premises systems to the cloud, with deeper visibility, granular data controls, and enhanced threat protection.

- Our mobile application management (MAM) capabilities and app protection policies can help protect the data at the app level including app-level authentication, copy/paste control, and save-as control.
- Configurable policies give you fine-grain control over what users can do with the data they access.
- You can apply policies to applications to protect data with or without enrolling the device for management, allowing you to protect corporate information without intruding on a user’s personal life.
- You can encrypt company data within apps with the highest level of device encryption provided by iOS and Android.
- You can also protect your company data by enforcing PIN or credential policies.

## Key takeaways

- **Rather than blocking shadow IT, look for solutions that allow you to monitor and assess for risk.**
- **CASBs can give you a detailed picture of how employees are using the cloud.**
- **With better visibility, you can then set policies that track and control how employees use these apps.**

06

## Step 06

# Moving to the cloud securely

Every organization is at a different stage of their journey to the cloud. Compliance requirements, local regulations, and other migration challenges mean that not every organization is ready to move critical workloads to the cloud.

But moving to the cloud doesn’t have to be a departure from your existing systems and processes. In a fully integrated hybrid IT environment, the cloud becomes an extension of your data center and the policies through which you control it. Hybrid cloud strategies also offer security leaders a measured approach to moving to the cloud, letting them move business functions to the cloud only when they are confident that the service offers the right amount of control.

Cloud service models affect how service providers and customers share responsibilities. This raises issues for CISOs as they navigate the challenges of relinquishing some of the controls of on-premises solutions for the greater security that cloud vendors can provide.

The rule of thumb for cloud security is that it's a shared responsibility. Cloud providers need to have state-of-the-art security and encryption, but customers must ensure that the services they purchase are in fact secure, and that they extend required security policies into their new cloud resources. Look for transparency when planning a cloud migration: vendors should publish detailed information on the security, privacy, and compliance of their services. They should also produce audit reports and other materials to help you verify their statements and help you understand where their responsibilities end and yours begin.

> **Public cloud providers offer better security than a small business or even a big enterprise is able to achieve. This is due to the investments that cloud providers are making to build and maintain their cloud infrastructure.**
>
> **Rene Buest,**
> *Senior Analyst and Cloud Practice Lead,*
> *Crisp Research* [7]

## Questions to ask your cloud provider

Assessing cloud providers isn't just choosing a service, it's choosing who to trust with your data. Critical questions about security and access control include:

01 **Is my data protected by strong security and state-of-the-art technology?**

02 **Is privacy by design incorporated to allow control of my data in my enterprise cloud?**

03 **Are there deep investments in robust and innovative compliance processes to help my organization meet its compliance needs?**

04 **Where will my data be stored, who has access to it, and why?**

05 **Does a third party review the cloud service provider annually?**

06 **What other country's compliance and regulatory standards does the cloud service provider adhere to?**

## The trusted cloud

People only use technology they can trust. You can move to the cloud securely when you're armed with knowledge from your cloud provider on their security, privacy, compliance, and transparency. Microsoft cloud services are built on these four principles, and the Trusted Cloud Initiative drives a set of guidelines, requirements, and processes for delivering rigorous levels of engineering, legal, and compliance support for our cloud services.

## Realize value faster with Microsoft cloud services and FastTrack

FastTrack has already helped over 40,000 customers maximize ROI, accelerate deployment, and drive adoption.

Migrate email, content, and light up Microsoft 365 services—including assessment and remediation guidance to help prep your infrastructure for the cloud.

Deploy and securely manage devices including Microsoft 365 powered devices.

Enable your business and gain end-user adoption.

Microsoft engineers deliver FastTrack to help you migrate to the cloud at your own pace and to help you get access to qualified partners if you need additional services.

## Key takeaways

- ✓ Establish identity and access management controls
- ✓ 60 percent of breaches stem from a compromised endpoint.[3]
- ✓ An identity-driven security strategy turns focus from tracking an ever-growing number of endpoints to managing users accessing corporate data.
- ✓ More robust endpoint protection provides post-breach insight into adversary techniques.

# Conclusion

The multifaceted nature of cyberthreats means that only solving some of your security challenges is no longer sufficient. Disparate solutions can still protect critical endpoints, detect breaches, and limit damage but the persistent nature of today's cyberthreats demands equally persistent defenses, which in turn demand a more holistic security approach.

Securing data and systems is now a top priority for every organization. Every company's security needs are unique, but companies face the same challenges and share the same responsibility to protect their data, people, and systems while encouraging innovation and growth. You need agile security frameworks that enable digital transformation, supported by holistic security strategies embedded into technologies, processes, and training programs. Microsoft 365 Enterprise offers a complete, intelligent solution that supports your digital transformation with security and compliance functionality built into every level.

Contact us

Microsoft 365 Homepage

[1] "Threat Landscape: By the Numbers," FireEye, 2016.
[2] According to Balaji Yelamanchili, executive vice president and general manager of Enterprise Security Business, Symantec, as quoted in: Symantec. "Symantec Introduces New Era of Advanced Threat Protection," October 27, 2015.
[3] Johnson, Ann. "Top Five Security Threats Facing Your Business and How to Respond." Microsoft Secure Blog. October 18, 2016.
[4] "The Cost of Malware Containment," Ponemon Institute (sponsored by Damballa), 2015.
[5] "Cloud Adoption Practices & Priorities Survey Report," Cloud Security Alliance, 2015.
[6] "Gartner's Top 10 Security Predictions 2016," Gartner, 2016.
[7] Rene Buest, quoted in "Top Cloud Security Fears & How The C-Suite Is Tackling Them," CIO, 2015.

# Conclusion

The multifaceted nature of cyberthreats means that only solving some of your security challenges is no longer sufficient. Disparate solutions can still protect critical endpoints, detect breaches, and limit damage but the persistent nature of today's cyberthreats demands equally persistent defenses, which in turn demand a more holistic security approach.

Securing data and systems is now a top priority for every organization. Every company's security needs are unique, but companies face the same challenges and share the same responsibility to protect their data, people, and systems while encouraging innovation and growth. You need agile security frameworks that enable digital transformation, supported by holistic security strategies embedded into technologies, processes, and training programs. Microsoft 365 Enterprise offers a complete, intelligent solution that supports your digital transformation with security and compliance functionality built into every level.

Microsoft 365 Homepage

Contact us

[1] "Threat Landscape: By the Numbers," FireEye, 2016.
[2] According to Balaji Yelamanchili, executive vice president and general manager of Enterprise Security Business, Symantec, as quoted in: Symantec. "Symantec Introduces New Era of Advanced Threat Protection," October 27, 2015.
[3] Johnson, Ann. "Top Five Security Threats Facing Your Business and How to Respond." Microsoft Secure Blog. October 18, 2016.
[4] "The Cost of Malware Containment," Ponemon Institute (sponsored by Damballa), 2015.
[5] "Cloud Adoption Practices & Priorities Survey Report," Cloud Security Alliance, 2015.
[6] "Gartner's Top 10 Security Predictions 2016," Gartner, 2016.
[7] Rene Buest, quoted in "Top Cloud Security Fears & How The C-Suite Is Tackling Them," CIO, 2015.