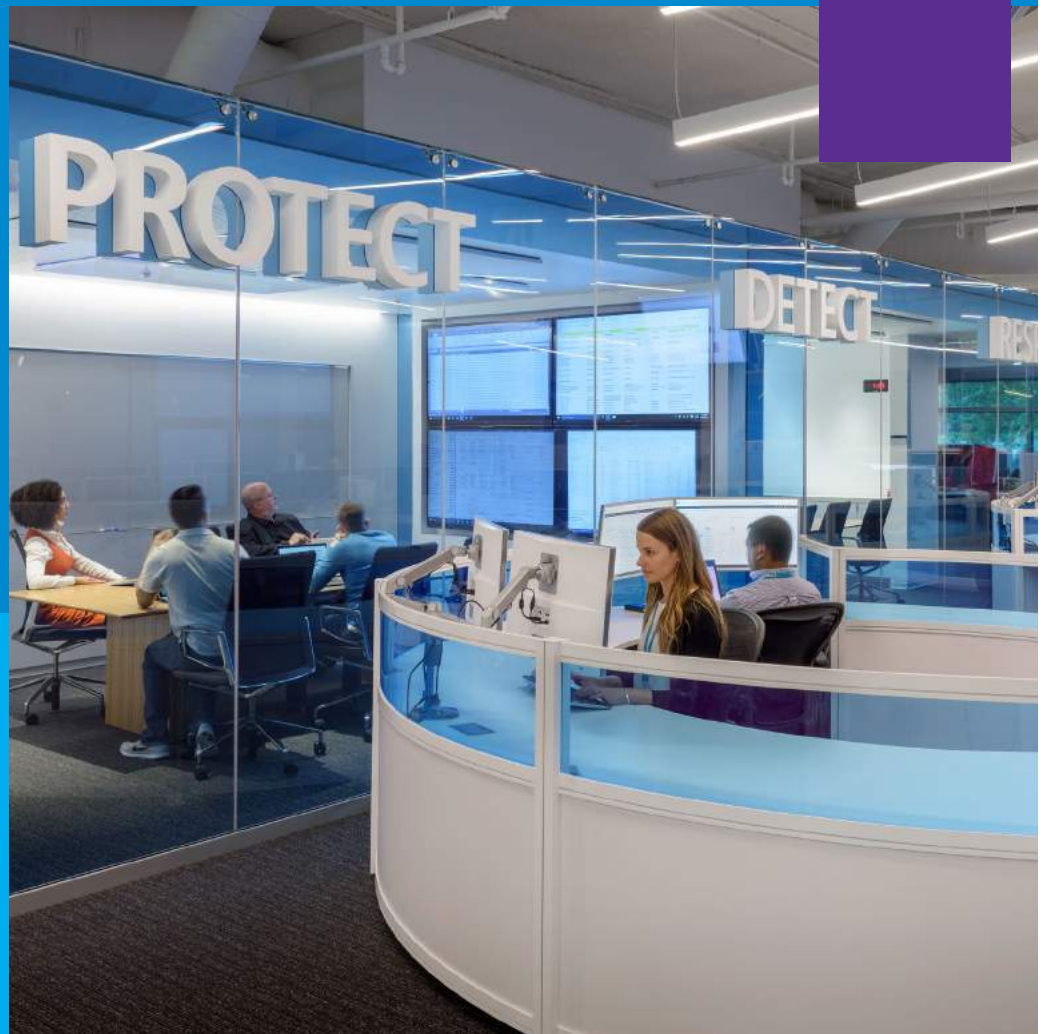




Microsoft as a Trusted Advisor and Partner on Cyber Resilience



WHITE PAPER



TABLE OF CONTENTS

- Authors..... 3
- Resilience, Threats, and Business Impact..... 3
- Importance of Cyber Resilience..... 5
- Build and Execute a Roadmap for Cyber Resilience 8
- How Microsoft Helps Support Your Cyber Resilience Strategy12
- Conclusion17



Microsoft Corporation | One Microsoft Way | Redmond, WA 98052-7329, USA | Sales 1-800-426.9400 | www.microsoft.com

Microsoft (Nasdaq “MSFT” @microsoft) is the leading platform and productivity company for the mobile-first, cloud-first world, and its mission is to empower every person and every organization on the planet to achieve more. Microsoft refers to Microsoft Corp. and its affiliates, including Microsoft Mobile Oy, a subsidiary of Microsoft. Microsoft Mobile Oy develops, manufactures and distributes Lumia and Asha and Nokia X mobile phones and other devices.

© 2017 Microsoft Corporation. This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Resilience, Threats, and Business Impact

RESILIENCE IN THE CYBERSECURITY REALM

Resilience is the ability to recover from or adjust easily to misfortune or change.¹ Cybersecurity is a realm abundant with both misfortune and change, requiring organizations to survive despite them and to grow stronger because of them. Hence, cyber resilience is the ability to manage risk by keeping the business operational and keeping critical systems (and data) available in the face of serious cyber-attacks.

This necessitates that organizations invest across the lifecycle of risk mitigations including Identify, Protect, Detect, Respond, and Recover (as described in the NIST Cybersecurity Framework²). Resiliency is a requirement that spans traditional physical and natural risks as well as cyberattack risks to the organization's business continuity. Resiliency in a digital world requires organizations to have a holistic approach to manage all these risks which span people, process, existing technology, and new technologies such as cloud services, Internet of Things (IoT), and Artificial Intelligence (AI).

Many organizations are going through a digital transformation leveraging a hybrid of cloud and on-premises assets to increase business efficiency and growth. While increased dependence on technology for business success is inevitable and, many would argue, necessary, this transformation poses business risks. For one, there is a more extensive attack surface to be protected (on premises, in the cloud). Also, personal data must be accounted for and protected no matter where it resides and whenever it is accessed. Since employees, contractors, suppliers, partners, and customers might connect to corporate applications and data from anywhere at any time, everyone's identity must be secured and managed. Furthermore, adversaries are both increasingly persistent and efficient. Considering that it takes a median time of 99 days to discover a breach,³ and just under 2 days (aka. 48 hours) for attackers to gain complete control of a network,⁴ organizations must develop comprehensive plans for keeping their hybrid infrastructure resilient to cyberthreats since it is impossible to be 100 percent secure.

The benefits of a cyber resiliency plan and roadmap is industry agnostic. It doesn't care what field of expertise or focus. The governments of the world have the same resiliency requirements as commercial and private industry. We have detailed throughout this document for customers regardless of industry to have the ability to build a plan and roadmap for their organization. This process will work for companies working on a government cloud or in our other regions and availability zones across the Azure cloud.

Cyber resilience is a journey that requires immediate steps to get ahead of current threats, as well as investment in foundational elements to sustain these gains over the longer term. Microsoft has built prescriptive roadmaps to help organizations rapidly become resilient to some of the most commonly encountered attacks. Our roadmaps provide specific actions for the first 30



Authors

Shawn Anderson – Enterprise Security Advisor, Enterprise Cybersecurity Group - Microsoft

Mark Simos – Lead Architect, Enterprise Cybersecurity Group - Microsoft

Seema Kathuria – Sr. Product Marketing Manager, Enterprise Cybersecurity Group - Microsoft

Diana Kelley – CTO/Evangelist, Enterprise Cybersecurity Group - Microsoft



days, the first quarter, and beyond. Microsoft has invested significantly to help organizations stay resilient to cybersecurity attacks on a modern enterprise with:

- **Prescriptive Guidance** to protect the range of on-premises and cloud assets, including:
 - **Mitigating Office 365 Attacks** – <https://aka.ms/O365secroadmap>
 - **Securing Privileged Access** – <http://aka.ms/sparoadmap>
- **Capabilities** to help with resilience across the security lifecycle (including Protect, Detect, Respond)
- **Strategic Guidance** to manage the complexity of security
 - **Reference Strategies** – to accelerate your strategic planning <http://aka.ms/MVA-cybersecurity-ref-strategies>
 - **Security Incident Response Tips and Guidance** – to manage technical, operations, legal, and communication challenges <http://aka.ms/IRRG>

Cybersecurity Portfolio

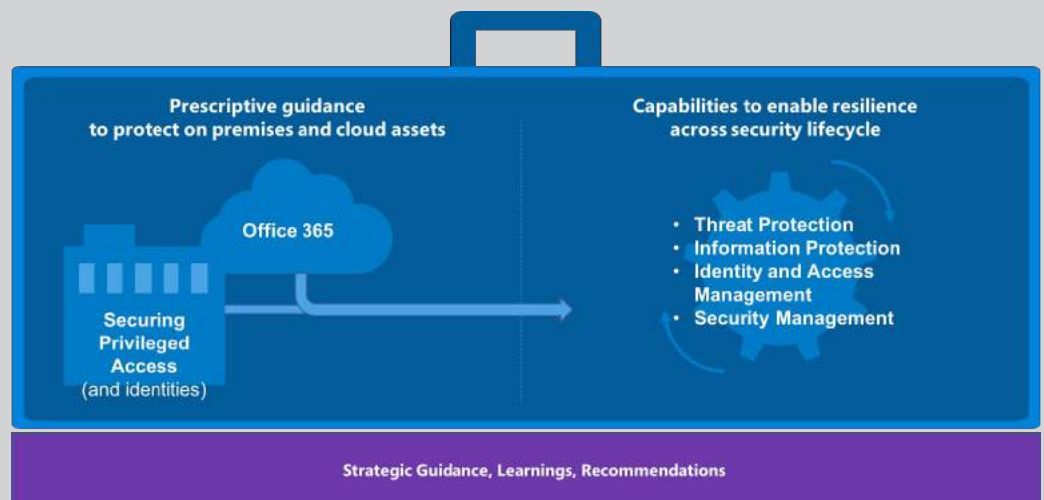


Figure 1:

Microsoft offers a broad portfolio of cybersecurity capabilities with both prescriptive and strategic guidance to help you build resilience across on-premises and cloud-based assets

ATTACKS ARE INEVITABLE – BUSINESS IMPACT ISN'T

Cyberattacks and data breaches continue to impact multiple organizations in the private and public sectors and in different industries worldwide.⁵ A recent attack called “Petya” (or sometimes “NotPetya”) resulted in several examples of significant business impact in the \$200-300+ million range.⁶ These numbers were reported by large global organizations including some reports of lost revenue that impacted operating results.

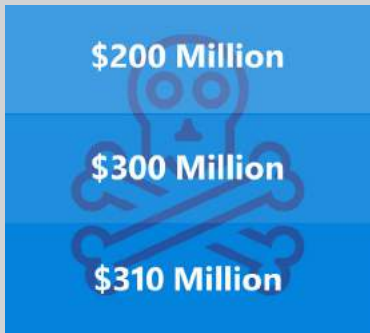


Figure 2:

Range of business impact from Petya ransomware in early 2017

To stay competitive and agile, enterprise organizations have been going through a transition in the way they conduct business with customers and partners. They are increasingly adopting cloud and mobility solutions. At the same time, cyber adversaries are increasingly focused on specialization and professionalization of attack skills and services to enable greater profits from attacks (in an industrialized dark economy).

Commonly, organizations are trapped in a reactive mode when it comes to protecting their critical data and infrastructure. Because time and human resources are fixed assets (and cybersecurity talent is in high demand), it is difficult to obtain and

utilize budget to build a proactive program of monitoring and protection using traditional approaches.

Despite what may seem to be “doom and gloom” scenario, there is light at the end of the tunnel. You can transform your security program into a proactive and resilient stance using the same cloud technology that is enabling your business transformation. This will help you both:

1. Mitigate the impact of an attack more easily
2. Reduce the likelihood of successful attacks

Importance of Cyber Resilience

If you accept that it is not a matter of if, but when, your organization will be a victim of a cyberattack, then you will appreciate the importance of taking a cyber resilience-based approach to security. As stated in the National Institute of Standards and Technology (NIST) Special Publication 800-53,⁷ “Whether systems are deployed to support the national air traffic control system, a major financial institution, a nuclear power plant, or the military services and warfighters, the systems must be reliable, trustworthy, and resilient in the face of increasingly sophisticated and pervasive threats—and also support the privacy of individuals.”

SECURITY COMPROMISES, SECURITY HYGIENE, AND EVENT OVERLOAD

From multiple customer engagements we have observed that approximately 86 percent of security compromises occur because of a lack of basic security hygiene (such as security patches, antimalware, backups, configuration consistency, and administrative credential protection). Even technically savvy nation states frequently use basic security hygiene issues to penetrate target environments.⁸

Keeping up with security hygiene issues is very challenging with traditional on-premises security approaches because they:

- Require significant manual effort to deploy and update
- Produce too many security alerts across too many dashboards for human analysts to process
- Limit visibility within siloed solutions
- Provide limited assurances for natural disasters and physical security incidents

Microsoft has taken an approach to resolve these problems that embraces modern cloud automation, analytics, integrated toolsets, and vast pools of security intelligence data that both:

- Reduces manual effort to resolve security hygiene issues
- Eases the burden of human analysts

Because cyber attackers will tirelessly try to gain access to your trade secrets and other “crown jewels” wherever they are, it is valuable to partner with a security savvy organization like Microsoft with deep expertise across existing on-premises assets as well as the full breadth of cloud solutions.

This kind of partnership can help you plan and implement a tailored strategy to build cyber resiliency which both protects and enables your business.

The following real-world examples are cases to illustrate where a lack of resiliency measures led to significant business productivity and operational impacts. Microsoft has engaged and partnered with multiple customer organizations facing these types of scenarios to plan and execute measures to become more resilient:

Example company A: Supplier of goods and services that fell victim to a ransomware attack which immobilized thousands of systems. Without paying the ransom, they have no idea how, when, or if they will recover their assets. This situation led to significant marketing/PR and safety risks for the organization and their people. The organization faced the challenge that even if they paid the ransom, there was no guarantee the attacker would provide the required decryption keys (and in fact they would be labeled as “likely to pay” so they can be targeted with more ransomware attacks). In such a scenario, Microsoft recommends basic security hygiene, particularly including that the organizations regularly patch and upgrade systems (or retire outdated systems) to avoid the possibility of future ransomware attacks.

Example company B: A large investment company employs thousands of traders who perform transactions on behalf of investors. This organization has multiple IT Datacenters in a single geography, but faces the risk of a catastrophic local event such as a hurricane, earthquake, or manmade disaster taking down both the primary and back

up data centers in the same time zone. Because they are now at the mercy of many factors (relative to competitors and peers who have embraced cloud technology) and their investors may consider taking their business elsewhere to ensure their trades will happen reliably, Microsoft recommends deploying business critical workloads with appropriate geo-redundancy configurations in Azure to ensure the organization is resilient to any localized event.

Here we share some of the common challenges we see among organizations and suggested approaches for responding to those challenges.



Cyber Resilient Approach

Challenge		Suggested Approach
Insecure IoT deployments		Building security in
Untested IR and response chaos		Red Team/Blue Team for testing and optimization
Systems left unpatched		Regularly patch and upgrade/retire outdated systems.
Cybercriminals "outsmarting" even mature security systems		Implement advanced threat detection and response approaches that use ML
Human error		Regularly train and educate personnel on security
Attacks are inevitable. It may be weeks or months after an incident until discovery.		Mitigate business impact by becoming cyber-resilient.

Figure 3:

Organizations are faced with the inevitability of attacks, and thus, need to be cyber resilient.

NEED FOR CONTINUOUS COMPLIANCE AND BUSINESS RESILIENCE

In addition to the business benefits of resiliency to help manage down cyberattack and other risks, many industries are required by law or regulation to achieve outcomes only available in a truly resilient organization. Public companies and those that are part of a regulated industry are required by law to publicly disclose data breaches and take prescriptive measures to address the damage to their business and customers. Compliance with standards such as the European Union's General Data Protection Regulation (GDPR) have begun to measure security outcomes rather than security configurations and processes. This regulation is also increasing fines significantly to ensure organizations are safeguarding personal data.

From a business resilience perspective, companies cannot afford to be down for weeks or days, because it puts them at risk of losing customers and credibility in the marketplace, or worse, impacts human life. One in five organizations lose customers due to an attack, and nearly 30% lose revenue.⁹

A BUSINESS INTERRUPTION MEANS DIFFERENT THINGS TO DIFFERENT INDUSTRIES

Manufacturing companies frequently cannot make up for production losses if their systems stop working, creating a deep concern about cyber resilience. For instance, pharmaceutical companies can be heavily impacted if production comes to a halt due to a cyberattack. They will not be able to fulfill customer SLAs, may lose business to competitors, and will suffer brand damage. Furthermore, the production losses can impact their top and bottom lines and even human lives. Imagine the human consequences if manufacturers of flu vaccines could not meet demand because production came to a standstill after a cyberattack, leading to a significant shortage worldwide. This would result in increased human exposure to the virus, the potential for exponential growth in the number of cases, and higher probability of loss of life among the affected population.

Financial services organizations are heavily regulated and place utmost importance on safeguarding both the privacy of their client data as well as their own trade secrets and intellectual property (IP). This helps them maintain a competitive stance in the market and the trust of their clients. Cyber adversaries heavily target financial institutions because of the high potential return of a successful attack. If a financial institution suffers a cyber-attack, the C-level/senior leadership team will be held accountable for brand damage, financial loss, customer distrust, and lawsuits that result from an incident.

Build and Execute a Roadmap for Cyber Resilience

This section of the document will walk you through how to build a roadmap for resiliency of a modern organization. Regardless of the business and compliance risks you face and your resource availability, you should take a phased approach towards cyber resilience starting with quick wins and following up with incremental progress. Additionally, you should ensure you don't let security concerns stop you from adopting critical technology enabling business transformation like cloud services.

When it comes to taking steps towards making IT cyber resilient and keeping data recoverable, many organizations have the misperception they need a solution that can stop every attack (e.g. the 100% approach). This approach frequently results in implementing too many technologies without the ability to manage them and extract value from them, or a state of "analysis paralysis" where very little happens because they do not know where to start.

Cyber resilience-based security requires balancing investment in traditional protection and detection measures as well as *response to and recovery from* cyberattacks. Careful planning and preparation across these areas can help you quickly strengthen the cyber resilience of your organization.

It is important to take a phased approach focusing on quick wins and incremental progress to ensure the organization is constantly making progress on the most important areas and can adjust to a dynamic environment. The security roadmap should always be based on business priorities and the technical reality of the threat environment and assets to be protected.



Build a Security Roadmap



Figure 4:

Process for building a security roadmap

This is our suggested process for building out your security roadmap:

1. Engage the right people.

First and foremost, make sure you have the right stakeholders from across the organization on the planning team and that there is executive buy-in. Additionally, a critical success factor is to include expertise in the planning process that deeply understand the security threat landscape and the modern cloud platforms and capabilities (something that Microsoft frequently helps organizations with).

This broad stakeholder participation is key to ensuring your security program is guided by the strategic business objectives and is grounded in the reality of the security threats and technology capabilities. Additionally, a good solid cyber resilience will impact people and business processes so those line of business representatives can provide the commitment needed to make sure these are executed well across the organization.

Your internal stakeholders should include representation from

- Each Major Business unit
- IT Operations
- Security
- Product Marketing
- Communications / Public Relations
- Legal
- Finance

2. Adopt a cyber resilience mindset

A critical factor in building a resilient organization is to establish the right cultural elements. The durable profit motive of the attack industry and the rapid evolution of attacks requires organizations to adopt a few key mindsets:

- **Assume compromise / assume failure** – Assume that attackers will be able to successfully compromise your environment. Your team's job is not to prevent all attacks, but to minimize the likelihood and impact of attacks by investing across the lifecycle of identify, protect, detect, respond, and recover.
- **Continuous learning** – Make learning (even learning from their own failures) a highly valued activity in your organization. To keep up with attackers, your teams will need to regularly learn better ways to protect the organization and better ways to prioritize investments.

3. Identify the most important assets

During the discovery stage, identify your top business priorities and catalog your most important assets.

Assets that are valuable for your organization from business impact and risk perspectives, can include:

- Systems that would stop a production line
- Systems that would halt sales operations
- Systems that would stop reporting of earnings
- Accounting/trading systems that handle business transactions (purchase orders, etc.)
- Financial systems that handle liquid/readily transferable assets
- Confidential documentation, such as trade secrets, competitive, etc.
- Regulated data (sensitive, confidential, private) of the business and its employees

Assets that are valuable to stakeholders outside your organization, can include:

- Regulated data of customers, partners and vendors that could incur significant fines if compromised (e.g. PCI DSS, GDPR, HIPAA, etc.)
- Information sharing systems in the supply chain that, if compromised, would compromise integrity, reliability, and availability

4. Build a security roadmap

Tips for building a good security roadmap:

- All elements in your security roadmap should include consideration of people, processes and technology to ensure that the solutions solve the problem in a sustainable way. This will help you keep the business operational and critical systems (and data) available in the face of serious cyber-attacks.
- Each item in the roadmap should focus on supporting one of these two objectives:
 1. Mitigate the impact of an attack more easily
 2. Reduce the likelihood of successful attacks
- When working with a new program, you can apply the “Three Bs”
 - **Baseline** – Identify where the program is using a standard such as the NIST cybersecurity Framework¹⁰
 - **Benchmark** – Compare where your program stands against industry peers and mature organizations
 - **Build** – Identify the short, medium, and long-term goals for your program and start investing

OPERATIONALIZE SECURITY

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

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

The 4 Pillars of Cyber Resilience

Information Protection	Threat Protection	Identity and Access Management	Security Management
			
Ensure documents and emails are seen only by authorized people.	Protect and recover quickly, so that you have the advantage, not the attacker.	Build an identity based security perimeter and implement an access control policy based on user risk level, to keep up with modern attacks and new asset types.	Gain visibility and control over security tools so you can be aware of suspicious or malicious incidents, and better prepared to take action on threats and respond to attacks.

Building security into the 4 pillars creates a cyber-resilient foundation for the business.

Figure 5:

Secure the four pillars to create a cyber-resilient foundation for the business.

Microsoft has organized these needs into four pillars we focus on solving for customers: information protection, threat protection, identity and access management 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.

How Microsoft Helps Support Your Cyber Resilience Strategy

Microsoft thinks differently about cybersecurity than most security industry vendors do because of our mission to empower every person and every organization on the planet to achieve more. Our approach reflects this philosophy:

- 1. Microsoft is focused on enabling a secure modern enterprise that meets both security and productivity needs.** Our culture places a high value on security, privacy, compliance as well as enabling the business mission.

If organizations focus on only one of these needs (to the detriment of the other), they will find themselves without either:

- An organization that prioritizes security and sacrifices productivity will incentivize users to adopt unsanctioned "Shadow IT" solutions (like mobile devices and unsecured cloud services), putting data and mission at risk while leaving IT unprepared to support users in need.

- An organization that focuses on productivity without meeting security requirements may find itself at major risk of data loss and operational downtime. This is exemplified by a steady stream of ransomware attacks which monetize productivity loss, including the WannaCrypt and Petya attacks that led to major operational downtime at global enterprises.

An Integrated Security Platform

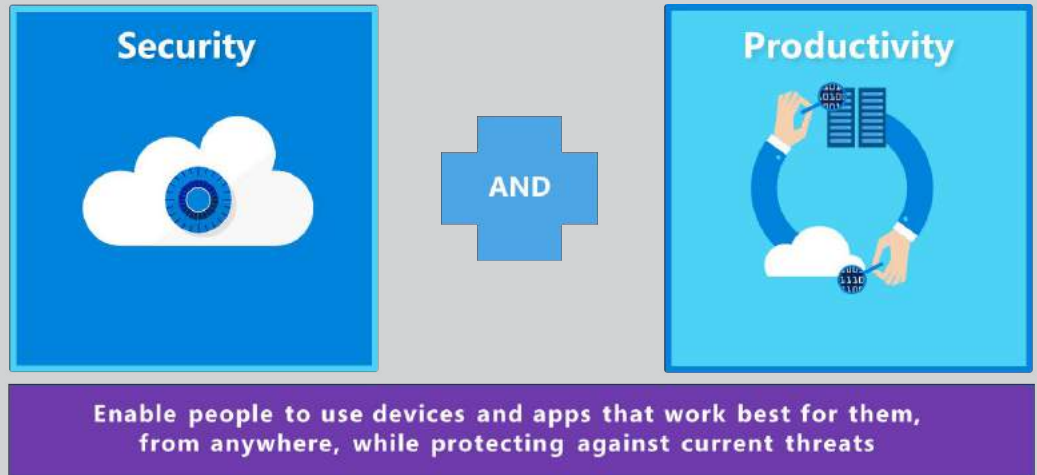


Figure 6:

Microsoft helps organizations achieve security and productivity.

COMMON INITIATIVES

- Biometric and Virtual Smart Card Authentication
- Mobile Application Management
- ...and More
- Self Service Password Reset
- Conditional Access to Resources

2. Microsoft is an integrated security platform. Microsoft focuses on creating an integrated security experience by integrating security into our platform and ensuring our customers can take advantage of our robust partner ecosystem. This takes the integration burden off our customers so that they can focus on managing risk and attacks instead of integration work.

3. Microsoft offers security roadmap support. Microsoft helps customers with development of their security roadmap and understanding of the security foundation first, and then assists with technology implementation to secure the four pillars mentioned earlier in the paper: information protection, threat protection, identity and access management, and security management. This allows the customer to focus on the business of IT rather than wondering, "What do we do next?"

Microsoft: A Cyber Resilient Foundation

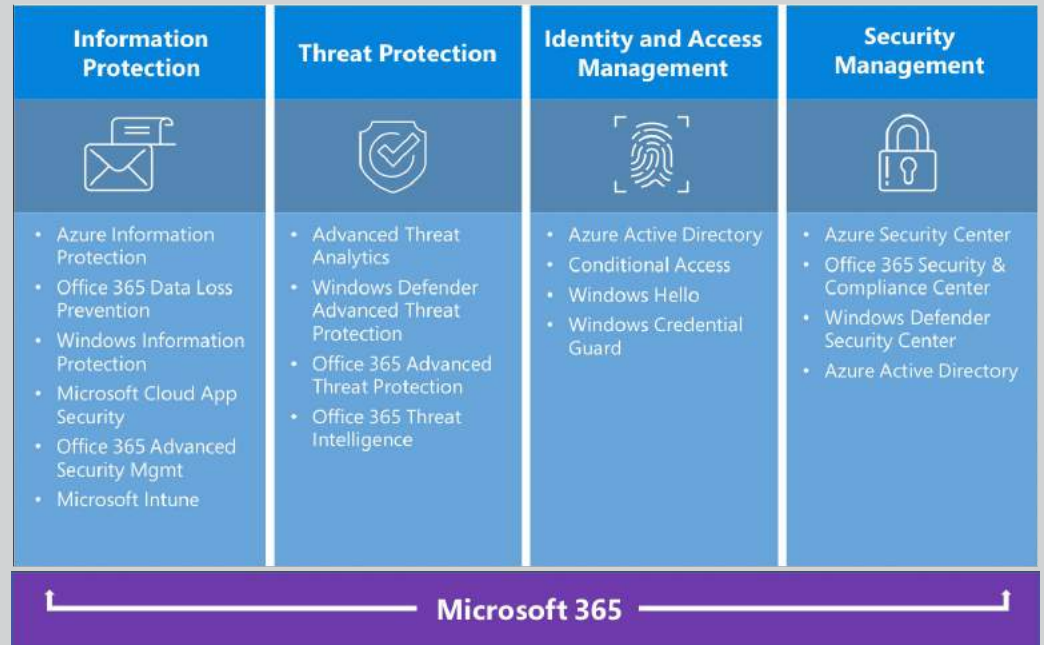


Figure 7:

Microsoft solutions mapped to four pillars to help create a cyber-resilient foundation for the business.

4. Microsoft provides large enterprises guidance, strategies, and solutions so they can build a cyber-resilient foundation for their business. Microsoft offers recommended strategies and solutions to help organizations execute on a cyber resilience-based security framework encompassing information protection, threat protection, identity and access management, and security management. We also give large enterprise customers the ability to assess and prioritize business risks. Develop cyber resilient strategies based on the security tenets of protect, detect, and respond, as follows:

PROTECT – to help protect organizations from advanced cyber-attacks, Microsoft has built solutions for the potential attack vectors:

- We can help secure your end-user identities where we leverage our machine learning and signal from the threat landscape to identify vulnerabilities to reduce the attack surface.
- Microsoft solutions help secure email, data, and even your app ecosystem.
- Microsoft solutions help protect your devices to prevent encounters, isolate malicious threats, and to control execution of untrusted applications or code.
- Microsoft can secure your cloud infrastructure by leveraging built-in controls across servers, apps, databases and networks.

DETECT – to help detect on those items they need to protect Microsoft provides numerous capabilities around anomaly, vulnerability, and suspicious activity detection.

- Microsoft has built several solutions and features to help our customers gain visibility across their organization. We offer solutions that can help detect suspicious behavior throughout the organization.

RESPOND – in the event of a breach, the ability to respond quickly is paramount to maintaining your business operations.

- Just as for 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.

- 5. Microsoft invests USD \$1 billion per year in security R&D, in part to build security into our solutions.** Our significant investment in security helps ensure we continue to build security not only into the very fabric of our cloud solutions but also across every product and service we provide. Microsoft has not only invested in enhancing security internally across the company, but also has made strategic investments in, and acquisitions of, new security companies and capabilities. Also, unlike companies that deliver standalone solutions, Microsoft offers embedded solutions that enable a defense-in-depth strategy.
- 6. Microsoft is committed to trustworthy computing.** Microsoft has been in the business of security for decades. It has always been there in many forms. Over the past few years, Microsoft has increased its commitment to security, not only through our financial investments but also through our overall approach. We have improved the security education of our workforce, implemented security development practices, and stay on top of security threat analysis and research. Furthermore, we build our Trusted Cloud on four foundational principles: security, privacy, compliance, and transparency. Learn more about these principles by visiting [this page](#).
- 7. Microsoft is a case study for what a cyber-resilient large enterprise can look like.** We plan to move all our data and services to a cloud-hosted environment. We call this plan the North Star, and it is based on following many of the recommendations and adopting Microsoft's solutions for building a sound cyber-resilient foundation that were described earlier.

KEY CONSIDERATIONS FOR BECOMING CYBER RESILIENT

- **Understand the cloud difference** – Networking in the cloud is slightly different from networking on premises, for a few reasons. With on-premises architectures, customers have a habit of putting up multiple defenses around hardware and software to keep people physically separated from the data. This limits productivity and efficiency. Networking in a hybrid or cloud environment requires planning and executing a security architecture with a focus on data protection and application management. With multiple tenants sharing resources and accessing data virtually/in a hybrid/cloud environment, you must implement a cloud-based identity and access management solution to control data access and prevent compromise.
- **Get the basics right** – Implement basic security hygiene measures including patching, using the most recent version of software, and creating a privileged access plan (get control of the admins!).
- **Train everyone** – Regularly educate employees and contractors on security best practices, hygiene, and cybercriminal tactics (e.g., phishing, malware, ransomware) so they will maintain heightened security awareness when communicating and exchanging data with anyone inside and outside the organization.
- **Plan for downtime** – Comprehensively plan for system downtime or disruption due to a cyberattack. This includes fuzz (security) testing applications as well as core infrastructure (e.g., Active Directory, domain controllers, email servers) for connectivity and performance. By planning ahead for a crisis, you will be able to restore core infrastructure elements such as user accounts, network access, and email communications more quickly and easily.
- **Back it up** – Back up business-critical data. Specifically, to protect against a ransomware attack, it is imperative to maintain a full backup in case your other defenses fail. Ransomware attackers have invested heavily in neutralizing backup applications and operating system features like volume shadow copy, so it is critical to have backups that are inaccessible to a malicious online attacker (including one who has stolen your admin account credentials).
- **Build resilience in** – Adopt systems and software to deliver reliability, trustworthiness, and resilience when faced with advanced threats.

Conclusion

Microsoft is committed to the success of our customers and strives to be the strategic technology and security partner that organizations can rely on. This is exemplified by our mission statement:

Our mission is to empower every person and every organization on the planet to achieve more.

Microsoft has been in the business of IT since its inception in 1975 and as far back as 2002, took measurable steps towards ensuring our products and solutions can be trusted and are secure. Today, we continue to build on that imperative by incorporating security into both our on premises and cloud platforms. We also actively partner with customers on their journey towards a secure cloud adoption. By partnering with us, organizations can build a cyber resilient foundation for their business to protect against, detect, and respond to cyber threats at all levels. As adversaries evolve and adeptly shift attack techniques and strategies, we need to be as prepared as possible. We must think differently, think bigger, and work together to keep our systems and people cyber aware and resilient.

For more details, see www.microsoft.com/security

References:

1. Merriam-Webster dictionary: <https://www.merriam-webster.com/dictionary/resilience>
2. NIST Cybersecurity Framework: <https://www.nist.gov/cyberframework>
3. "M-Trends 2016." 2016. Mandiant Consulting.
4. Anatomy of a Breach. 2016. Microsoft.
5. Heidi Daitch, 2017 Data Breaches – the Worst So Far. Blog post. <https://www.identityforce.com/blog/2017-data-breaches>
6. <https://www.cyberscoop.com/notpetya-ransomware-cost-merck-310-million/>
7. Security and Privacy Controls for Information Systems and Organizations. Draft NIST Special Publication 800-53, Revision 5. August 2017. <http://csrc.nist.gov/publications/drafts/800-53/sp800-53r5-draft.pdf>
8. NSA TAO Chief on Disrupting Nation State Hackers (USENIX Enigma 2016) <https://www.youtube.com/watch?v=bDJb8WOJYdA> <https://www.youtube.com/watch?v=bDJb8WOJYdA>
9. Cisco 2017 Annual Cybersecurity Report
10. NIST Cybersecurity Framework: <https://www.nist.gov/cyberframework>