04

Microsoft Services

Transform your digital security strategy to mitigate business risk

Technology is omnipresent, and this access to digital services is playing an increasing role in everything we do – shaping growth, disrupting industry landscapes and providing the catalyst for new business models, products, services and experiences for businesses to transform themselves.

Capitalizing on this phenomenon is the key to innovation and growth.

From the rise of connected devices and other "things" within the Internet of Things (IoT), the growing mounds of data, and the emergence of advanced analytics, machine learning and artificial intelligence, to augmented reality and the next frontiers, the challenge and opportunity for business leaders is to harness the ubiquitous, disruptive force of technology to be more agile, fuel efficiency and ultimately shape their destiny.

Naturally, this comes while navigating the expectations of a changing workforce, addressing evolving security threats and managing a host of other challenges.

Digital is changing how business gets done

Forces at work driving change

CYBERATTACKS ARE INCREASING

$4M

THE AVERAGE COST OF A DATA BREACH TO A COMPANY

4149 BREACHES IN 2016 EXPOSED

4.2B

RECORDS, 3.2B MORE RECORDS THAN PREVIOUS YEAR

FRAGMENTED IDENTITIES INCREASE OPERATIONAL RISK

63%

OF CONFIRMED DATA BREACHES INVOLVED WEAK, DEFAULT OR STOLEN PASSWORDS

Accelerating innovation and business growth is a key driver and addressing how that move will happen is critical.

Minimizing surprises and ensuring critical systems aren't slowed or interrupted in any way.

Deepening the relationship with your customers by protecting company assets and your brand,

Adhering to regulations, and increasing customer confidence, while controlling costs.

When breaches occur, operations and finance are the functions most likely to be affected – 36% and 30%, respectively – followed by brand reputation and customer retention, both at 26%.

MacAfee estimates the cost to the global economy of these breaches is as high as $575 billion every year, and $8 trillion projected cost of cybercrime to the global economy by 2022.

Sources:

https://app.clickdimensions.com/blob/softchoicecom-anjf0/files/ponemon.pdf

Risk Based Security Report

Security Week news

http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf

http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

Juniper Research and whitepaper

> “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*

Imagine if...

you could proactively identify and reduce security risks, mitigate damage, and respond more effectively to threats and attacks.

Mitigating business risk

FROM

We have a diverse set of technologies and find it difficult to understand our current operating state.

We don't know enough about our vulnerabilities, or details of how our processes, employees, and technology contribute to risk.

When news of an emerging threat breaks it takes a lot of effort to identify what parts of our networks or applications are at risk.

We have little ability to identify if we've been targeted by hackers, when it's happening, or how to defend against it.

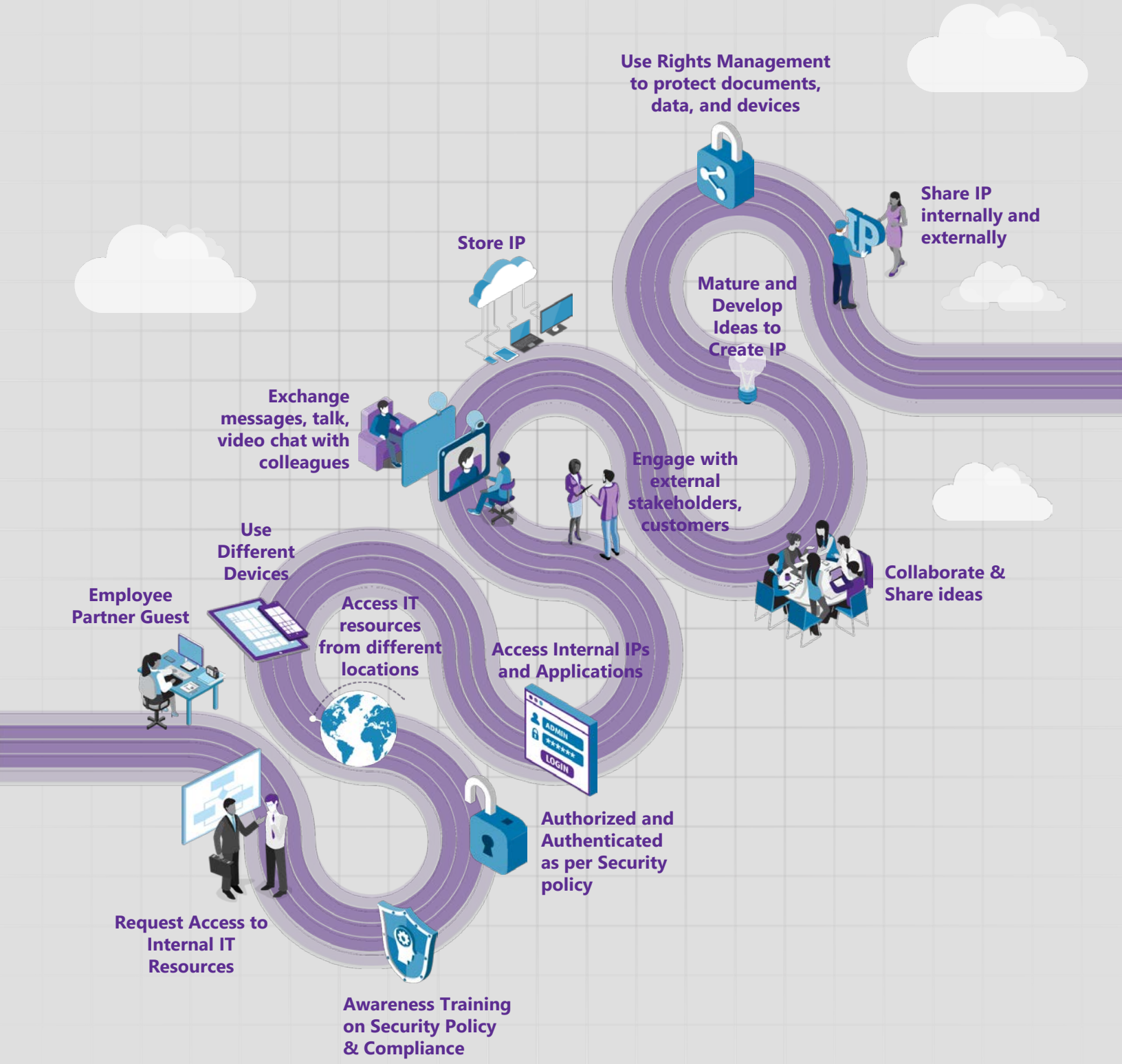
TO

We proactively mitigate cyberattacks with fast detection and response and improved controls to better keep malicious threats out of our networks.

We protect business data and other digital assets, especially our customer data.

We manage digital access to enable greater efficiency and innovation to be able to stay ahead of customer needs and market trends.

Employee Experience Journey



Managing digital security to protect the employee experience

EMPOWERED WORKFORCE

Employees working differently in different contexts

On the Go

On-Premises

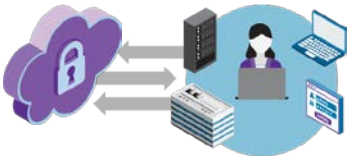
At Remote sites

Different Devices

With a Customer

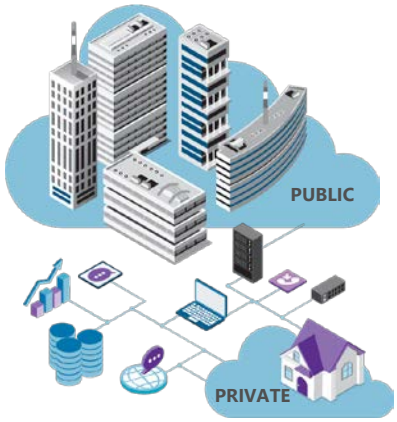
Secured anytime, anywhere, any device access

Identity & Access Management



Secured Infrastructure

Enabled employees



Connected, Collaborative, Efficient and Productive Workforce

TOP-LINE IMPACT

Connected, collaborative, efficient and productive workforce driving innovation and generating new revenue streams and strengthening existing customer relations

BENEFITS	START
Security Operations cost reduction Protect Revenue: Existing Customers Reduce IT operations costs: IT efficiencies Increase Employee Utilization: Mobility	Evaluate and redesign authentication policy to enforce single sign on for all applications and data entry points Define IT policies and controls based on external and internal requirements Encourage employees to use devices of their choice and implement device management policy and supporting architecture

STOP	CONTINUE
Preventing new work patterns due to lack of support for mobility, social features, big data, and cloud computing Detecting threats too late, responding slowly, and recovering inefficiently	Perform regular security audits and regulatory checks, to check whether security policy is compliant or not Develop and manage social media channels Develop and manage promotional activities

Minimize and mitigate attacks

Today's corporations operate in an environment where information breach is almost 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 business 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, access to sensitive data, or other malicious activity.

Simplify your infrastructure
Upgrade and modernize your infrastructure helps build strong attack defenses. Modernize your critical legacy systems while securing and 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.

"Organizations need information to quickly and accurately provide insights, prioritize and make decisions, whilst proactively manage information in a secure and effective way. The challenge is balancing both aspects of agility and security. Finding the right balance is vital for survival in digital age.

Tuan Jean (TJ) Tee
Chief Digital Advisor, Australia New Zealand

"Every employee is responsible for corporate cyber security, not just the IT security team.

Xiang Li
Digital Advisor, China

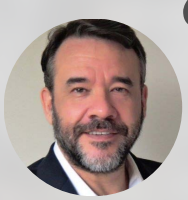
Protect business data

Data is a company's most valuable asset. If financial data, blueprints and other proprietary assets, or operational processes were stolen, it could jeopardize the financial stability of a company. Additionally, customers need to know their financial, personal, and business information (like inventory lists or industrial designs) are secure. 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/or 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 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 the General Data Protection Regulation (GDPR).



"Governance becomes a big topic. Every organization has to follow policy and procedure to comply with regulations. This puts an intimidation factor on the table. The Chief Information Security Officer's mission would be to eliminate the fear factor so as to help accelerate the digital journey.

Ian Webster
Senior Digital Advisor, Latin America

"One of the key differences a Chief Information Security Officer can make is to modernize the organization's security vision by aligning it with people and infrastructure. Don't mix technology with policy, and don't start with technology to minimize digital risk.

Steve Latropoulos
Technology Strategist, Australia New Zealand

Manage digital identities and access

You need to know that access to your business and your customers' data is 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 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.

"New ways of working safely, securely and collaboratively will likely require a cultural change to drive new behaviors and habits in daily working practices for many organizations. Executive and business sponsors need to endorse this change, help build champion networks to be advocates and support on the ground. Invest in communication and training that will enable employees to see clearly the benefits of this new world, and have the confidence to work with both agility and security.

Sophie Allen
Behavioural Architect,
Adoption and Change Management Global Domain
UK

"As employees bring their personal devices to work and adopt readily available applications, maintaining control over their applications across corporate datacenters and public cloud platforms has become a significant challenge. The ability to proactively monitor suspicious activity through advanced security reporting, auditing and alerting helps mitigate potential security issues.

Kim Schulze
Chief Digital Advisor,
South Africa, Microsoft

Security management

In today's connected, technology-driven world, where digital transformation is the only way to survive for any organization, an efficient security management practice becomes the cornerstone of any long term strategy of the Chief Information Security Officer, regardless of their industry. An effective security management solution should provide 3 key tenets:

Visibility
Understand the security state and risks across resources.

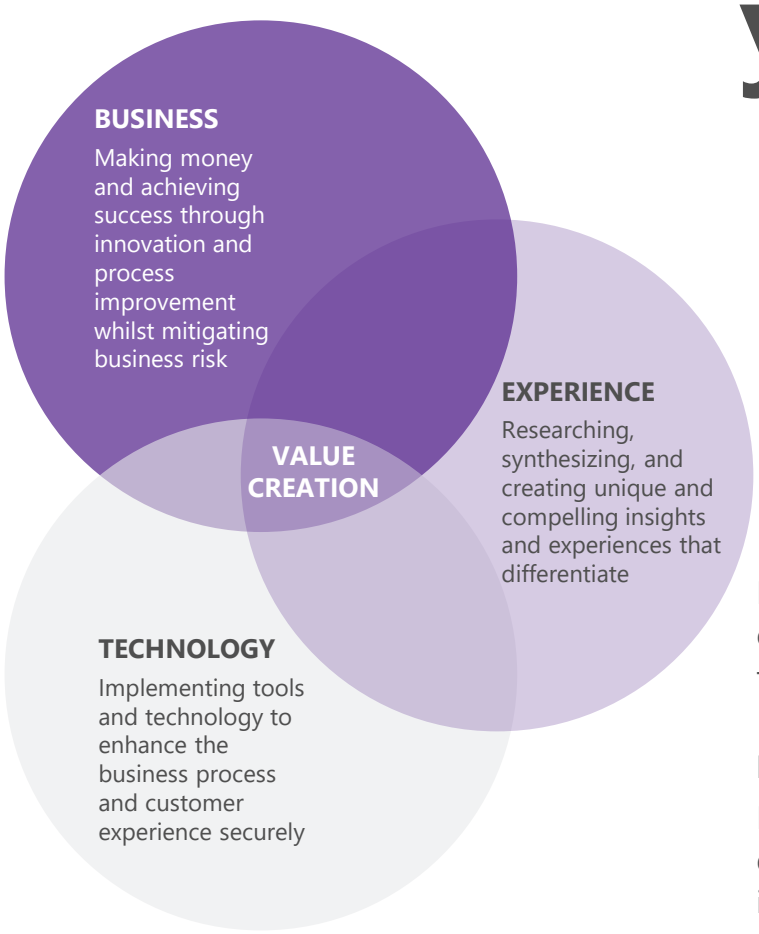
Controls
Built-in security controls to help you define consistent security policies.

Guidance
Effective guidance to help elevate your security through actionable intelligence and recommendations.

> "Organizations need to take a more holistic and innovative approach to managing security, one that can protect, detect, and respond to threats of all kinds in their digital transformation. Addressing the security challenges of today and tomorrow across users, devices, apps, data, and platforms through a single protected common identity for secure, risk-based conditional access to thousands of apps on premise and in the cloud.

Professor Chris Peiris
Director of Cyber Security, Australia New Zealand

Designing your digital protection strategy



Optimal impact and value happens where business, experience, and technology intersect

Mitigate risks and achieve desired business outcomes to enable a more secure digital transformation:

Engage your customers

Engage customers securely across any channel, deliver new experiences, and ensure customer information is protected

Empower your employees

Unleash the creativity and energy of your workforce by allowing them to collaborate and share knowledge securely anytime from nearly anywhere

Optimize your operations

Identify and reduce security risks, mitigate damage, and respond more effectively to threats and attacks

Transform your products

Deliver the first and best products and customer experiences and realize value in new markets with a secure innovation platform

Accelerating you to being a secure digital business

Dream
Envision the art of the possible

TRENDS AND INSIGHTS
What are the key trends and insights that are relevant to our industry?

DIGITAL VISION
How do we envision the future reality of our business?

DIGITAL JOURNEY MAP
How do our customers engage with our organization?

SCENARIO PLANNING
How will we challenge the convention by envisioning the Imagine if…? What if…?

SOLUTION STORYBOARD
What solutions would address our scenarios?

VALUE SCORECARD
What's the value of the new outcomes?

ROADMAP
What are the phases and milestones to get there?

Design
Build your desired state and roadmap

ECONOMIC JUSTIFICATION
How will this drive customer benefit?

ADOPTION & CHANGE MANAGEMENT PLAN AND ROADMAP
How can we address implementation challenges through an adoption and change management plan and roadmap?

DIGITAL TRANSFORMATION UNIT
What team will get us there?

PROTOTYPE
What will the future look like?

Deliver
Bring your vision to life

AGILE STORYBOARDING
What are the project features' sequence and interconnectedness?

RAPID PROTOTYPING
Can we see it in action?

VALUE ENGINEERING
Are we making the right tradeoffs to deliver the lowest cost consistent with required performance, quality and reliability?

TRANSFORMATION ROADMAP
How will we move forward in a prioritized manner?

VALUE DELIVERY AND MANAGEMENT
As we deliver, how will we ensure value and realize benefits?

Getting started with digital

The three critical components that organizations need to proactively tackle head on to mitigate risk and achieve their desired business outcomes to enable a more secure digital transformation are:

THREAT PROTECTION
Mitigating cyberattacks with modern protection, early detection, and 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.

SECURITY MANAGEMENT
Gain visibility and control over security tools.

You are reinventing what it means to do business, and we're committed to co-creating the right solutions with you.

Solutions that are disruptive but robust, delivering real results at speed.

Together we can reimagine the art of the possible.

Empower organizations to do more by accelerating the value imagined and realized from their digital experiences.

Imagine. Realize. Experience.

microsoft.com/services
microsoft.com/security
microsoft.com/digitaltransformation