Microsoft Security

Microsoft Defender External Attack Surface Management

See your rapidly changing external attack surface in real time.

As digital transformation has accelerated, the threat landscape is more sophisticated than ever before.

Enterprise attack surfaces are expanding faster than the controls traditionally used to manage them.

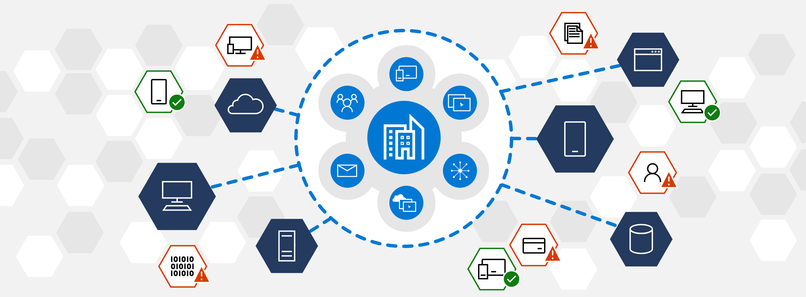
And factors such as work from home, mergers and acquisitions, and supply chain growth make it even more complex.

On top of that, threats are accelerating, with the cost of cybercrime now totaling more than USD 6.9 billion.

Many businesses have internet-facing assets they may not be aware of or have simply forgotten about.

Threat actors actively search for assets like these to use as entry points for attacks.

See your business as attackers can—from the outside in.



Discover

Discover internet-facing and exposed assets and resources you didn't know you had.

Monitor

Continuously monitor discovered devices and search for new vulnerabilities without the need for agents or credentials.

Secure

Understand vulnerabilites and exposed infrastructure so you can securely manage your resources.

Uncover your vulnerabilities with a real-time inventory of your assets.

Microsoft Defender EASM maps the internet to discover all of your unmanaged assets—including shadow IT and legacy services that may still be online—across all multi-cloud and hybrid resources.

Continuously monitor your digital footprint and exposure.

Maintain outside-in visibility into your resources for an always up-to-date view of your exposures—all without the need for credentials or agents.

Improve your security posture and enhance your current investments.

Expand the reach of your security tools by protecting these previously invisible resources with Microsoft Defender for Cloud or your cloud security solution of choice.

Ready to learn more?

Get more information about how you can get started with Microsoft Defender EASM.

Learn more >>

Or, find out how you can expand your threat protection further with integrated SIEM + XDR.

Learn more >>