

Defend against threats

Handle every threat, everywhere

Defend with the only security operations platform that combines the full power of a cloud-native SIEM, native XDR, global threat intelligence, and generative AI. This comprehensive, AI-powered unified platform helps SOC teams:

- Automatically disrupt in-progress attacks
- Detect and defend across the entire kill chain
- Get end-to-end-visibility into threats all in one place
- Automate threat response across security systems
- Proactively improve security posture and reduce risk exposure
- Supercharge SOC productivity with generative AI

See more. Act faster. Prevent attacks.

To battle increasingly bold, sophisticated, and well-resourced threat actors, security teams need integrated tools that work together. A unified platform built specifically for security operations can help the SOC coordinate defense and analysts quickly detect, prioritize, investigate, and resolve incidents with efficiency. Modern SOC tools should:

- **Triage quickly** with prioritized incident queues and generative AI-powered attack story summaries, helping analysts focus on the most important threats.
- **Boost analyst productivity** with a single experience that eliminates constant context-switching and manually filling in the gaps of siloed tooling.
- **Bridge the growing cybersecurity skills gap** by helping every analyst perform at a higher level. Analysts get step-by-step guidance, instant answers to questions, and complex queries and promptbooks.
- **Prevent breaches and reduce vulnerabilities** with tailored recommendations and suggested promptbooks that help find and protect critical assets, address exposures, and protect against adversary tooling, and protect against adversary tooling.

Seamlessly integrating AI with existing security tools, the skills of Microsoft security professionals, and Microsoft Threat Intelligence will strengthen your security posture.

Prevent attacks, detect and disrupt threats, and investigate and respond to incidents with Microsoft Security.



One unified platform to defend your multi-cloud, multi-platform environment

Defend against threats with built-in AI and automation to handle routine tasks. Discover high-value alerts in the noise. Manage the enormous volume of security signals generated within an organization. Get the full capabilities of the most advanced SOC tools integrated into a single platform, delivered through a fully unified experience, and enriched with global threat intelligence and generative AI. Augment SOC efficiency and extend teams with managed XDR and incident response services.

FEATURED PRODUCTS:	INTEGRATED:
Microsoft Defender XDR	Microsoft Defender Experts (Services)
Microsoft Sentinel	Microsoft Defender for Cloud
Microsoft Security Exposure Management	Microsoft Entra
Microsoft Copilot for Security	Microsoft Purview
	Microsoft Defender Vulnerability Management

The best protection is comprehensive security

Shift from reactive to proactive threat protection. Get tailored guidance on hardening your defenses and reducing your risk exposure. Disrupt in-progress threats, limiting the blast radius and making cleanup faster and less complex. Leverage AI and automation to correlate alerts into incidents and enrich with threat intel. Clean up compromised assets, prioritize analyst focus based on real-time risk exposure, and receive guidance on preventing future attacks.



Prevent attacks across your multi-platform, multi-cloud environment

Through one single portal, continuously monitor your digital environment, assess risk, and implement posture improvements using natively integrated security controls that work across all platforms, clouds, and hybrid infrastructure.



Detect and defend against threats across all systems

Get visibility into and disrupt hands-on-keyboard attacks in real time across identities, endpoints, email and collaboration tools, cloud apps, data, and hybrid and multi-cloud environments.



Investigate and respond faster with generative AI

Supercharge SOC team productivity and uplevel analysts' skills with generative AI that's integrated into their workflow.

Learn how a unified platform is leveling up SOC teams—while generating significant savings

Interviews revealed that, after investing in Microsoft threat protection, organizations saw a reduction in successful attacks and faster recovery. Key results also included enhanced production of the security team and the whole organization, as well as reduced investments in the security stack due to rationalization of tools from multiple vendors.

88%

reduction in response time to attacks

65%

reduction in investigative time

91%

reduction in time to onboard new analysts

\$1.6

million annual savings from vendor consolidation

THE RESULTS?

A 207% ROI over three years



Explore the reports

Built for your every need

Every security team differs and faces a unique threat landscape. A unified security operation builds the foundation you need to secure your digital environment while preparing for tomorrow. Since seeing is believing, check out how we can help across these scenarios:

- > Defend against ransomware
- > Defend against business email compromise
- > Modernize your SIEM
- > Protect identities
- > Reduce risk and unify security posture
- > Transform SOC productivity with generative AI
- > Augment your SecOps teams with Microsoft Security Experts



Learn more

Protect, detect, investigate, and respond with a unified platform at AI speed

Defend against threats with a powerful solution made up of multiple, integrated security products that help disrupt today's complex threats in near real time. Speak with a representative and put Microsoft's unified solutions to work—enhancing threat defense across your organization's entire digital estate.

Connect with a representative and put Microsoft security solutions to work



Get started