How does your cybersecurity posture need to change?

The digital transformation of today's enterprises has created a new state of play in cybersecurity – and new risks.

Microsoft

Empowering business
for what's next

Table of contents

The new security landscape

Recent high-profile incidents have brought cybersecurity to the forefront of mainstream conversations as the impact of attacks has been felt around the world by organizations and individuals alike. Unfortunately, given current trends, organizations will continue to see sophisticated cyber-attacks for the foreseeable future. Sustained ransomware campaigns, spear phishing, and other high-profile attacks continue to highlight the need for an advanced and comprehensive cybersecurity strategy.

The statistics clearly indicate the adverse impact cyber threats have on today's businesses. With this in mind, Microsoft has invested heavily in the security domain to enable organizations to mitigate the effects of the evolving threat landscape and empower them to succeed in the new norm of daily cyber-attacks.

The main challenges organizations are facing with respect to threat protection include: vulnerability to advanced attacks, the inability to detect malicious activities, and difficulty in responding to threats quickly. The escalation in the number of threats and their corresponding level of sophistication leave many organizations more exposed to risk. With the volume of threats and evolving capabilities of attackers, detection of malicious activity has become increasingly difficult for security professionals. Security teams often struggle to understand how to respond to threats and the length of time to respond can add to the devastating effects of a breach.

You need to ask yourself:

How will your organization protect itself from advanced cyber-attacks?

What are you doing to detect suspicious behavior within the organization and beyond?

What processes and tools will you implement to quickly respond to threats and quickly recover from the effects of an attack?

Before we take a deeper look at how Microsoft Enterprise Services can help customers with these threat scenarios, it is important to understand how the IT industry and threat potential has evolved over the last decade or so.

Digital transformation

To be competitive in the marketplace businesses are seeking to transform and innovate using new and powerful technologies. The proliferation and availability of cloud, mobile, and IoT technologies is fueling major disruptions in once-settled markets as:

1. **Digital native startups leverage this new technology to disrupt longstanding business models.**

2. **Existing organizations are driving digital transformation to empower employees, optimize operations, and deliver value to customers.**

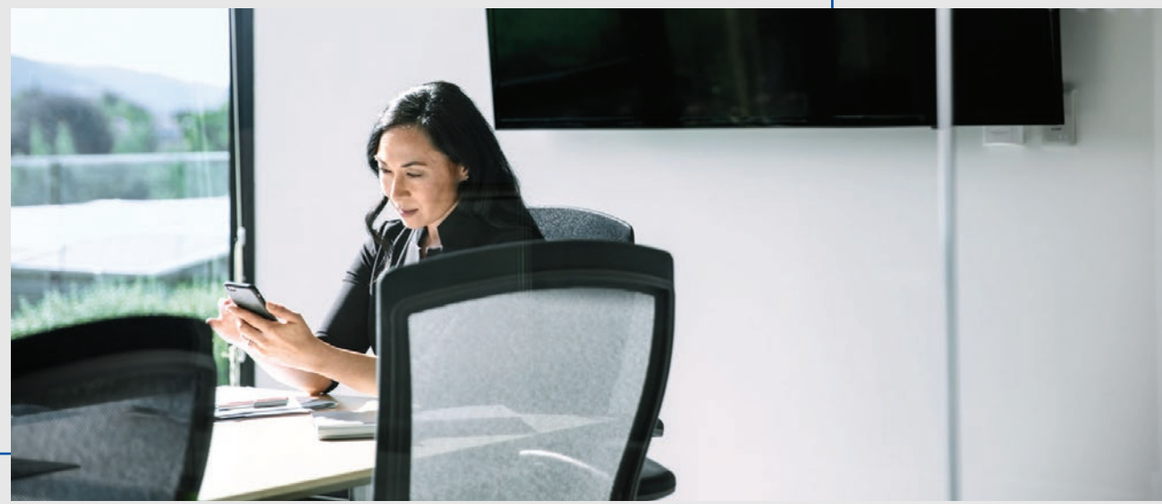
As organizations make the transition to a digital workplace they are often overwhelmed by a new set of security challenges which can impact innovation and speed to market. Likewise, Microsoft is seeing major transformation of almost all aspects of IT and information security. Several key trends stand out as Information Security departments operate in a world that has changed dramatically since the current generation of security best practices were established.

These trends are the IT transformation components that support the business's digital transformation and will provide both challenges and opportunities for information security at your organization.

DATA POINT

86% of CEOs considered digital transformation their #1 priority; believing technology will transform their business more than any other global trend.

Source: https://www.forbes.com/sites/gilpress/2015/02/27/new-pwc-survey-ceos-embrace-digital-transformation/



Enterprise IT is cloud hybrid

In an age where almost all enterprises are embracing digital transformation, it will be difficult for IT, business, and security stakeholders to resist the value proposition of cloud computing as vendors offer compelling new capabilities exclusively through cloud services. However, it will also be difficult and undesirable for many organizations to shut down all on-premises datacenters and networks due to a variety of reasons including dependence on legacy applications, bandwidth, unreliable connectivity in some geographies, and regulatory reasons. While Microsoft offers best in class solutions for these challenges, we still anticipate that enterprise IT departments will be operating under hybrid cloud models for the foreseeable future during this transition.

> "We have begun our journey to both private and public cloud platforms for select applications. Having met our strict compliance, security, and risk requirements, Microsoft was our choice as a strategic partner in this journey."

Keith Silvestri
Chief Technology Officer, KeyBank

KeyBank

Technology mobility and volume is exploding

With expectations set for the continued growth of mobile devices, organizations will have to improve their ability to manage the variance of trustworthiness across devices to better balance risk and productivity. Even so, users will continue to demand a world-class experience within native applications versus the limited productivity functionality of most current Mobile Device Management (MDM) solutions.

Pervasive digital transformation and IoT

Businesses will be digitally transforming to compete with cloud-native startups that seek to disrupt existing industries and markets. This will likely drive a massive increase in Internet of Things (IoT) device adoption and cloud service adoption to accommodate the need for storage, processing, analytics, blockchain, management, etc. Since personal computer risk strategies don't apply to most IoT devices, the IoT space will create increased challenges around new ways of managing device risk.

Increasingly hostile environment

Both the attack surface of the modern enterprise and the volume and sophistication of threats are continuing to rise. Fortunately, we have observed that attackers tend to follow rational behavior as they manage their return (successful attacks) for their investment (time and resources on an attack, developing or acquiring tools, and learning skills). Due to this, most attackers tend to favor the simplest and cheapest means to achieve their goals. Most attackers will choose a proven method such as an existing tool or a freely available toolkit before developing a new tool or technique.

Despite this advantage, one challenge is that many well-funded attackers such as nation states have already developed a large library of sophisticated tools that cost very little to use against another target. While not the norm, these well-funded attackers also have the time and capital to invest in new strategies that are necessary for some targets. Over time, these new tools make their way into the tool kit of the standard monetarily motivated attacker, forcing modern day security to compete not just with standard threats but with nation state capabilities. This problem is further enhanced as certain state actors target key economic and infrastructure targets as part of their campaigns.

New challenges for security professionals

While the challenges are significant, there is also a massive opportunity for organizations to solve longstanding security problems with this next generation of computing. Digital transformation provides unique challenges for security administrators but may also offer some surprising solutions.

Software as a Service (SaaS) adoption to increase collaboration and agility

SaaS provides rapid value without many of the challenges of traditional software deployment and maintenance. While IT professionals typically do not have to update this software, they do need to be aware of their use, assess their trustworthiness, and manage the available security controls. One of the major challenges of this is that 80% of users reported using non-approved SaaS apps.[2] Is your IT department ready to mitigate shadow IT while providing the tools your employees need to be productive?

Demand for a 1st class mobile experience

With many workplaces supporting a Bring Your Own Device or Choose Your Own Device model, users increasingly get to decide what devices and apps they can use to get their job done. This variety of devices and platforms create a challenge for IT professionals to meet the goal of providing a great user experience on secure mobile devices. Business users need fully functional applications for creating value on corporate data and capabilities beyond the limited functionality that come with most MDM providers.

Internet of Things

With the proliferation of IoT, the manageability and visibility of these devices varies greatly from PC to mobile devices in the following ways:

- Higher volume and limited functionality
- Limited resources to run traditional agents
- Frequently collect new forms of telemetry with new privacy and security implications

Cloud required to support analytics and IoT management

Even if IT departments are not adopting cloud platforms and infrastructure for its own value propositions, many of the new IoT architectures require cloud services to collect and report on IoT scenarios. This forces IT professionals to evaluate the trustworthiness and integration of controls for these platforms. Fortunately, this comes with both security and cost benefits as organizations report 11% lower IT support costs for worker solutions in the cloud.[3]

2 https://enterprise.microsoft.com/en-gb/articles/digital-transformation/10-stats-that-reveal-the-changing-face-of-it-security/
3 Forrester Total Economic Impact Analysis, "Improving Firstline Worker Performance With Microsoft Office 365"

Have you adapted to the modern threat landscape?

While the digital workplace has evolved, so too has the threat landscape across the globe, with hackers using more sophisticated methods to compromise users and networks. The days of young hackers sitting at a desk writing malware for notoriety is no longer the norm. They still exist, but more often than not today's attackers are mostly people or organizations out for financial gain or nation states that are trying to move their agenda forward. The way that hackers approach cyber-attacks today has dramatically changed, and organizations must therefore adapt and change the ways that they protect themselves.

In addition, today's cyber-attacks are often more rapid and disruptive than the types of attacks that security programs have traditionally encountered. Much like the worms of decades past, these attacks happen very rapidly because they are often fully automated and self-propagate once launched. The attacks are designed to be disruptive to operations by encrypting, and sometimes destroying, data. We can help-Microsoft's built-in, intelligent capabilities work together to more effectively govern data and save it from both inadvertent employee leaks and advanced threats.

Hope for the best, prepare for the worst

Not long ago, the mindset was for security professionals to do everything within their power to protect their organization from being breached. But times have changed, and the approach to cybersecurity has evolved into one in which the mindset should be that a breach has already occurred or will occur. Every organization should assume compromise, whether it's a legitimate employee accessing information they shouldn't by accident or a hacker that's been sitting quietly monitoring network traffic for clear text passwords or by using a user name password acquired by social engineering. Therefore, you need to ask yourself, if one of your user's account credentials or workstation has been compromised, what actions are you able to take to minimize the fallout and prevent someone from gaining a foothold in your organization? What solutions do you have in place to not only detect, but to recover from a breach? With the average cost of a breach hovering just under $4 million per incident[4], a quick response is vital for your organization. Today, organizations need to focus on both the prevention of attacks and post-breach detection and response.

4 Ponemon Institute, "2017 Cost of Data Breach Study: Global Overview"

A new approach to security

The digital world in which we now live requires a new approach to how we protect, detect and respond to security threats. In November 2015, Microsoft CEO Satya Nadella delivered a keynote that highlighted this need for a new approach to security. He showcased how innovations in Windows 10, Office 365, Microsoft Azure, and Microsoft Enterprise Mobility Suite work in tandem with each other, and with solutions from the security ecosystem, to deliver a holistic and agile security platform for today's enterprise.

Satya also shared how Microsoft uses its unique insight into the threat landscape to create an intelligent security graph that we use to inform how we protect all endpoints, better detect attacks and accelerate our response. The Microsoft Intelligent Security Graph is powered by inputs we receive from across on-premises and Microsoft cloud services such as Office 365, Azure, and Windows. Each month, there are an average of 400 billion emails analyzed for spam and malware, 450 billion user authentications processed, 1 billion Windows devices updated, and 18 billion web pages scanned.[5]

> "As the world continues to change and business requirements evolve, some things are consistent: a customer's demand for security and privacy. We firmly believe that every customer deserves a trustworthy cloud experience and we are committed to delivering that experience in the cloud."

Satya Nadella
CEO, Microsoft

Microsoft

5 Anderson, Brad. "Secure and Manage your Digital Transformation." Microsoft. 2017. https://myignite.microsoft.com/videos/34952

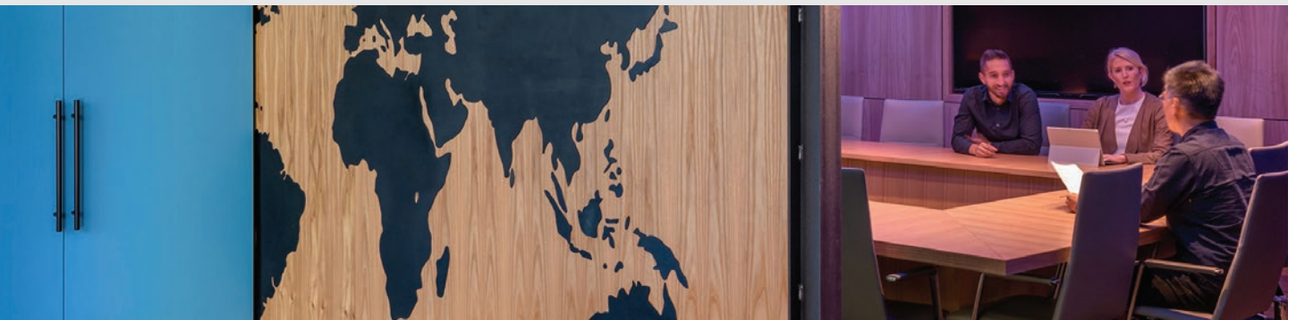
What makes the cloud safer than on-premises?

The cloud has significant advantages for solving today's cybersecurity problems. In contrast to on-premises computing, cloud services can detect and respond in almost real time. This response time advantage can be attributed to the continuous logging of activities and access to security event information across millions of devices with many millions of network connections. Behavioral analysis, anomaly detection and sophisticated statistical algorithms are used and continuously updated to help identify potential security incidents as they occur.

> "We wanted the best of both worlds—easy-to-use consumer-based technology that had the security, privacy, regulatory compliance, and governance of a corporate solution."

Mansour Zadeh
Senior Vice President and Global CIO, Smithfield Foods
Smithfield

Drawing from this telemetry, the Microsoft Intelligent Security Graph derives unparalleled insights to help organizations better protect against, detect, and respond to attacks. Added to this benefit is the 'community effect': When one organization is attacked, other organizations can immediately benefit from Microsoft's analysis of that attack. Thanks to the annual investment in security of more than $1 billion and the unprecedented amount of data collected and analyzed, Microsoft's security offerings in the cloud are stronger than ever.



Another advantage of the cloud is that it allows you to transfer some of the day-to-day responsibilities for cybersecurity to the cloud provider. More than 60 percent of organizations report having too few information security professionals, and the gap between qualified professionals and unfilled positions is expected to reach 1.8 million by 2022.[6] This shortage inevitably means there aren't enough resources to secure all of your assets and, left untended, attackers can achieve their objectives using techniques ranging from exploiting unpatched firmware, devices, and operating systems, to configuration weaknesses and human errors by users or administrators. Enterprise-level cloud providers–due to their scale, resources, and investments in defending their platform and their customers, are able to provide capabilities and security intelligence that few companies can match, enabling you to focus your team and budget on other parts of security.

Furthermore, while many companies take a "bolt-on" approach to security by adding additional layers and applications, Microsoft's broad set of services provide a holistic ecosystem of integrated security capabilities that work with an organization's existing technology investments. This takes the integration burden off our customers so that they can focus on managing risk and attacks instead of integration work.

Bottom line: the static infrastructure and tools of an on-premises environment cannot keep up with an ever-changing landscape of threats. The security built into Microsoft's cloud—from billions of inputs—can. Moving to the cloud will eliminate the burden (and possible delay) that security patches and server upgrades represent to your IT teams, enabling you to focus on delivering value to your customers while secure in the knowledge your enterprise is protected.

> "It quickly became clear that our data would be safer in the Microsoft cloud than in our own datacenters. After all, Microsoft is an expert in enterprise security."

Jeff Heyde
Director of Global Systems, Dana Holding Corporation
DANA

Businesses and users are going to use technology only if they can trust it. The Microsoft Cloud is built on four foundational principles-security, privacy, compliance, and transparency. 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. To learn more, you are encouraged to visit the **Microsoft Trust Center**.

6 Reed, Jason, Yiru Zhong, Lynn Terwoerds, and Joyce Brocaglia. "The 2017 Global Information Security Workforce Study: Women in Cybersecurity." Frost & Sullivan. 2017. https://iamcybersafe.org/wp-content/uploads/2017/03/WomensReport.pdf

The 4 pillars of cyber resilience

From a security operations standpoint, the top security priorities for most organizations can be bucketed into four areas:

1. **Safeguarding user identities and controlling access to resources**
2. **Defending against advanced threats and recovering quickly if attacked**
3. **Protecting sensitive and confidential information**
4. **Gaining visibility into and control over security tools**

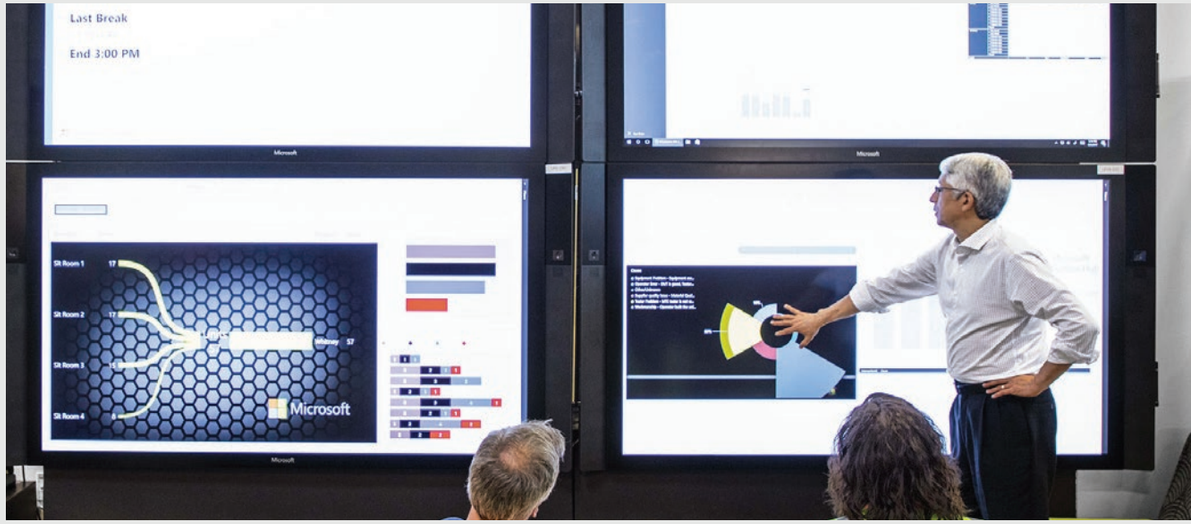
Identity & access management
Protect users' identities & control access to valuable resources based on user risk level with conditional access

Threat protection
Strengthen your pre-breach posture with built-in protection & recover quickly with automated remediation when attacked

Information protection
Protect documents and emails with encryption that travels with them as they move inside and outside your organization

Security management
Gain end-to-end visibility of your organization's security and manage policy centrally

Microsoft has organized these needs into four pillars we focus on solving for customers: identity and access management, threat protection, information protection and security management. By building and implementing a security roadmap for these four areas which focuses on your critical business priorities, you will build resilience against cyber-attacks into your business and let you focus on what you do best.



Developing a cyber resilient strategy

Microsoft is focused on enabling a secure modern enterprise that meets both security and productivity needs. With Microsoft Enterprise Services as your partner, you'll have full access to our expertise in the Microsoft portfolio and our capabilities, including those of our global network of professionals and partners. We have proven results that demonstrate our ability to lead change and deliver on our promise--to empower you to accelerate the value you imagine and realize from your digital experiences.

Microsoft provides organizations of all sizes guidance, strategies, and solutions so they can build a cyber-resilient foundation for their business. We can help you establish a baseline of your current security posture, then assist with the development of a security roadmap and subsequent implementation of technology to secure the four pillars mentioned earlier in the paper: identity and access management, threat protection, information protection, and security management. This allows you to focus on the business of IT rather than wondering, "What do we do next?"

Finally, we can help you develop cyber resilient strategies based on the security tenets of **protect, detect, and respond**, as follows:

Protect

Organizations are vulnerable across identity, apps and data, their devices and their infrastructure. Microsoft has built solutions for each of these potential attack vectors to help protect organizations from cyber-attacks.

Identity. We can help secure your end-user identities while leveraging our machine learning, behavioral analytics, and signals from the threat landscape to identify vulnerabilities and reduce the attack surface.

Apps and data. To protect your apps and data, Microsoft has developed solutions to help you secure email, data, and even your app ecosystem.

Devices. Microsoft has solutions to help protect your devices to prevent encounters, isolate malicious threats, and to control execution of untrusted applications or code.

Infrastructure. We can also secure your cloud infrastructure by leveraging built-in controls across servers, apps, databases and networks.

Detect

As organizations rapidly grow, the tendency is to rely more and more on technology and enable mobile and flexible working conditions. This causes increasing operational complexity within the organization and makes it more challenging to detect suspicious behavior. Realizing this, Microsoft has built several solutions and features to help our customers gain visibility across their organization.

Identity. Detect suspicious activities and compromised user credentials.

Apps and data. Detect risky apps and malicious data, identify and mitigate shadow IT, inspect and revoke file sharing.

Devices. Detect advanced threats, deviations from policies, abnormal behavior.

Infrastructure. Detect advanced persistent threats, advanced threats to hybrid workloads, and compromised systems.

Respond

In the event of a breach, the ability to respond quickly is paramount to maintaining your business operations. Like protection and detection, Microsoft has broken down response solutions across the organization by identifying the attack vectors. If organizations can cohesively respond across the potential attack vectors, they will be able to rebound more quickly from an attack.

Identity. Respond to compromised identities by elevating access requirements based on risk assessment.

Apps and data. Respond to compromised apps and data by removing or monitoring access.

Devices. Respond dynamically to any suspicious device or application.

Infrastructure. Respond early to compromised workloads across hybrid infrastructure by utilizing standard procedures enabled by automated machine learning processes.

> "The beauty of having these solutions is that they help secure us against inbound threats and monitor everything happening on our devices."

Mike Fermin
Assistant District Attorney, San Bernardino County

Improving your security posture with Microsoft Enterprise Services

Organizations need to protect themselves and Microsoft is positioned to help. Microsoft Enterprise Services has the industry expertise, technology and resources to help you better protect your business and critical assets. Our solutions help organizations integrate security capabilities within Microsoft products and provide solutions that help you protect, detect, and respond to cyber threats.

Cybersecurity Essentials

Our Cybersecurity Essentials solution is delivered by Microsoft Enterprise Services experts who help you assess risks and implement capabilities to protect your environment against cybersecurity attacks, detect attacks and respond to them as they happen.

Assess your cyber risk exposure and create an improvement roadmap

- Assess cyber risk exposure
- Identify cloud security additions to bridge security gaps
- Plan your personalized cloud security

Plan your personalized cloud security Protect your identity platform from advanced cyber-attacks

- Upgrade existing Active Directory
- Harden Active Directory against cyber-attacks
- Secure endpoints
- Protect assets using secure cloud identity
- Protect virtualized workloads

Secure privileged access from advanced cyber-attacks

- Workstations for privileged users
- Control privileged access
- Dedicated environment for Domain Administrators

Detect, investigate and Respond to suspicious activity

- Detect advanced threats on devices
- Detect advanced Identity threats

Information Protection

Our Microsoft Enterprise Services experts deliver our Information Protection solution to help you detect, classify, protect, and monitor your data on-premises and in cloud environments:

Prepare modern identity and secure admin operation for cloud-based services

- Create a hybrid identity environment
- Protect Administrator operations for cloud services

Enable information protection capabilities based on your requirements by detecting, classifying, protecting, and monitoring data

- Data discovery, classification & labeling, and rights management
- IT shadowing prevention, cloud data leakage prevention, cloud data visibility, and abnormal usage behavior detection on cloud data
- Accidental data leakage prevention in Windows 10 devices
- Data protection for mobile devices including Android and iPhone

Threat Modeling for Security Risk

Threat modeling is widely used inside Microsoft and is one of the mandatory approaches our developers use to build secure applications, systems, and services, and is a part of our Security Development Lifecycle (SDL). The SDL has a critical role in embedding security and privacy in our software and culture at Microsoft.

Microsoft Enterprise Services has developed specialized security assessment capabilities that we have deployed in the real world. Benefit from our wide-ranging knowledge and experience on threat modeling for systems on premises and in the cloud, and our commitment to promoting security in our services.

The threat modeling process can be used to identify which threats are most likely to affect your IT systems and environment. Having a solid understanding of your infrastructure and how your applications are implemented will enable you to prioritize which threats are the greatest risk and respond with appropriate countermeasures. Threat modeling's structured approach is more cost efficient—and more effective—than haphazardly applying security features without knowing what threats to address.

Threat modeling accomplishes the following:

- Defines the security of an application
- Identifies and investigates potential threats and vulnerabilities
- Brings justification for security features at both the hardware and software levels for identified threats
- Identifies a logical thought process in defining the security of a system
- Results in finding architecture bugs earlier and more often

Conclusion

If you're ready to take the next step into a more secure future, we can get you there. With internal access to the full platform stack and product engineering teams, Microsoft Enterprise Services is uniquely positioned to bring together product, services, and device offerings to provide innovate new solutions and resolve longstanding security challenges. You can benefit from our more than 35 years of commitment to promoting security in our products and services, to helping our customers and partners protect their assets, and working to help ensure that their data is kept secure and private.

Microsoft Enterprise Services can help get you started on your journey to a cyber-resilient foundation and help you address the following business challenges:

Understanding current cyber risk exposure and planning a security roadmap

Protecting the Identity platform and endpoints against cyber-attacks

Securing privileged access against cyber-attacks

Detect, investigate and respond to sophisticated cyber-attacks

We invite you to schedule a **Cybersecurity Improvement Workshop** with us. This one-day workshop is designed to determine your security posture and identify a prioritized list of cybersecurity initiatives to bridge gaps. During the workshop we'll start by discussing your top business priorities and concerns and define the scope of effort needed to help you better protect against and detect and respond to threats. The goal is simple – a small investment in time could mitigate against significant loss of data, credibility and downtime letting you focus on what you do best: delivering value to your customers.

When will you invest in a safer future?

Contact your Microsoft representative to learn more. For more information about Consulting and Support Solutions from Microsoft, visit www.microsoft.com/services.

What's next?

No matter where you are on your digital transformation journey, Microsoft Enterprise Services can help.

Empower employees

Empower a high-quality, committed digital workforce to work as a team anywhere, on any device, with seamless data access—helping you innovate, meet compliance requirements, and deliver exceptional customer experiences.

Engage customers

Reimagine the customer experience for a digital world and deliver more value through insights and relevant offers by engaging customers in natural, highly personal, and innovative ways throughout the customer journey—driving increased relevance, loyalty, and profitability.

Optimize operations

Gain breakthrough insights into risk and operational models with advanced analytics solutions and act on real-time intelligence to optimize risk management and meet regulatory requirements.

Transform products

Drive agility with open, connected systems and automated digital processes to support new product development and optimize distribution channel strategies, while meeting the security, privacy, and transparency expectations of customers, regulators, and shareholders.

Credits

Many subject-matter experts from various groups at Microsoft contributed to the conceptualization and articulation of the story contained in this document.

Binil Arvind Pillai

Director of Business Programs, Microsoft Enterprise Services

Nindy Hunter

Sr. Business Program Manager for Modern Workplace, Microsoft Enterprise Services

Andrej Budja

Architect, Cybersecurity, Microsoft Enterprise Services

Contributors

Gus Gustafson
Director Business Programs, Microsoft Enterprise Services

Eric Daigle
Director Business Programs, Microsoft Enterprise Services

Amy McCullough
Director Product Marketing, Microsoft Enterprise Services

Conor Bronsdon
Consultant, Olive & Goose

Joe Turick
Consultant, Olive & Goose

Kurt Frampton
Sr. Designer, Simplicity Consulting

Microsoft Enterprise Services empowers organizations to accelerate the value realized from their digital experiences.

Imagine.
Realize.
Experience.

microsoft.com/services