Microsoft's cybersecurity commitment

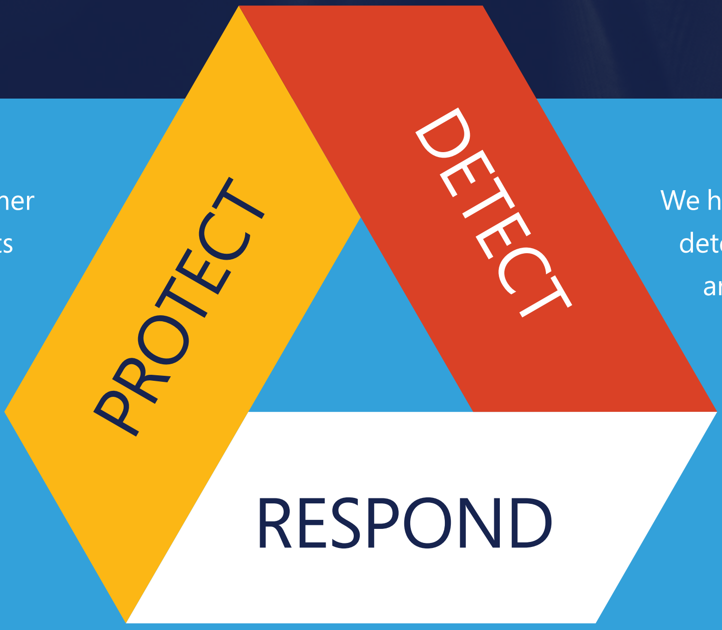
Published January 2015

Microsoft

At Microsoft, we take the security and privacy of our customers' data seriously. This focus has been core to our culture for more than a decade as part of our Trustworthy Computing commitment.

Our approach to security includes both technological and social aspects, and we are relentless in our efforts to ensure customer information remains safe and confidential. Drawing on almost four decades of experience, we make strategic investments to advance the security of our products and services, and regularly provide protection, guidance, and training to help our customers protect themselves. We are also a global advocate in advancing cybersecurity across the industry to create safer and more trusted computing experiences for everyone.

Our commitment to cybersecurity focuses on **protecting, detecting**, and **responding** to emerging threats.



We work to protect customer data by delivering products and services that are highly secure and by proactively combatting cybercrime.

We have global threat detection capabilities that are designed to help keep our customers' data highly secure.

We actively monitor changes in the threat landscape, and respond to emerging threats with timely security updates and by partnering with governments, law enforcement, and the industry to combat cybercrime.

Three core elements guide Microsoft's work and focus on cybersecurity: **security and privacy fundamentals**, **technology innovations**, and **industry and government collaboration**.

1 Security and privacy fundamentals

We have a culture of strong privacy principles and leading security practices that govern our approach to helping protect customer information. This approach has been informed by years of experience in dealing with, and responding to, a wide range of threats from cybercriminals.

Software development —Building security and privacy into our products and services from the start of our software development process is core to helping protect customers' data. The Microsoft Security Development Lifecycle is an industry-leading approach to building more secure software. It modifies the typical software development process by integrating well-defined security and privacy requirements throughout. This approach has been adopted by other commercial organizations and governments around the world as the basis for their security development programs.

Cloud operations—Our online services adhere to a rigorous set of security controls that govern operations and support through a process called Operational Security Assurance. This process makes the infrastructure of Microsoft cloud-based services more resilient to attack by decreasing the amount of time needed to protect, detect, and respond to real and potential Internet-based security threats.

Malware protection—Microsoft has a global network of world-class malware researchers and resources committed to working with the industry to eradicate malware. Our researchers monitor the threat environment based on feedback provided through our security products, research into industry trends, advanced automated malware analysis techniques, and industry partnerships. By using advanced research, machine learning, and heuristics, and continuously monitoring for malicious behaviors, our researchers are able to provide timely detection for new or emerging threats. Customers who use Microsoft antimalware technologies such as Windows Defender benefit from the ongoing protections provided by our malware researchers.

Security response—Should the unexpected occur, Microsoft has a global team of incident responders dedicated to ensuring customer safety when using our products and services. Our incident responders are on constant alert for security threats, monitoring security newsgroups, and responding to reported vulnerabilities 365 days a year. Through a well-defined process, they are able to quickly mobilize world-class global security teams capable of investigating, analyzing, and resolving security incidents.

2 Technology innovations

Microsoft is committed to investing deeply in building a trustworthy computing platform and providing security expertise to stay ahead of cybercriminals now, and as their tactics evolve.

Product security—Microsoft is committed to making ongoing investments that advance the security protections integrated into our products. For example, in Windows 10 we're actively addressing modern security threats with advancements that strengthen identity protection and access control, information protection, and threat resistance. With this platform, we will have nearly everything in place to move the world away from the use of single factor authentication options, like passwords. We are delivering robust data loss prevention right into the platform itself. When it comes to online threats, such as malware, we have a range of options to help enterprises protect against common causes of malware infection on PCs.

Cloud security—To help protect customer data in the cloud, Microsoft employs stringent security controls in its operations as part of its Operational Security Assurance (OSA) framework, and also provides controls that customers can take advantage of. Our multidimensional approach to securing online services starts in our facilities, where we maintain robust physical *security controls*, such as video surveillance, monitoring, fire suppression, security perimeters, multi-factor authentication, and backup power. Our network security controls include traffic flow authorization, denial-of-service mitigation, and vulnerability scanning. Host and application security controls include security updates, malware protection, highly secure development, highly secure operations, encryption options for data at rest and in transit, and incident response. We have strict security controls on who has access to the service at various levels, which include background checks, automatic account deletion, unique accounts, and limited access privileges. When it comes to *customer controls*, Microsoft provides identity and access management capabilities such as multi-factor authentication, highly secure password synchronization, and identity federation. For client and end-point protection, we provide device wipe, selective wipe, and walled gardens. For data protection, we provide encryption solutions, data loss prevention, and antimalware protections. Together, service-level capabilities and customer controls provide defense-in-depth measures that are designed to help protect customer data.

When it comes to compliance, Microsoft has over 30 years of experience working with enterprises to build on-premises workplace environments that comply with standards and regulations. We've used that experience in our cloud services and the modern compliance environment.

Security expertise—Microsoft's security engineering teams conduct some of the industry's most advanced security science research. The groups use applied science to develop more effective and scalable ways to discover and mitigate vulnerabilities, research innovative exploit mitigation techniques they can then apply to Microsoft products and services, and track new exploits to provide early warnings.

> Microsoft employs stringent security controls in its operations as part of its Operational Security Assurance (OSA) framework, and also provides controls that customers can take advantage of.

The Microsoft Malware Protection Center (MMPC) is one of the most experienced antimalware organizations in the industry. By building strong partnerships with organizations inside and outside Microsoft and continuously analyzing threat data, the MMPC stays agile to combat evolving threats. The mission of the MMPC is to help protect customers and computers by building a comprehensive network of partners dedicated to fighting cybercrime, by providing advanced defense through automation and cloud protection services, and by quickly responding to malware incidents.

The MMPC provides a critical head-start to these partners defending our customers across a wide variety of security industries.

The Microsoft Information Security & Risk Management group—which comprises architects, developers, program managers, technologists, and analysts— regularly provides guidance and shares best practices with our customers on how Microsoft manages risks within our environment.

Customer Service & Support (CSS) and Microsoft Consulting Services —Microsoft provides a wide range of capabilities from rapid incident response and recovery to world-class architects, consultants, and engineers to help support our customers' cybersecurity strategies with global reach and delivery. Organizations who take advantage of our consulting services benefit from: best practices and lessons learned based on extensible security capabilities that safeguard Microsoft's own technology infrastructure and information assets; remote security incident response capabilities; experienced investigators and malware reverse engineers; security solutions and consulting; and advanced tools and technologies to help detect threats to the network.

3 Industry and government collaboration

Microsoft actively works with the public and private sector to fight cybercrime and advocate for enhancing cybersecurity.

Industry collaboration—The Microsoft Active Protections Program provides our security software partners with early access to security vulnerability information in advance of Microsoft's monthly security update. Early access to this information helps our partners more quickly and effectively integrate protections into their security software or hardware products (such as antivirus software, network-based intrusion detection systems, or host-based intrusion prevention systems). This program provides a critical head-start to our security partners and, as a result, helps protect our customers across a wide variety of security industries.

To help customers make sound risk-management decisions and identify potential adjustments to their organizations' security posture, Microsoft regularly publishes information on threat landscape trends for more than 100 countries and regions worldwide. The information in these reports includes in-depth perspectives and analysis on exploits, vulnerabilities, and malware based on data from over a billion systems worldwide and some of the busiest online services.

Fighting cybercrime—Microsoft works to proactively fight cybercrime. Our Digital Crimes Unit (DCU) is a team of lawyers, investigators, data analysts, and other specialists committed to identifying and disrupting cybercrimes affecting our customers. To do this, we partner with global law enforcement agencies—including Europol, the FBI, and Interpol—academia, global governmental agencies, and nongovernmental organizations. Focusing on fighting botnets and other forms of malware, reducing risk for our customers, and protecting vulnerable populations (children and the less tech-savvy), this group applies legal, technical, and analytics expertise to help create a safer digital world. The intelligence derived from these operations is shared with Computer Emergency Response Teams (CERTs), Internet Service Providers (ISPs), and other organizations globally to clean infected devices. We also build this intelligence into our products and services (Azure Active Directory Premium, Azure Operational Insights and Microsoft Update as examples), and cybersecurity offerings from Microsoft Services.

The Digital Crimes Unit manages the Microsoft Cybercrime Center, a working laboratory in Redmond, WA, where we host customers and governmental officials, work with partners on malware operations, and bring together cybersecurity experts from within Microsoft and across the industry to work in partnership to fight cybercrime. In addition, DCU manages Cybercrime Satellite Centers in Beijing, Berlin, Singapore, Tokyo, and Washington D.C. We further extend cybersecurity-related customer and partner engagements through our partnership with Microsoft Technology Centers, located in more than 30 locations worldwide.

Government collaboration—Microsoft partners with government and educational institutions globally to help advance the operations of governments and the delivery of services to their citizens, expand the quality and reach of educational opportunities, and find new ways to help grow local economies. We have global policy experts that promote practical policies through legislative and regulatory engagement and promotion of global, industry led standards. Our experts share expertise and best practices with national, regional, and local authorities and critical infrastructures, and identify cybersecurity technology and policy issues on the horizon and leading industry's response. Recognizing that governments have unique security obligations to their citizens to protect and defend their national IT infrastructure and national economies from cyber threats, Microsoft has established a Government Security Program. This program is designed to address these complex needs and build trust in Microsoft products and services without sharing customer data.

Microsoft's Digital Crimes Unit manages the Cybercrime Center in Redmond, WA and Satellite Centers worldwide where we host customers and governmental officials, work with partners on malware operations, and bring together cybersecurity experts from within Microsoft and across the industry to work in partnership to fight cybercrime.

Microsoft

blogs.microsoft.com/cybertrust