Microsoft

PSM
TECHNOLOGY | TALENT

6 steps to building a holistic security strategy for your nonprofit

Table of contents

The role of security in furthering your nonprofit's mission

In the past, cybersecurity and privacy were often low on the list of priorities for nonprofits. But, as cyberthreats have increased so have the risks of ignoring those threats. Breaches, compromised data, and cyberattacks can put vulnerable beneficiaries at risk, disrupt nonprofit operations and services, expose them to liability, and tarnish the reputation they have so painstakingly built.

Determining the best approach to security gets more difficult as attacks grow more sophisticated, staff and volunteers use a wider array of devices and applications, and data flows into and out of your organization through more channels. And don't think small organizations are smaller targets for data breaches. The risk is often higher for small organizations because they have fewer safeguards in place.

Many recent data hacks have generated a demand for more regulations around data security. One major example is the General Data Protection Regulation (GDPR), which applies to organizations that operate in Europe.

This regulation went into effect in May 2018, requiring organizations to protect the personal data and privacy of European Union citizens involved in transactions around the world. The GDPR applies no matter where you are located. Organizations that don't comply can face a significant fine. Similar regulations are being created in the U.S.

Leaders of nonprofits have to balance these challenges with the need to collaborate, innovate, and further your mission in the most cost-effective way possible. You need a multifaceted 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 a requirement for nonprofits of all sizes. The goal is to minimize the potential impact of increasingly sophisticated attacks by more effectively protecting a growing group of users, devices, applications, data, and infrastructure. And to do that with fewer resources.

Today's nonprofits need agile security frameworks built on holistic strategies embedded into technologies, processes, and training programs. This eBook highlights some of the strategies and best practices that nonprofits can use to successfully integrate security into the fabric of their operation.

> *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,**
> *Microsoft CEO*

Build a holistic security strategy for your nonprofit with Microsoft 365.

Microsoft 365 Enterprise provides organizations with a modern desktop that includes an integrated combination of Windows 10 Enterprise, Office 365, and the advanced security of Enterprise Mobility + Security. It is a complete, intelligent solution that empowers staff and volunteers to be creative and work together, securely from anywhere on their preferred device.

Microsoft 365 includes built-in holistic, identity-driven protection for users, devices, apps, and data. It provides sophisticated machine-learning models to reveal suspicious behavior in on-premises systems or in the cloud. And it applies advanced analytics to deliver richer insights that can help you detect and respond to attacks quickly. This level of security is woven into all layers of Microsoft 365. Here are six ways you can use Microsoft 365 tools to help protect your people, data, and devices while maintaining a high level of productivity.

01 Build an integrated security solution to speed response

Threat actors have evolved from "smash-and-grab" attacks to 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]

[1] "Threat Landscape: By the Numbers." FireEye. 2016.
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/Infographic-mtrends2016.pdf

> **The average large organization uses 75 distinct security products.[2]**

Cyberthreats have evolved from "smash and grab" attacks that compromise systems with a persistent, long-term presence to a much broader range of vulnerability. Attackers now use a variety of vectors and an increasingly advanced array of tools and techniques. These include:

- Stealing credentials
- Installing malware that erases itself to avoid detection
- Modifying internal processes and rerouting network data
- Social engineering scams
- Targeting staff mobile phones and home devices

To respond to this rapidly evolving threat landscape, organizations are deploying more and more security tools. The challenge is that each of these tools addresses specific issues, but they rarely work together. Many use proprietary dashboards, consoles, and logs. Because they are difficult to integrate, it is hard to create a comprehensive view and prioritize threats quickly. This is even more challenging when dealing with both cloud and on-premises resources. As a result, attacks can sometimes go undetected for up to 140 days.[1]

[2] Balaji Yelamanchili, executive vice president and general manager of Enterprise Security Business, Symantec, in "Symantec Introduces New Era of Advanced Threat Protection," October 27, 2015. https://www.symantec.com/en/in/about/newsroom/press-releases/2015/symantec_1027_01

Microsoft security management solutions

To gain more visibility and control over your security, Microsoft 365 provides a holistic approach to security where protection starts at the front door of your system and continues to protect your data anywhere while 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

Apply security controls across a growing number of endpoints

Nonprofits know that a data breach can have enormous costs both to an organization's finances and reputation. They must establish sufficient security controls to gain the visibility they need into threats and attacks. And they must address the growing trend toward consumerized IT, where staff and volunteers expect to be able to work anywhere, on any device or any platform, regardless of whether it has been sanctioned by the organization.

In this world, identity-driven security strategies allow organizations to transcend device control and apply controls based on role and need—no matter how the user connects. This focus on authenticating and managing users as they access the organization's assets enables nonprofits to protect data regardless of where it's stored, how it's accessed, or with whom it's shared.

There are a number of technologies that support this strategy. Identity and access management (IAM) solutions and mobile application management with data loss prevention (DLP) solutions help reduce risk by protecting access to applications and data on-premises and in the cloud. IAM can eliminate the need for multiple credentials by giving staff a single identity to access cloud and on-premises resources. Cloud-based IAM systems can also use 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.

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

How Microsoft defends its platform: The Cyber Defense Operations Center:

In 2015, Microsoft opened the Cyber Defense Operations Center to bring together our cybersecurity specialists and data scientists in one facility to help protect, detect, and respond to security threats against our infrastructure and services in real time. Since that time we have advanced policies and practices that accelerate the detection, identification and resolution of cybersecurity threats, and have shared our key learnings with customers.

Simplified and intelligent security management provides more visibility and control

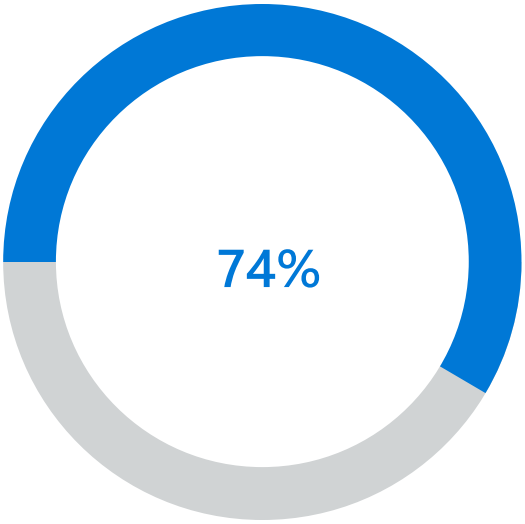
The key to a nonprofit's security is not having a single console for everything, but integration where it makes the most sense. You don't need all the point solutions to manage data points to help secure your end-user devices and expanding networks. Microsoft 365 provides intelligent security management with specialized controls based on your organization's needs, visibility where you need it, and guidance on how to harden your organization's security posture based on unmatched intelligence.

This gives you the flexibility to easily manage security with built-in controls and take advantage of security intelligence and guidance to enhance your security posture and defend against threats by:

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

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

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



74 percent of nonprofits reported that they don't use multifactor authentication to access agency email and other business accounts.[3]

Increasing security through identity and access controls

Microsoft 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).

Key takeaways

- **Establish identity and access management controls**
- **74 percent of nonprofits reported that they did not use multifactor authentication to access agency email and other business accounts, which is a critical security step.[3]**
- **An identity-driven security strategy turns focus from tracking a rapidly growing number of endpoints to managing users accessing corporate data.**
- **More robust endpoint protection provides post-breach insight into adversary techniques.**

[3] The Nonprofit Guidelines for Cybersecurity and Privacy whitepaper, 2017, Microsoft Corporation.

03 Expedite response to fast-moving threat actors

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 enough. Organizations must assume that a breach has either already occurred or one will occur soon. Based on that assumption they must find ways to significantly reduce the time required to detect and recover from it.

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

[4] Ponemon Institute, "The Cost of Malware Containment" (sponsored by Damballa), 2015.
https://www.ponemon.org/local/upload/file/Damballa%20Malware%20Containment%20FINAL%203.pdf

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 advanced security and analytics solutions use those insights to automatically act to prevent and respond to similar breaches and thus reduce the time to mitigation. When combined with the experience and knowledge of human experts, these solutions can be powerful tools against fast-moving threat actors.

Nonprofit security staff should work with the organization's management and 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 to best serve your organization.

Microsoft's threat protection solutions

Microsoft believes threat protection should enable organizations to protect against advanced threats and recover quickly when attacked. These solutions should also help detect suspicious behavior within the organization. And because no security solution is 100 percent 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 preventing attacks and responding more effectively to those that occur.

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 Moving to the cloud securely

Each organization planning to move some or all their workloads to the cloud must set their own path and their own timeline. Compliance requirements, local regulations, and other migration challenges are major factors in those decisions.

Fortunately, moving to the cloud doesn't have to mean leaving your existing systems and processes behind. In a fully integrated hybrid IT environment, the cloud becomes an extension of your existing system and the policies you use to control it. Hybrid cloud strategies also offer nonprofits a measured approach to moving to the cloud, so you can move functions to the cloud when you are ready.

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

Cloud security is a shared responsibility. Cloud providers need to have state-of-the-art security and encryption. Customers must ensure that the services purchased are in fact secure, and that they extend required security policies into the 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 understand where their responsibilities end and yours begin.

Questions to ask your cloud provider

Assessing cloud providers involves more than just choosing a service. It is about choosing who to trust with your data. Critical questions to ask about security and access control include:

- ✓ Is your data protected by strong security and state-of-the-art technology?
- ✓ Do you incorporate privacy by design and allow control of our data in our enterprise cloud?
- ✓ Do you make deep investments in robust and innovative compliance processes to help my organization meet its compliance needs?
- ✓ Where will my data be stored, who has access to it, and why?
- ✓ Does the cloud service provider subject itself to annual third-party review?
- ✓ Will the cloud service provider reject any requests for the disclosure of customers' personal data that are not legally binding?

- ✓ Does the cloud service provider adhere to the compliance and regulatory standards of different countries and locations?

The Trusted Cloud

People only use technology they can trust. You can move to the cloud securely when you have confidence in your cloud provider's security, privacy, compliance, and transparency. The Microsoft Cloud is built on these four principles. Our 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 the Microsoft Cloud and FastTrack

FastTrack offers planning, end-to-end guidance, and a range of online resources to help you deploy Microsoft cloud solutions. Customers who have eligible subscriptions to Microsoft 365, Azure, or Dynamics 365 can use FastTrack at no additional cost for the life of their subscription.

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.

FastTrack has already helped over 40,000 customers accelerate deployment and drive adoption. It can help you:

- Migrate email and content, as well as activate Microsoft 365 services, including assessment and remediation guidance to help prep your infrastructure for the cloud
- Deploy and securely manage devices including devices powered by Microsoft 365
- Expedite end-user adoption

Key takeaways

- **Moving to the cloud does not have to mean a departure from existing systems and processes.**
- **A hybrid cloud offers a measured approach to cloud migration.**
- **When evaluating cloud service providers, ensure that they adhere to international standards.**
- **Look for vendors that publish detailed information about how they operate their services and handle data.**

05 Risk of shadow IT

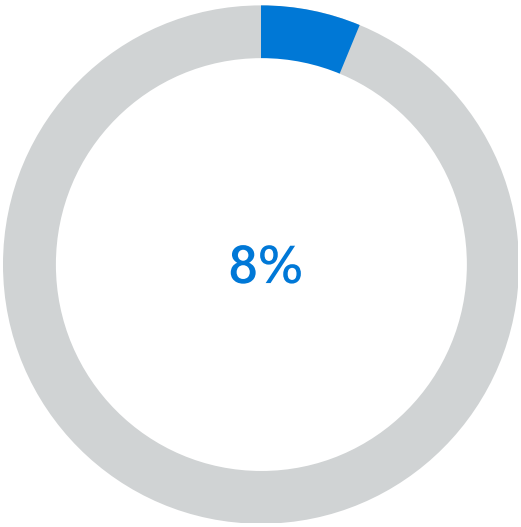
Even if your organization doesn't use cloud-based solutions, your staff probably does. This trend, known as shadow IT, is far bigger than most people know. Research shows that only a small fraction of organizations know the scope of shadow IT within their environment,[5] and the number of cloud services used by their staff is rapidly outpacing internal IT estimates.

> *By 2022, a third of successful attacks experienced by enterprises will be on their shadow IT resources.*[6]
>
> Gartner's Top 10 Security Predictions 2016

Shadow IT exposes your organization to huge risks in IT and application management, security, and compliance.

[5] "Cloud Adoption Practices & Priorities Survey Report." Cloud Security Alliance. January 2015. https://downloads.cloudsecurityalliance.org/initiatives/surveys/capp/Cloud_Adoption_Practices_Priorities_Survey_Final.pdf

[6] Gartner, Smarter With Gartner "Gartner's Top 10 Security Predictions 2016." June 15, 2016. http://www.gartner.com/smarterwithgartner/top-10-security-predictions-2016/



Only 8 per cent of companies know the scope of shadow IT within their organizations.[7]

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 cloud apps and can't give IT visibility into how your staff is using cloud resources.

Blocking shadow IT is not the answer, because users always find a way around restrictions. Overly rigid control deters innovation, conflicts with unplanned and demanding technology requirements, stifles productivity, and can decrease engagement and increase turnover among valuable staff.

Ultimately, we all have to accept that shadow IT is the new normal. Allowing individuals and teams to use the cloud applications that best meet their needs helps drive productivity and innovation. Gaining visibility, control, and threat protection of shadow software-as-a-service apps are important steps in managing risk and facilitating the digital transformation that has already started in your organization.

[7] Cloud Adoption Practices & Priorities Survey Report, January 2015, Cloud Security Alliance

Getting a handle on shadow IT

- Which cloud apps staff are using
- The risk these apps pose to the organization
- How these applications are being accessed
- The types of data being sent to and shared from these applications
- A picture of the upload/download traffic
- Any anomalies in user behavior like impossible travel, failed logon attempts, or suspicious IPs?

Better visibility and control over these apps and services helps nonprofits develop and enforce reasonable, effective cloud policies without sacrificing the security and compliance the organization demands.

Microsoft's information protection solutions

Your organization can use the cloud without putting sensitive data at risk. Microsoft information protection solutions can give you visibility and extend your security policies into the cloud. Microsoft Cloud App Security, a CASB solution, 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 comprehensive 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 financial or donor data may be stored. The ability to control what happens after the data is accessed is critical. You can bring the security of your on-premises systems to the cloud, with deeper visibility, highly specific data controls, and enhanced threat protection by:

- Using 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.

- Taking advantage of configurable policies that give you fine-tuned control over what users can do with the data they access.

- Applying policies to applications to protect data with or without enrolling the device for management. This allows you to protect organizational information without intruding on the user's personal life.
- Encrypting your data within apps with the highest level of device encryption provided by iOS and Android.
- Enforcing PIN or credential policies.

Key takeaways

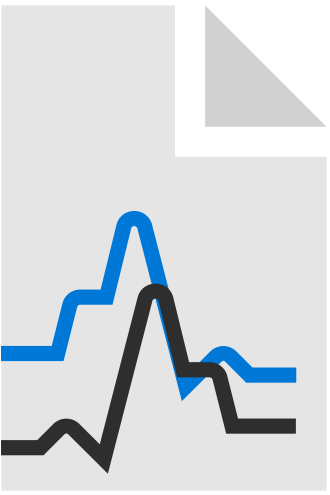
Rather than blocking shadow IT, look for solutions that allow you to monitor and assess for risk.

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 Balance end-to-end information protection with productivity

Data leaves your control now more than ever as your staff, volunteers, and directors share it. This drives productivity and innovation, but it can have significant consequences if highly sensitive data falls into the wrong hands. Many nonprofits must manage and secure data stored in multiple locations and shared across international borders. Organizations must meet a growing number of data security regulations, including GDPR. This will have a significant impact on how nonprofits store and manage data related to donors, volunteers, directors, and staff; report breaches; communicate policies; and invest in internal resources.



The challenge with many security requirements is that users will tolerate only so much inconvenience before finding workarounds. Classifying and encrypting data are the best ways to keep it safe while still supporting productive information sharing and collaboration. Expecting your staff 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 is 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-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 is stored or with whom it is shared.

Microsoft's information protection solutions

You can protect against data leaks and accidental mishandling by securing information no matter where it is. Microsoft information protection solutions help you protect sensitive data throughout the lifecycle—across devices, apps, cloud services, and on-premises.

This includes identifying, classifying, protecting, and monitoring 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.

> *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, *Corporate Vice President for Enterprise Mobility, Microsoft*

Key takeaways

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

Conclusion

The multifaceted nature of cyberthreats means that it is not sufficient to only solve some of your security challenges. Disparate solutions can protect critical endpoints, detect breaches, and limit damage, but the persistent nature of today's cyberthreats demands equally persistent defenses. And that requires a more holistic security approach.

Securing data and systems is becoming more and more important for nonprofits. Although each organization's security needs are unique, all face the same challenges. All share the same responsibility to protect their data, people, and systems while encouraging innovation and growth. This requires an agile security framework that enables digital transformation, supported by holistic security strategies embedded into technologies, processes, and training. Microsoft 365 Enterprise offers a complete, intelligent solution that supports digital transformation with security and compliance functionality built into every level.

To learn more about nonprofit offers and to get help finding the right products for your organization, contact PSM Partners.

psmpartners.com

Sales@psmpartners.com

Learn more about how Microsoft can help with your holistic security strategy.