Microsoft Cyber Security: A Key Ingredient in All Its Products

Microsoft products dominate the business world, powering everything from boutique businesses to the Department of Homeland Security. The company understands the critical role security and privacy play in every organization and builds Microsoft cyber security features into all its products.

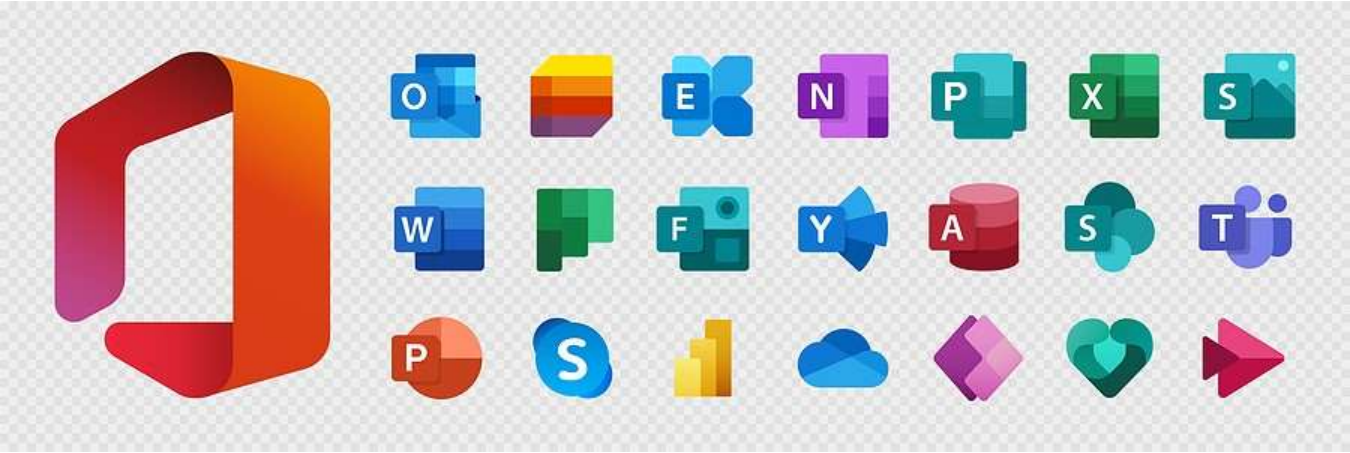
This commitment to security starts in the development process of every product. Additionally, Microsoft customers have access to world-class email filtering, a comprehensive data loss prevention solution and superior endpoint management.

Prioritizing Security by Design

Microsoft takes pains to build security into all its products from the very beginning. To that end, the company developed and continually updates a set of practices it calls the Security Development Lifecycle. These practices include:

- Security training for all employees – All Microsoft employees receive both general security awareness training and training specific to their roles.
- Security requirements – Development teams define security and privacy requirements for each product up front based on factors such as known threats and legal requirements. The team tracks and updates security requirements throughout the development process.

- Threat modeling – This involves identifying potential threats to an application or product. Developers then prioritize and address those threats based on their likelihood and impact.



- Using approved tools – Microsoft developers use a suite of secure development tools that include secure development environments, compilers, and built-in security checks.
- Perform security testing – Before releasing any product, developers perform several tests. These include checking the source code for security flaws, performing dynamic testing of the fully compiled software and using penetration testing to highlight security weaknesses.
- Gradual release – Even after a Microsoft product passes all the security tests, the company releases it in stages to progressively larger groups. After release, Microsoft products are monitored closely to identify potential security incidents.

Email Filtering

Email remains the most consistent attack vector. To that end, Microsoft provides Defender for Office 365. This cloud-based email filtering service delivers advanced protection against email threats such as phishing, ransomware, and business email compromise. Key features include advanced threat hunting, automated detection and response and attack simulation training.

Cloud-Native Data Loss Prevention

Data loss prevention (DLP) involves monitoring sensitive data across various locations to ensure against data breaches and unwanted destruction. Microsoft Purview allows organizations to create and manage DLP policies. These policies identify, monitor, and protect sensitive data across Microsoft services and Office applications.

DLP identifies sensitive items using machine learning and deep content analysis. When a situation triggers a DLP policy, the system automatically takes protective action. This can include encrypting data, blocking access, or reporting incidents. Built-in dashboards and reports simplify the process of monitoring and analyzing DLP incidents and policy performance.

Endpoint Management and Protection with Microsoft Intune

In a business environment dominated by remote work and BYOD policies, endpoint management takes center stage. Microsoft Intune delivers a cloud-based endpoint management solution that simplifies management of both company-owned devices and personal devices.

With automated policy deployment, the security team defines policies for device configuration, compliance, conditional access, apps and more. The team can then easily deploy policies to any device with internet access. At the same time, users benefit from self-service features to quickly install apps, reset passwords, and perform other administrative tasks.

Optimize Microsoft Cyber Security Features with Expert Help

Microsoft offers a range of powerful security features, beginning with a commitment to embedding security into every product. Tools such as Defender, Purview and Intune integrate fully into Microsoft 365, allowing organizations to fine-tune and strengthen their security approach.

These tools, while powerful, can prove complex to implement. The cyber security experts at eMazzanti Technologies can help. As a certified Microsoft Partner with deep security expertise, we will help you choose and properly implement the right tools for your organization.