

Microsoft Trustworthy Computing



Key Points

- Microsoft is committed to helping create safer, more trusted computing experiences. The company's approach is called Trustworthy Computing, a long-term, collaborative effort to create and deliver secure, private, and reliable computing experiences for everyone.
- Microsoft believes that technology should adhere to business practices that promote trust. Microsoft acts according to the principle that the technology industry should focus on solid engineering and best practices to ensure that the delivered products and services are more reliable, secure, and trusted.
- Microsoft supports collaboration among technology companies, governments, consumers, and businesses to solve the security challenges of today and tomorrow. Even parents need to be aware, taking steps to help ensure family online safety, including the use of safety settings.

BACKGROUND

The Internet allows people to enrich their lives, build commerce, and communicate around the globe. At the same time, the more people connect online, the greater the need to understand the implications of online security, safety, and privacy.

Microsoft's approach, Trustworthy Computing, is a long-term commitment and collaborative effort to create and deliver secure, private, and reliable computing experiences for everyone. As the Internet becomes increasingly critical to the computing ecosystem, Microsoft is also advancing the company's vision of End to End Trust.

Microsoft believes fundamentally that sensitive data and personal information must be protected and that technology should adhere to business practices that promote trust. Microsoft acts according to the principle that the technology industry should focus on solid engineering and best practices to ensure that the products and services they deliver are more reliable, secure, and trusted. Microsoft supports collaboration among technology companies, governments, consumers, and businesses to solve the security challenges of today and tomorrow.

SECURITY

Microsoft focuses on innovation in secure software development. The Microsoft Security Engineering Center helps to protect Microsoft customers by delivering more secure products through the Microsoft Security Development Lifecycle (SDL). The Microsoft SDL is Microsoft's security assurance process for software development that builds security into every phase of software development and provides defense-in-depth guidance and protection. Microsoft shares the SDL with the software industry to help build safer, more trusted computing experiences for everyone.

- Microsoft's Security Science team performs research that helps to understand online attacks and techniques.
- The Microsoft Malware Protection Center analyzes malicious software and develops solutions that are used in Microsoft security technologies.

- The company also produces the Microsoft Security Intelligence Report, which analyzes the threat landscape of exploits, vulnerabilities, and malware using data from Internet services and over 600 million computers worldwide.
- In the event a vulnerability in Microsoft software is discovered, the Microsoft Security Response Center monitors the situation and responds to the incident. It also manages the security update release process company-wide, and serves as the single point of coordination and communication for these matters.

PRIVACY

- Microsoft regards customer trust as critical to business success and regards protecting privacy as a foundation of that trust. People and businesses must have control of their information and how it is used.
- Microsoft was one of the first companies to appoint a chief privacy officer more than 10 years ago, and today more than 40 Microsoft employees work on privacy full-time. Meanwhile, hundreds more at the company help to ensure that privacy policies and technologies are applied across products and services.
- Microsoft builds privacy-enhancing technologies into products and services to help consumers protect their personal information.
- To help organizations more effectively manage the data in their possession, Microsoft provides guidance, frameworks, and technologies that are designed to help protect and manage personal information, mitigate risk, achieve compliance, and promote trust and accountability.

RELIABILITY

Cloud computing can provide substantial cost and efficiency benefits and deliver the latest tools and technology more easily. However, with the rise of cloud computing, reliability becomes even more critical. If cloud computing is to fulfill its promise, online services must be as or more available and resilient than their server and desktop counterparts. Microsoft is working to strengthen the reliability of cloud computing by reengineering key products such as Microsoft Exchange Server and Microsoft SharePoint Server to work better as cloud services. Microsoft is also implementing cutting-edge data protection and robust service redundancy in online services data centers.

POLICY CONSIDERATIONS

Microsoft believes public and private partnerships are also essential to address the increasing complexities of cyber crime. The company works with law enforcement agencies by providing them with technical training and in the development of new technology tools to help combat cyber crime. Microsoft has also assisted in protecting consumers through legal action to thwart cyber criminals. For example, the groundbreaking legal and technical efforts led by Microsoft, in cooperation with academic and industry experts around the world, worked to shut down the notorious Waledac and Rustock botnets, networks of tens of thousands of computers hijacked to spread malware, send spam, and commit other forms of cyber crime.



Helpful Resources

Microsoft Trustworthy Computing
www.microsoft.com/twc

Microsoft Safety & Security Center
www.microsoft.com/security

Microsoft Security Response Center
www.microsoft.com/msrc

Microsoft Security Intelligence Report
www.microsoft.com/sir

An overview of Microsoft privacy policies and initiatives
www.microsoft.com/privacy