Enabling a more secure transformation in the digital era

Microsoft

Empowering business
for what's next

Table of contents

Trillions at risk – the growing cybercrime problem

Cybercrime is a growing concern for businesses and governments worldwide. With an estimated cost of $3 trillion in economic value due to cybercrime by 2020[1], many enterprises are asking – how can we protect ourselves in this new digital era? How can we verify identities and ensure security for our customers and employees?

> "Digital Transformation has raised the stakes, with 69% of senior executives telling Forbes that this is forcing fundamental changes to security strategies. If you're going to open your organization up to new customers, new markets, and anytime, anywhere access, you need to do it securely."

Ann Johnson

Corporate Vice President, Cybersecurity Solutions, Microsoft

Microsoft

In the digital world that we live in, you can no longer simply protect your on-premises workstations and hope for the best. The opportunities, collaboration, and mobility that the cloud has led to also presents new risks and vulnerabilities. Reports from the Center for Strategic and International Studies (CSIS)[2] and McAfee[3] estimate that the cost of cybercrime to the global economy is around $600 billion annually, a stunning 0.8% of global GDP. Of that, cyber espionage – such as the massive breach by Chinese hackers of the US Office of Personnel Management that exposed the personal information of 21 million Americans [4] - accounts for 25% of that damage, more than any other category of cybercrime. The connectivity of today's institutions and workers has opened a vast terrain for cybercrime extending IP and data theft well beyond traditional defense perimeters.

How are today's cyber threats changing?

One major challenge of the expanding defense perimeter is the growing need to verify identity across devices. As employees' access applications and data from multiple devices at work, at home, and on the go – the challenge of verifying an employee's digital identity increases exponentially. The same is true for an organization's customers as their ability to interact with IoT and SaaS applications spreads across new devices and locations. As organizations expand their digital estate, more attacks surfaces are exposed. To make matters worse, each breach that happens is costing more. The trend is clear – we need to adapt how we think about cybersecurity for today's digital world.

DATA POINT

The average cost of a breach is up over $200,000 from 2017-2018 and organizations are taking a staggering 196 days to detect breaches on average.

Source: https://securityintelligence.com/ponemon-cost-of-a-data-breach-2018/

1 Envision Your Modern Workplace 2018
2 Center for Strategic and International Studies (CSIS)
3 https://www.mcafee.com/enterprise/en-us/solutions/lp/economics-cybercrime.html?utm_campaign=TL_EC_18Q1&utm_source=mcafeeblog&utm_medium=organic&eid=18TL_ECGLQ1_ML_SO_ST&elqCampaignId=23320
4 http://securityaffairs.co/wordpress/26525/hacking/chinese-hackers-hacked-us-systems.html

At Microsoft, we have a high amount of visibility to this change. Our Microsoft Intelligent Security Graph compiles a vast array of signals from 450 billion user authentications, to 400 billion emails scanned, 18 billion Bing web pages scanned, and 1.2 billion devices updated every month.

From that data some worrying trends have emerged:

1. 100 million user identities are attacked every month, a 300% increase in identity-based attacks in the last year[6]

2. Attacks overall have increased 300% in the last year[7]

6 https://www.beckershospitalreview.com/cybersecurity/microsoft-reports-300-increase-in-cyberattacks-in-past-year-4-report-insights.html
7 https://www.gcicom.net/News-and-Events/Blog/Business-as-usual-in-a-digital-warzone---how-Microsoft-protects-its-users-from-cyber-attacks)

> "Cybersecurity is difficult, and it's not going to get any easier. Running a large environment means managing huge volumes of attempted breaches every day. This is big business. Cybersecurity Ventures estimates cybercrime will cost more than $6 trillion a year by 2021."

Ann Johnson

Corporate Vice President, Cybersecurity Solutions, Microsoft

Microsoft

The new Digital Estate

Cybercrime is a growing concern for businesses and governments worldwide. With an estimated cost of $3 trillion in economic value due to cybercrime by 2020[1], many enterprises are asking – how can we protect ourselves in this new digital era? How can we verify identities and ensure security for our customers and employees?

Why have cybersecurity threats evolved so much? The answer is simple – the way we work has evolved too. With largescale changes in today's digital world dealing with mobility, teamwork, and elsewhere, have come potential vulnerabilities. When it comes to defending against cyber-attacks we must consider – what is our new digital estate? How do we think about what our assets are and what we have to defend against?

This is vastly different today than it was five or 10 years ago. IT organizations are now responsible for protecting a set of technologies they may not own. This can be everything from the increasing trend of using user-owned mobile devices to access corporate data to the systems and devices that your partners and customers use to access your information. This vast increase in attack surfaces completely changes the security paradigm.

You no longer have control of all aspects of your digital estate which are potentially vulnerable, and any one of these points can be a point of vulnerability for your overall estate. That increased risk changes the game when it comes to security: you can no longer simply draw perimeters around your organization. Instead, you need to consider the full array of stakeholders and devices that are involved in your organization's defense. You need to understand your digital ecosystem.

How does the digital ecosystem shape our approach to digital protection?

A digital ecosystem consists of a full set of stakeholders such as attackers, regulatory agencies, end customers, partners, technology vendors, suppliers and law enforcement agencies. Together, they drive confidence in the integrity of information assets used to drive collaboration and engagements and shared across customers and businesses. Each stakeholder plays an important role in managing digital risk to this ecosystem and these stakeholders come together in a variety of ways to build a more resilient ecosystem.

The digital ecosystem

Facing this building digital resilience, today's attackers have honed their skills beyond most single organization's ability to proactively detect, thus reducing business confidence and slowing the pace of technology innovation. By harnessing the different elements of the digital ecosystem to work in concert, organizations can achieve a state of digital resilience to cybersecurity threats. In order to achieve this resilient state, we need to understand the changes happening in our digital ecosystem and in our workplace.

Intelligent Cloud and the Intelligent Edge

Today, we're all operating in a world of an intelligent cloud and intelligent edge. The digital world has evolved into a set of intelligent cloud services with copious computing power and data storage capabilities along with a set of edge devices that span everything from IoT devices, PCs, tablets, smartphones and beyond. These edge devices feature many of the same machine learning and AI powered capabilities, but less storage capacity and computing power when compared to major cloud services. Ideally, these two tiers of intelligence work together in harmony as one unified system. However even when successful, this preponderance of new devices and new sources of data drive many of the potential vulnerabilities that we must address to successfully provide security to our modern workplaces.

What are the key challenges of managing digital risk?

One of the major challenges in protecting the modern workplace is the fragmented and confusing nature of the security market. There are dozens and dozens of categories of solutions, and within each of those categories there are sometimes hundreds of solutions to choose from. Many of our customers tell us that they struggle to understand which solutions are necessary to implement in their organization.

Adding to the confusion, the modern threat landscape is continually evolving. While most companies only see a sliver of the changes that occur, Microsoft has great insights into this evolution thanks to the wide array of audiences and technologies we cover in our business. To help our customers stay informed, we publish a report every six months to provide an update on what we've seen called the Security Intelligence Report. As we look back on the last couple of years, we've observed the emergence of a few key trends.

How important is identity?

As we noted earlier, there has been a meteoric rise in identity-based attacks, up 300% this year alone. This is due to identity being the key to securing any one of those elements of the digital estate diagram we looked at earlier. You need to understand the identity of the person who is trying to access the information or the application or the device. Identity is becoming the essential control plane for security. Attackers understand that, and so they are focused heavily on stealing user credentials. Once they have a valid username and password, they can work their way toward their ultimate target: information.

The Target

Information is, after all, your most attractive target. We are no longer protecting against hackers or kids writing scripts who launch attacks for fun or notoriety. The attackers you're protecting against are typically bent on digital larceny for monetary gain, and information is most likely their target. Making matters worse, one implication of the new digital estate is that information is moving into and out of systems that IT controls. It flows out of controlled systems onto mobile devices. It is emailed to people outside the organization. It is going out to partners and customers. Therefore, your digital exposure is growing, as is the size of the target for these sophisticated criminals.

Automated attacks and tools

Another trend we see is that attackers are now heavily using automation tools and other sophisticated methods to help their attacks spread with incredible speed. This speed of attack makes it highly difficult for a human or even a team of humans to keep up. We're seeing that 96% of the malware we detect is automated polymorphic malware that changes its look and shape every time it infects a new system. This is a means of escaping traditional types of detection and is just one example of how attackers are using automation to strike quickly.

Too many attacks, too few resources

Lastly, many security operations center (SecOps) analysts are finding themselves completely swamped because they're using an average of 60 security solutions which aren't even integrated with each other. SecOps is also where many of our customers tell us they are experiencing a talent shortage. Organizations are finding it difficult to hire quality security analysts to conduct investigations and recover quickly from attacks. A stunning 60% of organizations report having a shortage of information security professionals[9] and are struggling to hire more.

9 https://iamcybersafe.org/wp-content/uploads/2017/03/WomensReport.pdf

How can we protect ourselves?

In the current world of increasing digitization and rapid technology innovation we must confront the fact that our economy cannot expect to eliminate cyber-attacks from our digital ecosystem. Large organizations spend relatively little on protecting themselves from attacks and have minimal information and insight with which to analyze the risks associated with vulnerabilities. While some organizations have dramatically reduced their cybersecurity risks by assigning significant budgets to addressing the problem and assigning ownership to CISO's, they still face an increasing tension between security and the innovation and flexibility they need.

Digital Resilience – protect your business and enable innovation

In order to ease this tension, organizations and government institutions can plan to achieve a state of digital resilience in which they understand the risks of cyber-attacks and can make business decisions where the results justify the incremental risks. If they find the risks of such attacks are manageable, rather than strategic, they do not put their brand and competitive position at risk. As innovation accelerates growth and brand value, the risk of cyber-attacks does not prevent organizations from continuing to take advantage of technology innovation.

To provide digital resilience, organizations need to build foundational capabilities integrating cybersecurity with business:

1. Prioritize assets based on business risk
2. Integrate cybersecurity into enterprise-wide risk management and compliance process
3. Incorporate "Bolt-on security" in the broader IT environment
4. Develop rapid analysis and active defense capabilities

> "IoT is growing at an astonishing velocity and creating a massive attack surface. It's moving at an incredible pace and the entire industry is now playing catch up to embed security."

Craig Hancock
CEO, CISO, Telstra
TELSTRA

Assume Breach

If we can no longer rely on traditional perimeter-based security solutions such as firewalls and proxy servers, what is next for cybersecurity? Clearly, hand in hand with the business opportunities posed by digital transformation, come risk as attackers test new innovations and use the expanding attack surface of the modern workplace to find new cracks in an organization's defenses. In the modern workplace you have to accept that a breach is going to eventually occur if one hasn't already.

With an "assume breach" mindset, organizations protect themselves in the context of a broader digital ecosystem that shapes the risk, constraints and dependencies for their business decision making.

By assuming breach, an organization can prepare their defenses accordingly; creating layers of protection, preparing breach responses, protecting important data, and fully equipping yourselves to handle the impact to your organization.

How can we overcome our cybersecurity challenges?

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.

To help cut through all the confusion and clutter, Microsoft has distilled our cybersecurity challenge into a few key strategies for success:

1. **Identity-based protection**: With identity-based attacks up 300% in the last year, this is the first strategy we recommend to every organization. This is critical starting point for a strong defense against today's attacks.

2. **Protect information – *wherever it goes:*** As documents and emails move around both inside and outside your organization, digital protection must go along with your data.

3. **Prioritize and automate detection**: As attackers adopt automation, you need to also have automation in your corner. Protection, or prevention, is still every bit as important as ever. But even the best protections can be beaten, and so you must be able to quickly detect attacks and have automatic responses prepared to react.

4. **Effective tools**: We know that IT teams need tools that work, and quickly. Time is our most precious resource and your business needs to be able to use tools that integrate the investigative experience from the end point across every surface that the attack has touched, while also providing guidance and insights to prepare for not just present but future attacks.

These four strategies form the core of where we think organizations should focus their energy and investments for security. They are the same strategies that we focus our own research and development investments on at Microsoft, with one important addition – at Microsoft, we also build for compliance.

Privacy & Compliance

With all of the cybersecurity challenges organizations are facing today, we know that the last thing you need is a regulatory challenge. That's why one of the core pillars of Microsoft's business is regulatory compliance. Unlike some organizations, we don't rely on selling customer data. Instead, all Microsoft technology is already GDPR compliant and we're committed to maintaining regulatory compliance across our technology.

Microsoft's Commitment to Security

> "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

At Microsoft, as we operate our cloud services for our customers, we consider our responsibility in an even broader context. It includes privacy, compliance, and control; both over your data and with transparency over what is happening to it. Our goal is to provide you the transparency you need to achieve your compliance needs, and the reliability that you count on for your cloud services. That reliability means not just effective tools, it means the digital protection that our customers need to keep their services running and to protect their business and customer data. Throughout this paper we will show you how we envision digital protection for our customers and how you can approach this challenge for your evolving digital estate.

We spend about a billion dollars every year on research and development for cybersecurity and digital protection. As we build our capabilities we ask ourselves - how can we at Microsoft do something that's unique, something that other parts of the ecosystem are not able to provide? What are the additional capabilities that we can layer on top of what our partners are already doing – to makeyou safer? One key area of opportunity: security intelligence.

Intelligence - The Microsoft Intelligent Security Graph

The center piece of our investment in security intelligence is the Microsoft Intelligent Security Graph. With this, we synthesize a vast amount of data from a wide variety of sources into actionable intelligence. 400 billion emails and 450 billion authentications are analyzed each month, over 18 billion Bing web pages are scanned, and 1.2 billion devices running Windows are updated. That gives us a great deal of security intelligence across multiple mediums. With this we can ask - where are the attacks, and what do they look like these days? What can we expect from attackers in the coming weeks and months?

Analytics, Artificial Intelligence (AI), and the intelligent edge

Today, the modern business landscape is increasingly ruled by data. A full 82% of businesses consider analytics crucial to their business strategy and that number is growing. Businesses benefit tremendously from the performance, flexibility, and low cost of cloud enabled analytics and AI workloads. While in the past businesses had to rely on manual data collection and spreadsheets, today's business leaders continuously gather data with every customer interaction enabling fine-tuned analytics and AI models.

What does this mean for intelligent security?

As businesses race to transform and take advantage of these opportunities to become more effective and efficient, Microsoft has built and continues to enhance a platform that looks holistically across the intelligent edge of today's cloud & mobile world. Platform investments are focused across four key solution areas– identity & access management, information protection, threat protection and security management - with a comprehensive approach that is inclusive of the technologies our customers are using.

- With **1.2 billion Windows devices** updated worldwide each month and operating the largest anti-virus and anti-malware service in the world, Microsoft is able to apply this vast store of data to analyzing vulnerabilities and potential concerns prior to addressing them with speed.

- Processing over **450 billion authentications** monthly into our cloud services make Microsoft a leader in the burgeoning identity as a service sphere, perhaps the most important challenge of the modern security environment.

- Scanning over **400 billion emails** monthly for spam and malware through Office 365 and Outlook.com enables machine learning algorithms to effectively combat phishing attacks before they happen and can help alert us when accounts are compromised.

We also value the opportunity to work with partners in the Digital Ecosystem to collectively develop security strategies and solutions that help mitigate the evolving threat landscape. We work closely with our peers, with industry alliances, and with government agencies to ensure that we are developing the best security solutions possible to protect our customer community.

Why a graph?

We built a graph because what is important is connecting these pieces of intelligence, so that these signals are not just individual points of information. The graph brings them together as something that we can draw patterns across. We can learn from one point of data to influence how we interpret another point of data, allowing us to build an integrated, intelligent security experience that helps us keep up with (and stay ahead of) attackers and attack trends as we protect our customers.

What about platform security?

The first side of platform security is the secure foundation of our cloud services. To enter a server environment an individual must pass through multiple physical layers and provide multiple forms of identification. They would also be scanned for metal in their pockets to make sure that they are not bringing devices in to steal information. On top of that physical security around our data centers, we have the built-in security tool and technologies that are part of all of our products both in and out of the cloud.

What are the different pieces of our operational security?

At Microsoft, we're committed to operational security – continuously running red vs. blue team exercises to discover potential vulnerabilities attackers might use against us. These exercises are part of our Cyber Defense Operations Center which is devoted to defending our services and IT Infrastructure. They work hand in hand with our Digital Crimes Unit to track breaches and respond quickly. We're also committed to operational security for our customers through restricted access for Microsoft employee's when investigating customer support issues, a fundamental use of multi-factor authentication, and providing the encryption and key management capabilities that customers need to protect their data.

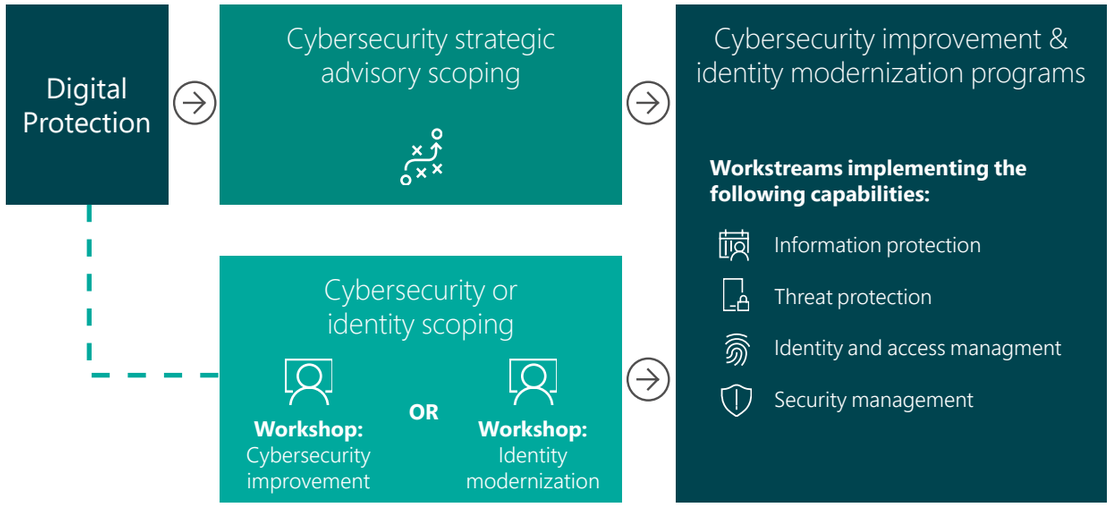
How can Microsoft Services help?

We have laid out for you how we think about security – holistically, realistically, and in depth. While this level of security can be daunting to consider, it is actually easy to get started and to incrementally add additional capabilities over time as your digital protection strategy evolves and matures. By aligning cloud and digital resilience our solutions help you:

- Protect sensitive data wherever it lives, travels or is shared
- Customize your policies and apply a range of protection options, including encryption, blocking access, applying visual markings – you are in control
- Enforce your security policies while also enabling end-user productivity by providing education and notifications to end-users to help them work in a responsible manner

We will continue to invest in enhancing our protection capabilities as well as strengthening the integration across our technologies.

Our approach for addressing your digital risks



What is Digital Protection?

Our digital protection program is a way to mitigate your risks while achieving your desired business outcomes. As we saw earlier, cybersecurity in today's workplace is evolving and growing in its challenges. However, there are ways to manage those risks.

A Digital Protection Program is the solution to managing the risks of a digital world. There are three elements to a successful Digital Protection Program— the ability to protect, detect, and respond to threats, the ability to protect data, and the ability to manage digital identities and access:

Threat Protection: Mitigating cyberattacks with modern protection, early detection, rapid response and improved controls to better keep malicious threats out of your organization.

Information Protection: Protecting business and customer data and other digital assets.

Identity & Access Management: Managing digital identities and access enables greater efficiency and innovation to be able to stay ahead of customer needs and market trends.

Let's examine each of these components in more detail.

How can you minimize and mitigate attacks?

Today's corporations operate in an environment where information breach is likely inevitable. Cybercriminals know where to go inside your network to target the highest value assets—finance, operations, and customer data. Add to that the challenge of legacy IT systems exposing businesses to attacks. Aging infrastructure also makes it difficult to expand your business, maintain relevance, and secure the business and data in compliance with regulations and market expectations. It is also difficult to create new experiences for customers without secure systems and the ability to verify that customers' identities and information are safe. When your company is better protected from external threats, you will be able to:

Minimize surprises: Mitigate the probability of downtime related to inappropriate access to sensitive data or other malicious activity.

Simplify your infrastructure: Upgrading and modernizing your infrastructure helps build strong attack defenses while simplifying their technical intricacies.

Control costs: Deliver security-promoting and resilient processes that can be scaled for varying workloads.

Secure applications: Secure agile application development practices to help reduce attack vectors.

How can we protect business and customer data?

Data is a company's most valuable asset. If financial data, blueprints and other proprietary assets were stolen, it could jeopardize the financial stability of a company. Your customers need to know that their financial, personal, and business information (like inventory lists or industrial designs) are secure as well. When business assets are protected, your company, your employees, and your customers are protected, and you can ensure you are able to:

Protect your brand: Powerful brands take decades to build but can be destroyed in hours. Keeping your company and your customer assets secure is fundamental to building and maintaining a strong brand.

Increase customer confidence: Customers make bets with companies they can trust. Being able to articulate the ways you keep their data secure is a part of your company's competitive value proposition.

Adhere to compliance guidelines: Discover, protect, manage, and report on personal customer information per regulatory requirements like GDPR.

How can you manage digital identities and access?

You need to know that access to your business and your customers' data are not compromised by the digital access policies and technologies you have in place. And, your company needs to be able to innovate faster than the speed of the market with a modernized identity platform. When digital identities and access are well-managed, you will be able to:

Accelerate innovation and business growth: Deliver the applications and information employees need with a consistent, secure experience across devices.

Ensure employees can work where they are: Enable rich collaboration and allow access to data anywhere and anytime for a secure mobile workforce.

Reduce complexity and increase agility: With more self-service options, employees can be more agile and productive.

Balance control and access: Maximize employee productivity while ensuring secure and appropriate access to data and organizational resources with unified identities for all applications, self service capabilities, and/or conditional access.

Cybersecurity Advisory Service

Our Digital Protection program provides an end to end view on customers' cybersecurity and identity posture by identifying the threat landscape and helping to prioritize the highest risks. Getting to the state of a fully secure and modern enterprise is a journey that requires time as well as expertise. A partnership with Microsoft Services can guide your enterprise along this journey to protect your enterprise against evolving cybersecurity threats, securely move to the cloud and keep data safe. Our Cybersecurity Strategic Advisor – whether as a standalone engagement or a complimentary component of a larger security investment from Microsoft – is designed to assess your enterprise's overall security posture and guide you along a roadmap that will build a resilient foundation with the goal of preparing your business for today's security realities.

Cybersecurity Advisory Services provide professional consulting services to assist customers in better understanding and prioritizing the security challenges that face their organization. The Cybersecurity Strategic Advisor is designed to help align security investments and resources to today's modern security threats and business objectives while building a resilient foundation preparing your business for today's security realities. This personalized engagement results in the creation of a roadmap that is customized to a customer's business. This roadmap accounts for the organization's resources and tolerance for change at the right time. This is a proactive service based on Microsoft recommended practices and field experience that will:

- Identify the threat landscape and help prioritize the digital risks of the business
- Understand modern and advanced threats and recommend protections for your enterprise
- Enterprise-level assessments of security people, processes and technologies
- Development and assistance with a prioritized cybersecurity roadmap

Cybersecurity Improvement Program

This program helps enterprise organizations protect their business from cyber threats. Using a structured and interactive dialog, we will help you assess your organization's current Cybersecurity posture and identify gaps which would limit your ability to withstand cybersecurity threats. We believe the goal for threat protection should be:

- Enabling organizations to have the ability to protect themselves from advanced cyber-attacks, including protecting their information in the event of a breach.
- Providing organizations with solutions which 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 which enable damage control and limit the effects from an attack.

PROTECT
organizations from advanced cyber attacks

DETECT
malicious activities

RESPOND
to threats quickly

Identity Modernization Program

Our Identity Modernization Program assists IT organizations in meeting the increasing identity-based demands required to support a digital enabled business. Identity Modernization provides enterprise customers with a proven holistic security methodology to achieve a modern (Hybrid & Cloud) identity and access management platform. We believe the goal for identity modernization should be:

- Modernizing identity environments to take advantage of the latest security & identity capabilities
- Optimizing management and secure identities across datacenter and cloud
- Enabling business without borders across datacenter and cloud

MODERNIZE
identity environments to take advantage of the latest security & identity capabilities

OPTIMIZE
management and secure identities across datacenter and cloud

ENABLE
business without borders across datacenter and cloud

Recommended Solutions

Our recommended solutions to solving the challenge of Digital Protection:

Modern Identity Foundation

At Microsoft, we recognize that no organization's modern workplace transformation is complete without a secure identity for employees. As employees move from device to device, you need to be able to verify identity and simply manage access. Using multi factor authentication or other IAM solutions, we can secure your employee's digital identity and ensure users are authenticated to use applications and gain access to data. We can manage user identity and associated access privileges through solutions such as:

- Conditional access
- User and sign-in risk calculation
- Multi-factor authentication
- Privileged identity management

We can help you verify user's identity before you let them access your resources. Together with our experts we can develop a strategic plan of action to achieve your modernization objectives safely and effectively.

Information Protection

Our Microsoft Services experts deliver our Information Protection solution to help you detect, classify, protect, and monitor your data on-premises and in hybrid and cloud-only environments. Based on your requirements, our solution enables the following capabilities:

- 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

Cybersecurity Essentials

Our Cybersecurity Essentials solution is delivered by Microsoft Services experts who help you assess your cyber risk exposure and help create a roadmap to improve your security posture; protect your identity platform from advanced cyber-attacks; secure privileged access from advanced cyber-attacks; and detect investigate and respond to suspicious activity and advanced threats.

- Assess your cyber risk exposure and create an improvement roadmap
- Protect your identity platform from advanced cyber-attacks
- Secure privileged access from advanced cyber-attacks
- Detect, investigate and Respond to suspicious activity

Modern Workplace Security Essentials

Microsoft cloud services are built on a foundation of security, privacy, control, compliance, and transparency that can provide you with security controls and capabilities to help you protect your data and applications. Meanwhile, your organization owns your data, devices, and identities, as well as the responsibility for protecting them. When considering adopting cloud services, it is important to have a clear understanding of all security features available to you and to implement a successful approach in planning how, or if, these features meet your goals and objectives. To facilitate this, Microsoft Services has created a unique approach to help you bridge these responsibilities and develop and implement a comprehensive strategy to meet your security objectives.

Governance & Compliance

Microsoft Services experts work with you to develop prescriptive governance and compliance solutions specific to your intended use of the platform. The engagement covers both technical and operational governance topics and produces governance directives that will facilitate controlling and administering. Microsoft is fully GDPR compliant and committed to not just staying up to date and compliant, but also protecting your data from potential threats. We provide superior data governance tools to enable simple and effective recordkeeping and reporting, while allowing for better internal transparency. A strong data governance strategy will prepare your business as customers demand more security around the storage and use of their data, and as employees demand that the security perimeter extends beyond the corporate realm
and onto mobile devices.

Why Microsoft Services?

Unlike some companies, we tailor our approach for each company – providing guidance and expertise in the areas that are most important to your company. With Microsoft Services as your partner, you'll have full access to our expertise in the Microsoft portfolio and our capabilities as well as those of our global network of professionals and partners. We are accountable for our solutions for the long term. We are flexible, working for you, and 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.

Conclusion

Microsoft Services experts are on the leading edge of technology trends, providing thought-leadership to help you develop innovative solutions for your business. Trusted by the world's largest organizations, our highly trained experts integrate decades of industry learnings, understanding of geographic constraints, and depth of knowledge of your organizations business needs to deliver exceptional service. Microsoft Services digital advisors, architects, engineers, consultants, and support professionals help you implement and adopt Microsoft products, services, software, and devices to solve, envision, and understand new possibilities for your business.

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 your data is kept secure and private.

Microsoft Services can help get you started on your modernization 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
- Develop prescriptive governance and compliance solutions specific to your intended use of the platform
- Secure platforms for seamless collaboration

We invite you to begin your journey to a more secure workplace by scheduling a discovery workshop with us. This one-day workshop is designed to determine your security and identity posture and identify a prioritized list of security/identity initiatives to bridge any gaps.

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 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, Cybersecurity & Identity Solutions Strategy, Microsoft Services

Gary Versters

Director BPM Mgmt Svcs, Microsoft Services

Contributors

Hani Adhami
Architect ID & SEC, Microsoft Services

Ian Ruthven
Assc. Architect, Microsoft Services

Amy McCullough
Director, Solution Area Marketing, Microsoft Services

Conor Bronsdon
Consultant, Olive & Goose

Hannah Rames
Consultant, Olive & Goose

Kurt Frampton
Sr. Designer, Simplicity Consulting

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

Imagine.
Realize.
Experience.

microsoft.com/services