# Ivanti Neurons for EASM

Combat attack surface expansion with full visibility of external-facing assets and actionable intelligence on exposures

The increased prevalence of Everywhere Work and everlasting digital transformation have led to unchecked attack surface expansion. Ivanti Neurons for External Attack Surface Management (EASM) provides a comprehensive, continuous view of internet-facing assets on your attack surface and associated exposures. Armed with this intelligence, you can eliminate high-risk exposures to proactively protect against cyberattacks.

ivanti
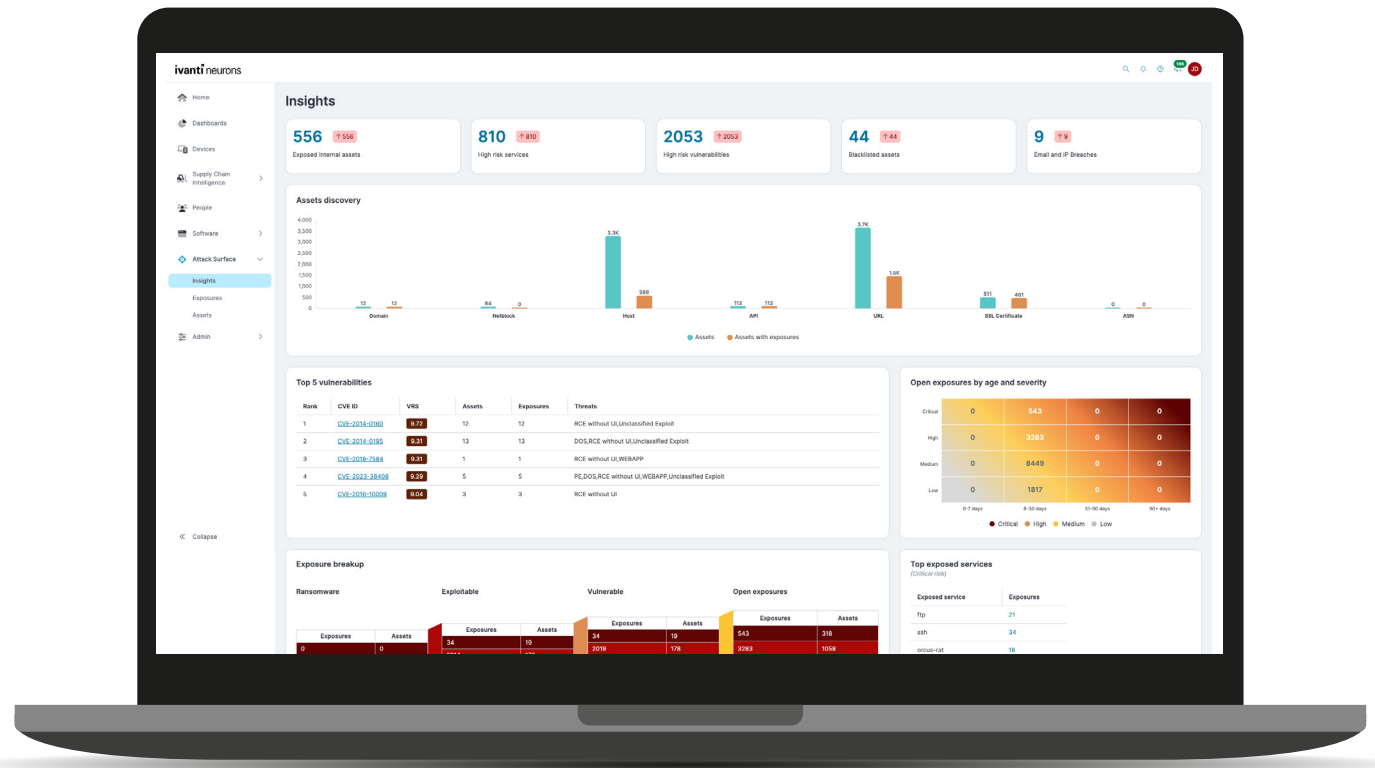
Unchecked attack surface expansion

The transition to Everywhere Work and onward march of digital transformation have accelerated use of shadow IT and cloud-based tools. Simultaneously, organizations are experiencing increased adoption of IoT devices and more interconnected supply chains.

As a result, security teams are struggling to attain visibility of external-facing assets across their attack surface. They also thus lack visibility into exposures associated with those assets.

Unknown, unvetted, unmanaged and unpatched assets leave organizations at risk of data breaches, fines and downtime. Security teams require continuous visibility of their entire attack surface to properly protect their organizations.

Introducing Ivanti Neurons for EASM

Gain and maintain visibility of every external-facing asset across your organization's attack surface with Ivanti Neurons for EASM. Leverage actionable, risk-based intelligence on exposures affecting those assets to proactively protect against data breaches, fines and downtime.

30%

EASM EFFECTIVENESS
On average, organizations using EASM tools discover 30% more assets than they knew they had[1]

ivanti

Key capabilities

Achieve full visibility

Unlock visibility of every internet-facing asset and associated exposure across your organization's attack surface. Agentless monitoring uncovers assets that evade detection by traditional discovery tools, as well as those that aren't normally monitored by security teams — think misconfigured Amazon S3 buckets, overlooked QA and dev environments, forgotten marketing websites and Java apps running on servers everyone thought were decommissioned.

Continuous monitoring ensures near-real-time visibility of these assets, so you know right away when existing assets become exposed or new assets are deployed and can respond accordingly.

Asset types discovered by EASM	Exposure vectors discovered by EASM
■ API ■ Domain ■ Host ■ Netblock ■ SSL certificate ■ URL	■ Application security ■ Data leaks ■ DNS health ■ Email security ■ Network security ■ Patching cadence ■ Social engineering

A workspace feature allows for assets and exposures to be grouped by categories, such as departments and subsidiaries. It also proves helpful when using Ivanti Neurons for EASM to monitor the external attack surfaces of third-party organizations, such as supply chain partners.

Prioritize high-risk exposures

Leverage actionable intelligence on exposures across your external attack surface to determine where to direct remediation efforts. Intelligence includes a Vulnerability Risk Score (VRS) for every CVE that Ivanti Neurons for EASM finds.

VRS empowers informed decision-making by enabling security teams to quantify the risk posed by a vulnerability and understand its threat context. It considers CVSS scores from the National Vulnerability Database (NVD) plus a range of other attributes that reflect the impact of a vulnerability in a given environment.

Report on risk

Satisfy reporting requirements from senior-level security stakeholders and aid in due diligence on potential acquisitions, partners and vendors with PDF reports. These exportable reports provide a thorough rundown of the exposures associated with an organization's external attack surface.

Address attack surface gaps

Tap into the power of Ivanti Neurons to close critical attack surface gaps unearthed by Ivanti Neurons for EASM. Couple Ivanti Neurons for EASM with the following products to enable the fastest response to issues impacting external-facing assets:

- Ivanti Neurons for ITSM: Orchestrate response to issues across teams.
- Ivanti Neurons for UEM: Manage and secure endpoints.
- Ivanti Neurons for Patch Management: Remediate vulnerabilities.
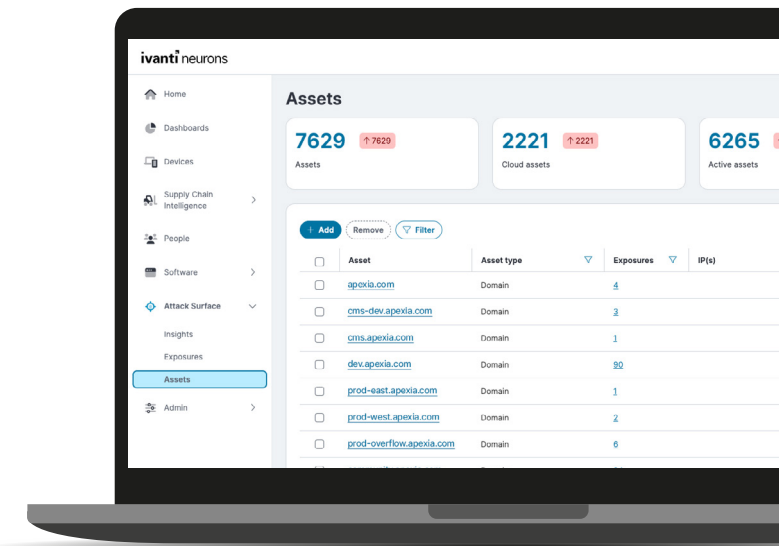
Extensive EASM use cases

EASM addresses a range of challenges facing modern enterprises.

- **Discover and inventory digital assets:** Find and inventory internet-facing assets from websites, IPs, domain names, SSL certificates and cloud services across cloud, IT, IoT and OT environments.

- **Analyze and prioritize exposures:** Prioritize remediation of exposures impacting external-facing assets, from unpatched vulnerabilities to misconfigurations and open ports.

- **Curb cloud sprawl and shadow IT:** Identify public assets across cloud providers — including cloud instances created by employees outside the proper channels.

- **Detect data leakage:** Monitor for data leakage or exposure of sensitive data via collaboration tools and cloud apps used internally and by third parties.

- **Conduct risk assessment on subsidiaries, third parties and acquisition targets:** Execute comprehensive security checks before integrating systems with other entities.

- **Reduce phishing and social engineering attacks:** Monitor for phishing domains, identify spoofed websites and detect potential social engineering attacks targeting employees and customers.

- **Adhere to regulatory compliance requirements**: Comply with regulations including GDPR, HIPAA and PCI DSS that require discovery and asset inventory.

About Ivanti

Ivanti elevates and secures Everywhere Work so that people and organizations can thrive. We make technology work for people, not the other way around. Today's employees use a wide range of corporate and personal devices to access IT applications and data over multiple networks to stay productive, wherever and however they work. Ivanti is the only technology company that finds, manages and protects every IT asset and endpoint in an organization. Over 40,000 customers, including 88 of the Fortune 100, have chosen Ivanti to help them deliver an excellent digital employee experience and improve IT and security team productivity and efficiency. At Ivanti, we strive to create an environment where all perspectives are heard, respected and valued and are committed to a more sustainable future for our customers, partners, employees and the planet. For more information, visit ivanti.com.

ivanti

For more information, or to contact Ivanti, please visit ivanti.com.

1. Forrester, "The External Attack Surface Management Landscape, Q1 2023," 9 January 2023