Identity – building trust in a digital world

Microsoft

Empowering business
for what's next

Table of contents

Today's digital workforce

In a world of anonymous online interactions and remote access to everything from your home's doorbell to business apps, identity is more important than ever.

Every Morning, some workers start their day by opening their favorite ridesharing app on their mobile device, finding a stranger to ride to a shared office space with, and remotely communicating over email and Skype with their co-workers; some of whom they've never met in person. On their lunch break, they set up an appointment for another stranger to come walk their dog, again through an app, and they leave for a client meeting where they will share some internal business data through a PowerPoint, after logging into an on site device, or using their own laptop to log onto a previously unknown WiFi network in order to stream the presentation to a projector.

Throughout the day, their personal data and the data on their devices has been exposed to unmanaged networks in a variety of ways, all while they access critical business data for their work on those same devices. This scenario is not atypical. By 2020 72.3% of the US workforce is expected to be mobile workers[1], giving access to business-critical data on ever expanding swathe of off premises devices. You need to ask yourself – with this massively expanded defense perimeter for your business, how can you keep your business and its data safe while enabling the modern digital infrastructure that will allow your business to thrive?

1 https://msenterprise.global.ssl.fastly.net/wordpress/2018/01/Microsoft-Envision-your-modern-workplace.pdf

The modern transformation

It probably isn't a big surprise that technology is the top priority for many CEOs.

These digital transformations require leaders to examine existing business models, re-envision them, and embrace new ways of bringing together people, process, and data to create value for their customers. Central to these transformations, is identity. Without identity, having secure access through the cloud is impossible, and it is our IT organizations that must handle the pressures of this transformation, facing evolving security threats while they manage the risks of transformation to enable employee productivity regardless of what device they use.

DATA POINT

Of the 460 CEOs Gartner surveyed in its 2018 CEO survey, 62 percent said they have digital initiatives or transformation programs in progress.[2]

2 https://www.gartner.com/newsroom/id/3873663

The security challenge of the modern transformation

If the answer to how you can protect your business lies in a reimagining of security through identity, its important that we consider how cybersecurity today is changing. Traditional security and cybersecurity measures have often relied on defensive perimeters, but in the digital era you need to rethink your strategy to address the evolving way we work and access data. Today, identity is the most important control plane for modern security. The problem is, attackers have already recognized this fact.

Attackers are after identity

At Microsoft, we collect a large amount of telemetry data through our Microsoft Intelligent Security Graph. The 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[3]
2. Attacks overall have increased 300% in the last year[4]

DATA POINT

A 300% increase in identity-based attacks in the last year.

3 https://www.beckershospitalreview.com/cybersecurity/microsoft-reports-300-increase-in-cyberattacks-in-past-year-4-report-insights.html

4 https://www.gcicom.net/News-and-Events/Blog/Business-as-usual-in-a-digital-warzone---how-Microsoft-protects-its-users-from-cyber-attacks

> "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

Why is identity the key to modern security?

Attackers are already signaling that they view identity as crucial to modern security, concentrating their attacks on this important control plane as identity-based attacks lead the 300% overall increase in attacks experienced over the last year. This attack concentration is due to the changing shape of the modern workplace, with identity playing such a vital role in every cloud IT environment, cyber-attacks against identities will only continue to increase in their sophistication and persistence.

Why is cloud migration, and hence identity, so important?

With the proliferation of Software as a Service (SaaS) applications, organizations are being offered a range of innovate technologies capable of enhancing productivity and empower employees in a range of ways. However, the growth of these innovative new technology opportunities also means that the separation between high performing and low performing organizations is separating. Businesses know they need to provide flexibility and grow their digital agility while maintaining control of digital assets; modern identity is the facilitator of all of this by providing a secure, trusted form of access management.

Modernization can help your business and failing to modernize can be fatal for it. However, modernizing and digitizing your business is challenging – cloud based solutions require a consistent and manageable identity solution that meets the requirements of end users and of corporate IT while maintaining digital agility. Without finding ways to span on premises and cloud environments, the transition to the cloud is incredibly challenging, and hybrid cloud environments are nearly impossible without secure identity modernization.

As businesses strive to innovate and outpace their competitors, the pace of digital transformations is accelerating:

- The IDC forecasts that the percentage of enterprises creating advanced digital transformation initiatives will more than double by 2020, from 22% today to almost 50%.

- Gartner says that 125,000 large organizations are launching digital business initiatives now and that CEOs expect their digital revenue to increase by more than 80% by 2020.[5]

5 https://www.forbes.com/sites/gilpress/2015/12/06/6-predictions-about-the-future-of-digital-transformation/#7dc593541102

Identity is the key to digital transformation

As we use an increasing number of devices to log in and access data, the simple expediencies of seeing an individual log into their device on premises, and of building a security perimeter around your on-premise devices, are no longer viable. Industry leaders from all verticals are digitising essential functions within enterprise to improve competitiveness, gain efficiency or provide better services to customers. These cloud enabled digital transformations all create more opportunity for workers to work remotely from their laptops, smartphones, tablets, and other devices.

When we enable a modern enterprise with the digital tools and agility needed to work from anywhere, anytime, we need to have a single identity for each employee. This creates an environment where trusted identity is crucial to successful digital transformation, and where a simple and secure sign in process is essential.

DATA POINT

90% of CIOs report that upgrading or simplifying user experience is a key concern [6]

You need to ask yourself:

- Has my business successfully developed trust in our digital transformation?
- Are we prepared for the new security challenges posed by digital transformation?
- How can we protect and use identity in our digital transformation?
- How can we provide security while ensuring a painless user sign in experience?

6 https://info.microsoft.com/rs/157-GQE-382/images/EN-CNTNT-eBook-CIOsGuideToAADP.PDF

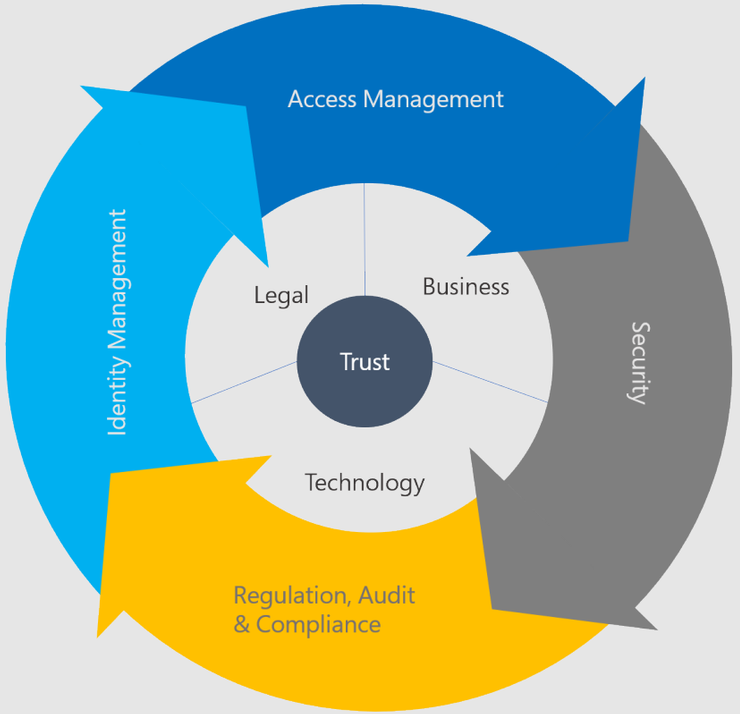
Identity – building trust in the digital world

As industries worldwide have started to digitize, from automated manufacturing to mobile banking platforms, the identity platform that supports these functions has been facing increasing challenges verifying who you say you are and what level of access you are authorized for. Due to this strain, attackers are increasingly targeting this potential vulnerability, as previously shown. Therefore, it is essential that any digital identity platform be secure, usable and trusted. This applies to everything from using blockchain for social security purposes, to long standing financial institutions.

As we expand digital ecosystems and continue to use increasing amounts of data, new trust issues around security and identity are being raised. As we add more touchpoints where data is collected and exchanged, it also means more potential points of entry and an increasing attack surface for attackers. Your entire business depends on the ability of users' to access the services they need in a secure and trustworthy way. If you lose the trust of your customers, or if those services aren't available when customers need them, the consequences are severe. Its due to this that verification has become essential – all data and sign ins need to be treated with scepticism. Trust must be built through verification.

Only when all elements involved can trust in the security of data and communication as well as the protection of their intellectual property, can digital enterprises function properly. Developing this trusted relationship will enable different elements to interact via secure identities. It is through this that trust and identity form the cornerstone of successful digital transformation. Without identity modernization and verification, it is nearly impossible to establish the trust necessary for different aspects of the digital enterprise to function properly together. Without trusted and secure identity the vision of remote, empowered and efficient workers will not come to fruition.

What are the key dimensions of establishing trust in the digital age?



Identity Management

The first key to developing trust in the digital age is identity management. This requires defining how users are provisioned and authorized to access systems and includes their roles as derived from within a role management system. This role management system generally rolls into access management. Another important feature of identity management is to identify which user information will be shared, and how often it will be updated.

Security

In order to establish trust, you must secure identity and protect crucial information. This means defining encryption requirements, and also creating a federated agreement with defined standards and protocols.

Access Management

Another essential piece of trust establishment is managing access. If you have a secure system with defined and established identity but access isn't managed – what would be the point? Instead, there needs to be a form of authentication that spans organizations. This allows partner companies to determine user access permissions based on role or other considerations. This kind of system will work, but it is essential to schedule periodic access reviews to get rid of old credentials, check for errors, and update roles as needed. With the increasing proliferation of devices and users in an organization, there needs to be a central means of managing and storing information about users and their access.

Regulation, Audit and Compliance

Regulatory and compliance needs can vary from industry to industry. It is therefore important to identify privacy requirements and regulations that are applicable to different industries. Compliance audits should check both that regulatory requirements are being fulfilled, but that negotiated policies, service level agreements, etc. are being followed by each party.

Consider the following:

- How do you assess existing identity and access environments at your organization?
- How do you begin the process of modernizing your existing identity environment or building a new one?
- How do you enable your identity and access management to take advantage of cloud-based identity solutions?

How is identity strategy changing?

DATA POINT

More than 80% of hacks and cyber-attacks were traced back to lost, weak or compromised user credentials [7]

Traditionally, identity has been approached through passwords. Multiple character sets, expiring passwords, long character requirements – all typical. Ironically these recommendations have often resulted in weaker passwords over time as user result to predictability to remember their logins. In the modern workplace, new solutions have been developed to protect our user credentials and the crucial information that lies behind them. With conditional access policies we can control users' access based on group membership, the device platform, device state, and device location. This enables evaluation of location and risk level to impact data access, allowing us to limit potential breaches from compromised user credentials. Multi factor authentication, Windows Hello provides strong authentication using biometric security such as face and fingerprint recognition, and Windows Defender Credential Guard protects sign-in tokens and identities against pass the hash, pass the ticket, and domain password theft by isolating credentials away from the operating system using virtualization-based security. With these and other tools, plus the $1 billion we at Microsoft invest annually in security research, we've formed an industry leading approach to addressing identity modernization.

> "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."

Anne Johnson
Vice President Strategic, Enterprise and Cybersecurity at Microsoft

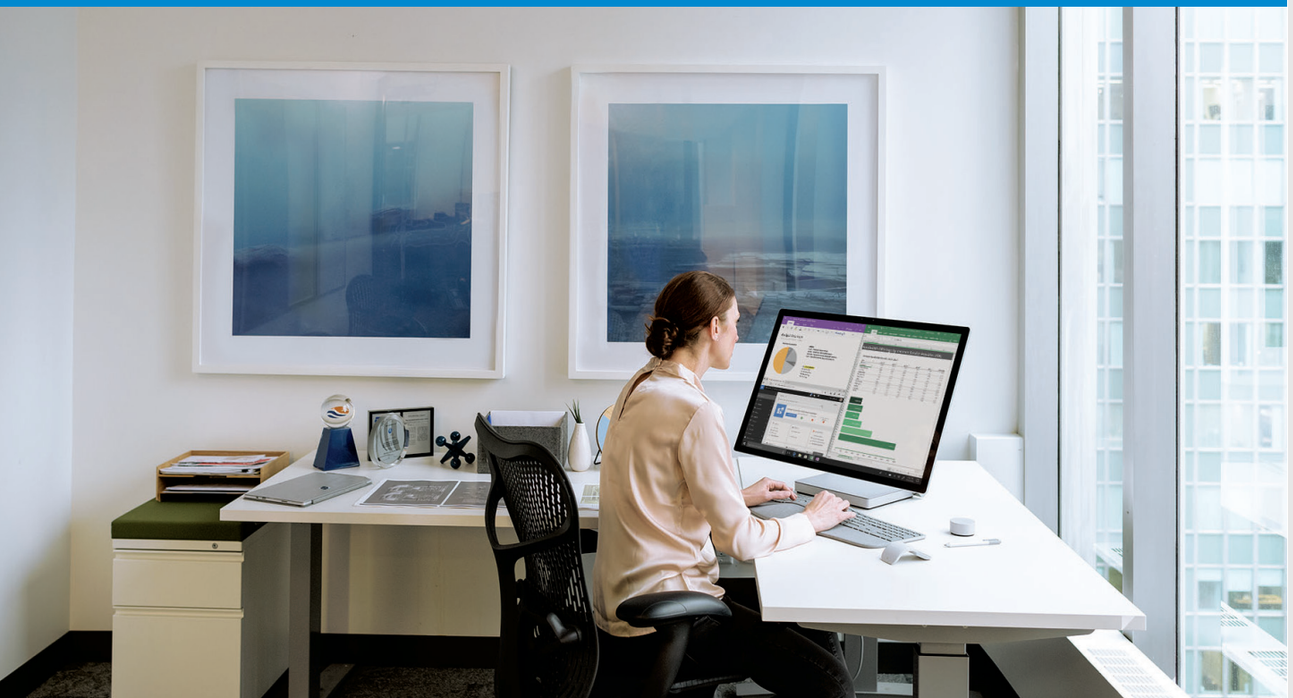
Microsoft

7 Verizon 2017 Data Breach Report

How can we develop digital identity?

As we have outlined, traditional security perimeters fail to provide adequate protection in the modern workplace. Today's security strategy needs a central strong point – identity as the control plane and new perimeter which attackers must overcome. This is how identity becomes the trust boundary, it controls how users access applications and information and from which device. A strongly protected single identity is the core of successful security measures for the modern workplace and having a successful identity and access strategy is crucial to maintain trust while enabling productivity in your organization.

However, we face significant challenges in establishing a single identity across industries. This would mitigate identity fraud, provide trusted customer experiences, and lower the cost to serve. One option is a digital identity developed through governments, which may potentially bridge the gap between the physical and digital interactions. From the Sweden BankID, to Estonia's DigitalID, trusted institutions across the world are working to solve the challenge of sole identity, recognizing that in our increasingly digital world, trust is the cornerstone of our society. While there is no single solution that addresses identity challenges successfully across industries, progress on tackling identity challenges can be made through the creation of a framework that delivers tangible benefits to the users.



Among the fundamental challenges to achieving trusted single identity are:

- **Ubiquity** – customers currently use a multitude of various identity credentials, a single trusted source of truth is required to establish a single trusted individual credential
- **Management platform** – secure identity management platform to streamline the identity management processes
- **Acceptance** – acceptance can be the main challenge which can be addressed through explicit government mandate or exceptional customer experience and widespread acceptance across private and public providers

> "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

The Microsoft Approach to Identity

Microsoft's end-to-end Identity Solutions are designed to meet your company's access management needs while supporting your security standards. Microsoft Services can clean up your existing identity situation, help you enable cloud, and help you move towards a centralized identity provider—all while helping you improve your security.

Microsoft's approach to the security challenge

As we approach security challenges, we've broken down our thinking on the topic into four key pillars that we see shaping modern security:

Holistic
Addresses security challenges across users (identities), devices, data, apps, and platforms—on-premises and in the cloud.

Innovative
Protects your data from new and changing cybersecurity attacks.

Intelligent
Enhances threat and anomaly detection with the Microsoft Intelligent Security Graph driven by a vast amount of datasets and machine learning in the cloud.

Identity-driven
Offers one protected common identity for secure access to all corporate resources, on-premises and in the cloud, with risk-based conditional access.

> "Customers that turned on Microsoft's risk policies have reduced their compromise rates from Identity-based attacks by 96%.[8]"

Joy Chik

Vice President, Identity Division in Microsoft's Cloud + Enterprise group

Microsoft

What enables a well-formed identity?

With the knowledge that identity is at the core of our security vision, it is integral to our security solutions that we build an identity solution framework; it is the key to a productive and secure environment. As we have built our technology, and as we tailor our approach in each engagement, there are several key areas we consider how to address:

- **Improving Access Control**: Implementing a Microsoft Identity Solution will give you more options and control in defining your access requirements.
- **Empowering Users**: These solutions are designed to enable users with anywhere, anytime access, across devices, and allow the sharing of information to occur as users' roles dictate.
- **Managing Costs**: Provide scalable access management across your organization, and centralize identity stores to reduce the costs of administration.
- **Planning for the Future**: Microsoft's solution can help you clean up your identity situation for a mobile workforce and potential cloud integration.
- **Improving Security**: Augment your existing security with a well-defined and integrated identity solution to improve your security processes and practices.

8 Ignite 2018: Microsoft security: How the cloud helps us all be more secure

The 4 Pillars of Identity

When modernizing identity at an organization, we need to build a framework that maps to the objectives we just outlined. As we've learned on this topic and developed, Microsoft has broken identity as a topic down into 4 key elements, or pillars that form the backbone for our Identity Modernization strategy:

Administration: comprises both entitlement and identity administration covering groups, policies, and roles as well as identities, attributes, and credentials.

Authentication: utilizes identity data from Administration to verify transactions, authenticate users, and provide a seamless single sign-on experience.

Authorization: takes the authorized (trusted) identities and the identity and entitlement data from administration and applies access policies to provide real time entitlement resolution and authorization decisions.

Analytics (and Intelligence): interact with Authorization, Authentication, and Administration to continually track who did what, when they did it, and how they obtained access (who granted it).

Administration

The administration pillar surrounds how identity objects are managed, whether manually or automated, over the lifetime of the identities' existence. Administration provides a system which is highly configurable based on and around business processes, as well as the agility to scale resources according to demand. By carefully distributing and automating management, we can provide cost savings as well as the flexibility to change proliferation, control, and synchronization when needed.

Authentication

This pillar is about validating if the user is who they proclaim to be, while providing an appropriate level of validation and security throughout the authentication transaction. Utilizing authentication we enable the integration of disparate sources, applications and protocols by providing a standard. When authenticating we can deploy many different industry standard methods of validation and assurance to provide a flexible, standards compliant authentication that integrates across the organization

Authorization

The Authorization pillar covers what an identity can access and what are they allowed to do once they gain access. Identity authorization provides the ability to manage policy control and use extensive methods of assigning entitlement in order to increase security and cut administrative requirements. This process also makes enforcement simple by standardizing based on a common approach.

Analytics (and Intelligence)

Analytics gathers and applies the data from Administration, Authentication, and Authorization:

- From Administration: identity and entitlement data
- From Authentication: authentication activity data
- From Authorization: access activity data

Analytics takes all of these inputs and applies contextual data to build intelligence that helps guide decision making for Identity and Access Management (IAM), security, risk management, and more. By auditing identity through intelligent analytics, we can be both proactive and reactive based on the telemetry we collect. Automated reports and alerts can identity problems quickly when they occur and enforce policies. Through the collation, centralization and governance of audit data from disparate enterprise resources we are able to apply machine learning based analytics to find trends and identity potential threats. Through proper data analysis we can ensure proper authorizations, historical accuracy, and compliance as well as provide opportunities for improvement.

Identity Modernization Program

Our Identity Modernization Program builds on the 4 pillars of Identity to assist 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 datacenters and cloud
- Enabling business without borders across datacenters and cloud

MODERNIZE
identity environments to enable the latest security & identity capabilities

OPTIMIZE
management and secure identities across datacenter and cloud

ENABLE
business without borders across datacenter and cloud

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 – with Azure Active Directory identities users can seamlessly move from device to device or across SaaS applications. Using multi factor authentication or other IAM solutions, we can secure your employee's digital identity and ensure users are authenticated before using applications and or gaining 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.

> "If you configure your users with Multi factor authentication (MFA), that reduces the risk (of attack) by 99.9%. Unfortunately a surprising number of customers haven't turned on MFA- its like driving without a seatbelt."[9]

Joy Chik
Vice President, Identity Division in Microsoft's Cloud + Enterprise group
Microsoft

9 Ignite 2018: Microsoft security: How the cloud helps us all be more secure

How does Microsoft make access simple and secure?

> "Some employees could spend half an hour a day connecting to VPNs and signing in, and that doesn't capture forgotten passwords or support calls. We're using Azure AD to give each one of our 20,000 employees one identity and one password."[10]

Chris Suozzi
Executive Director, Active Directory/Messaging/IDM,
Hearst Communications
HEARST

While many employees fear that identity and security solutions will create burdensome user experiences, Microsoft is intent on proving the opposite. Yes, everything needs to be verified when a user signs on; identity and access management protections form the 1st bulwark of your security, however much of this verification process can happen in the background. Azure Active Directory Conditional Access keeps the sign in process frictionless by applying machine learning and AI powered analytics to evaluate real time risk based on factors such as application access, user and location, device, and other factors.

While most identity solutions bear onerous requirements, Microsoft's approach is uniquely frictionless for users while using our unique intelligent capabilities to prevent attacks before they happen. Meanwhile, your IT team can use the Azure Active Directory Identity Governance capabilities to easily and securely manage your corporate resources from the day an employee or partner starts, to the day they leave. Microsoft ensures security and compliance needs are met while providing boundaryless end to end solutions across users, devices, applications, and data.

10 https://customers.microsoft.com/en-US/story/hearst-media-and-cable-enterprise-mobility-and-security

The next step - Secure and trusted identity through a password less future

Microsoft is already hard at work building the future of identity. That future is now with the announcement of the public preview of the Azure Active Directory password-less login via the Microsoft Authenticator App. This new technology will allow users to take something they have (their mobile device) and something they are (their fingerprint) and sign in to any workstation through the Microsoft Authenticator App. Instead of running the risk of stolen passwords, Microsoft is ready to empower companies and individuals to be even more secure and productive.

> "Over 82% of breaches are caused by stolen passwords- that's why we're making passwordless access a reality.[11]"

Joy Chik
Vice President, Identity Division in Microsoft's Cloud + Enterprise group

Microsoft

11 Ignite 2018: Microsoft security: How the cloud helps us all be more secure

What's next?

Microsoft Services experts are on the leading edge of technology trends, providing thought-leadership to help you develop innovative solutions for your business. We recognize the importance of identity as the new control plane for modern security, and we've developed the solutions needed for identity modernizations. 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.

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.

We invite you to begin your journey to a secure trusted identity 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. We'll help guide your strategic decisions based on your identity capabilities and identity how Microsoft can assist you to achieve your business goals.

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.

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 Services

Andreas Wasita

Architect, Microsoft Services

Ian Ruthven

Portfolio Architect, Microsoft Services

Contributors

Conor Bronsdon
Consultant,
Olive & Goose

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

Imagine.
Realize.
Experience.

microsoft.com/services