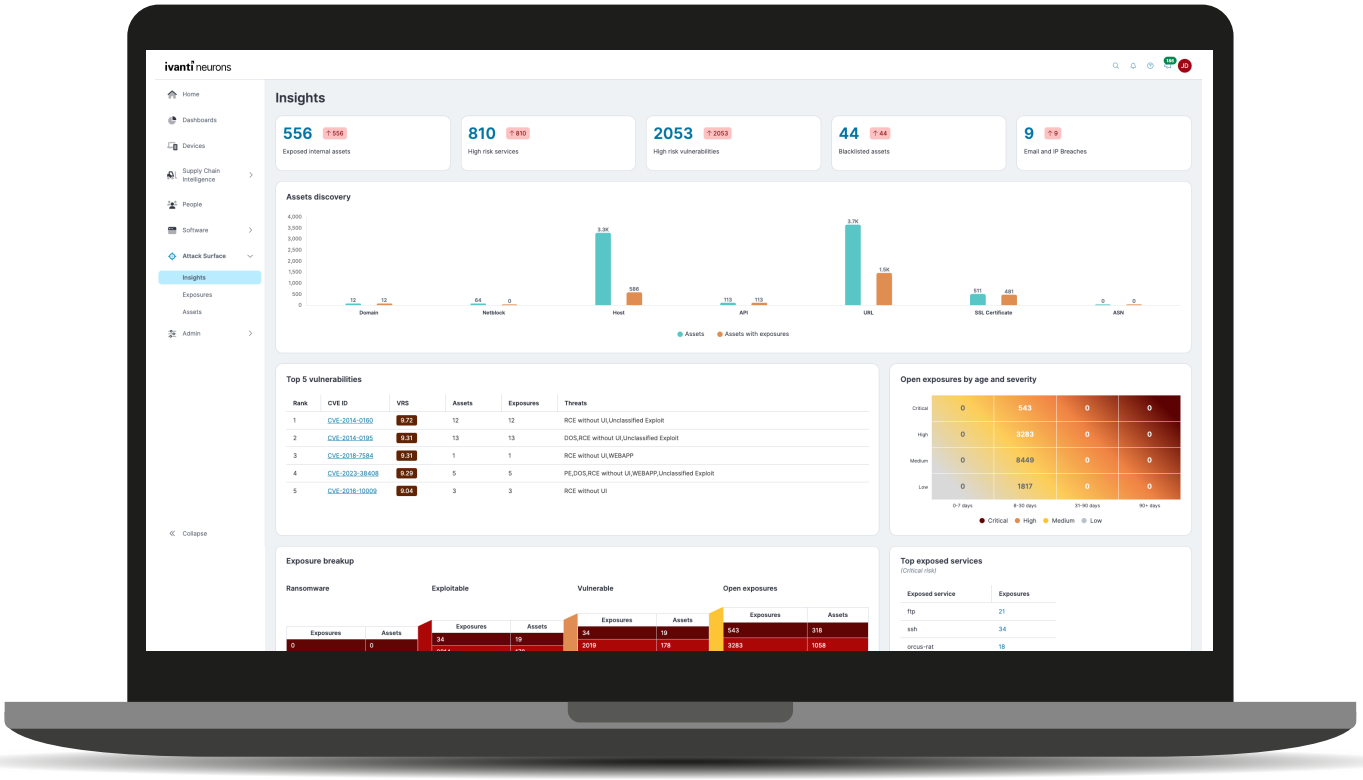
Ivanti Neurons for EASM

Vollständige Sichtbarkeit exponierter Assets und aussagekräftige Sicherheitsinformationen über Gefährdungen helfen dabei, der Ausweitung der Angriffsfläche wirksam entgegenzuwirken.

Die zunehmende Verbreitung von Everywhere Work und die fortschreitende digitale Transformation haben zu einer unkontrollierten Ausweitung der Angriffsfläche geführt. Ivanti Neurons für External Attack Surface Management (EASM) bietet einen umfassenden, kontinuierlichen Überblick über Ihre mit dem Internet verbundenen Assets und die eentsprechenden Gefährdungen. Mit diesen Sicherheitsinformationen können Sie potenzielle Risiken beseitigen und sich proaktiv vor Cyberangriffen schützen.



Unkontrollierte Ausweitung der Angriffsfläche

Der „Everywhere Work"-Trend und der Vormarsch der digitalen Transformation haben die Nutzung von Schatten-IT und Cloud-basierten Tools beschleunigt. Gleichzeitig werden in Unternehmen zunehmend IoT-Geräte eingesetzt und die Lieferketten stärker vernetzt.

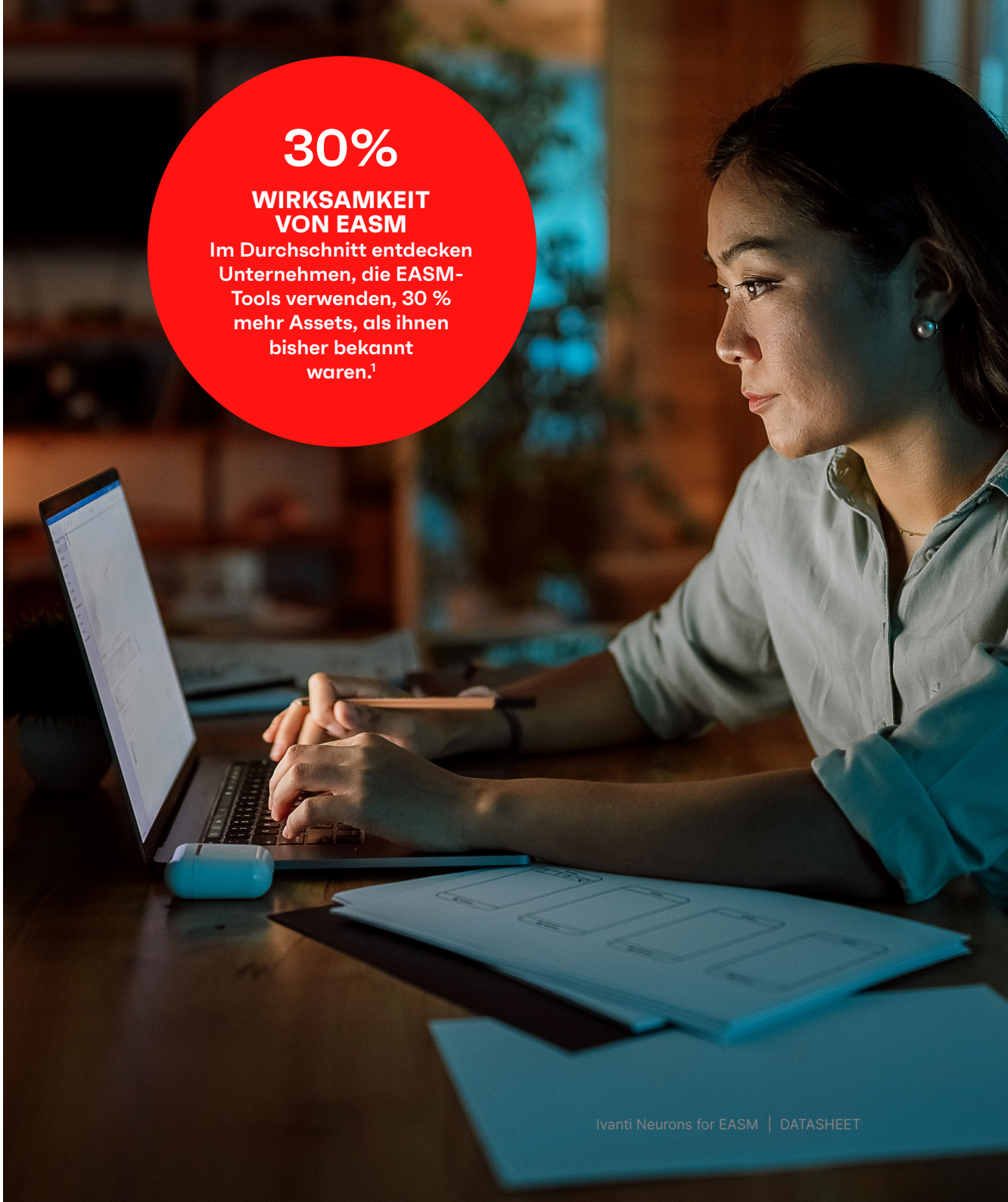
Infolgedessen ist es für Sicherheitsteams schwierig, einen Überblick über die exponierten Assets und die damit entsprechenden Angriffsflächen zu erhalten. Damit fehlt ihnen auch der Überblick über die Gefährdungen, die mit diesen Assets verbunden sind.

Durch unbekannte, nicht überprüfte, nicht verwaltete und nicht gepatchte Ressourcen besteht für Unternehmen das Risiko von Datenschutzverletzungen, Geldstrafen und Ausfallzeiten. Sicherheitsteams benötigen einen kontinuierlichen Überblick über die gesamte Angriffsfläche, um ihr Unternehmen angemessen zu schützen.

Einführung von Ivanti Neurons for EASM

Verschaffen Sie sich mit Ivanti Neurons for EASM einen Überblick über alle exponierten Assets Ihres Unternehmens. Nutzen Sie die zielgerichteten, risikobasierten Sicherheitsinformationen über Gefährdungen, die diese Assets betreffen, um sich proaktiv vor Datenschutzverletzungen, Geldstrafen und Ausfallzeiten zu schützen und unmittelbar wirksame und angemessene Maßnahmen ergreifen zu können.

ivanti



Wichtige Funktionen

Vollständige Sichtbarkeit erlangen

Verschaffen Sie sich einen Überblick über die mit dem Internet verbundenen Assets und die entsprechenden Gefährdungen für die Angriffsfläche Ihres Unternehmens. Die agentenlose Überwachung entdeckt Assets, die herkömmliche Erkennungstools nicht sehen können, sowie solche, die normalerweise nicht von Sicherheitsteams überwacht werden – man denke nur an falsch konfigurierte Amazon-S3-Buckets, übersehene QA- und Entwicklungsumgebungen, vergessene Marketing-Websites und Java-Anwendungen, die auf Servern laufen, von denen alle dachten, sie seien längst stillgelegt.

Die kontinuierliche Überwachung sorgt für eine nahezu Echtzeit-Sichtbarkeit dieser Assets. So wissen Sie sofort, wenn bestehende Assets gefährdet sind oder neue Assets bereitgestellt werden. Und sie können entsprechend reagieren.

Vom EASM ermittelte Assets	Vom EASM entdeckte Gefährdungsvektoren
■ API ■ Domain ■ Host ■ Netblock ■ SSL-Zertifikat ■ URL	■ Anwendungssicherheit ■ Datenlecks ■ DNS-Zustand ■ E-Mail-Sicherheit ■ Netzwerksicherheit ■ Patching-Häufigkeit ■ Social Engineering

Eine Gruppierungs-Funktion ermöglicht die Zuordnung von Assets und Gefährdungen zu Kategorien, wie z. B. Abteilungen und Tochtergesellschaften. Sie ist ebenfalls hilfreich, wenn Ivanti Neurons for EASM verwendet wird, um die externen Angriffsflächen von Drittanbietern zu überwachen, z. B. von Partnern in der Lieferkette.

Risikoreiche Gefährdungen priorisieren

Nutzen Sie aussagefähige Sicherheitsinformationen über die Gefährdungen in Ihrer externen Angriffsfläche, um zu bestimmen, wo Sie Maßnahmen zur Abhilfe ergreifen müssen. Sicherheitsinformationen enthalten einen Vulnerability Risk Score (VRS) für jede CVE, die Ivanti Neurons for EASM findet.

VRS ermöglicht eine fundierte Entscheidungsfindung, indem es Sicherheitsteams in die Lage versetzt, das von einer Schwachstelle ausgehende Risiko zu quantifizieren und ihren Bedrohungskontext zu verstehen. Es berücksichtigt CVSS-Scores aus der National Vulnerability Database (NVD) sowie eine Reihe anderer Merkmale, die die Auswirkungen einer Schwachstelle in einer bestimmten Umgebung widerspiegeln.

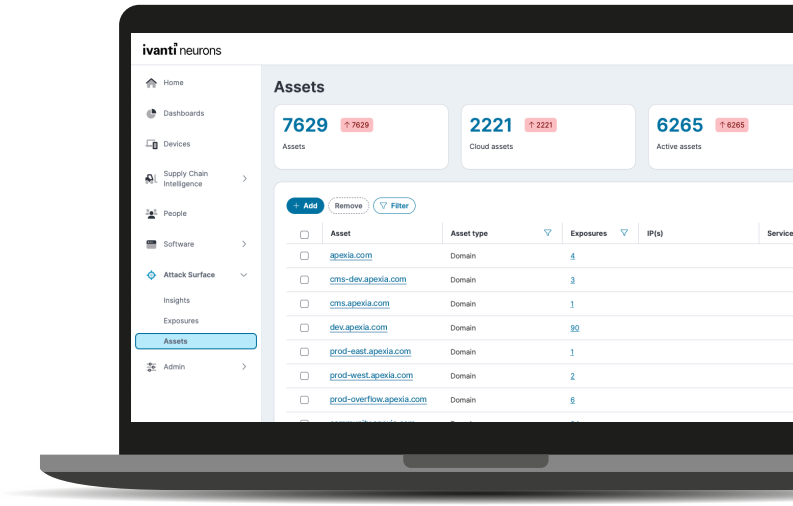
Berichte über Risiken generieren

Erfüllen Sie die Berichtsanforderungen von Sicherheitsverantwortlichen auf höchster Ebene und unterstützen Sie die Due-Diligence-Prüfung potenzieller Übernahmen, Partner und Anbieter mit PDF-Berichten. Diese exportierbaren Berichte liefern einen umfassenden Überblick über die mit der externen Angriffsfläche eines Unternehmens verbundenen Gefährdungen.

Lücken in der Angriffsfläche schließen

Nutzen Sie die Leistungsfähigkeit von Ivanti Neurons, um kritische Lücken in der Angriffsfläche zu schließen, die von Ivanti Neurons für EASM aufgedeckt wurden. Kombinieren Sie Ivanti Neurons for EASM mit den folgenden Produkten, um die schnellste Reaktion auf Probleme zu ermöglichen, die sich auf exponierte Assets auswirken:

- Ivanti Neurons for ITSM: Orchestrieren Sie Reaktionen auf Probleme teamübergreifend.
- Ivanti Neurons for UEM: Verwalten und sichern Sie Endgeräte.
- Ivanti Neurons for Patch Management: Beheben Sie Schwachstellen.



Umfassende EASM-Anwendungsfälle

EASM geht auf eine Reihe von Herausforderungen ein, mit denen moderne Unternehmen konfrontiert sind.

- **Digitale Assets entdecken und inventarisieren** Finden und inventarisieren Sie die mit dem Internet verbundenen Assets wie Webseiten, IP-Adressen, Domainnamen, SSL-Zertifikate und Cloud-Dienste in Cloud-, IT-, IoT- und OT-Umgebungen.
- **Gefährdungen analysieren und priorisieren** Priorisieren Sie die Behebung von Gefährdungen, die sich auf exponierte Assets auswirken, von ungepatchten Schwachstellen bis hin zu Fehlkonfigurationen und offenen Ports.
- **Cloud-Wildwuchs und Schatten-IT eindämmen** Identifizieren Sie öffentliche Ressourcen bei allen Cloud-Anbietern – einschließlich Cloud-Instanzen, die von Mitarbeitenden an den vorgesehenen Prozessen vorbei erstellt wurden.
- **Datenlecks erkennen** Überwachen Sie, ob durch interne und von Dritten genutzte Kollaborationstools und Cloud-Anwendungen Datenlecks entstehen oder sensible Daten preisgegeben werden.
- **Risikobewertungen bei Tochtergesellschaften, Dritten und Akquisitionszielen durchführen** Führen Sie umfassende Sicherheitsprüfungen vor der Integration von Systemen mit anderen Einheiten durch.
- **Phishing- und Social-Engineering-Angriffe reduzieren** Überwachen Sie Phishing-Domains, identifizieren Sie gefälschte Websites und erkennen Sie potenzielle Social-Engineering-Angriffe auf Mitarbeitende und Kunden.
- **Gesetzliche Vorschriften einhalten** Erfüllen Sie Vorschriften wie GDPR, HIPAA und PCI DSS, die eine Erkennung und Bestandsaufnahme erfordern.

Über Ivanti

Ivanti steigert und sichert Everywhere Work, damit Menschen und Unternehmen erfolgreich sein können. Wir sorgen dafür, dass Technologien für die Menschen arbeiten, und nicht umgekehrt. Die Mitarbeitenden von heute nutzen eine breite Palette von Firmen- und Privatgeräten, um über mehrere Netzwerke auf IT-Anwendungen und Daten zuzugreifen und so produktiv zu bleiben, egal wo und wie sie arbeiten. Ivanti gehört zu den wenigen Technologieunternehmen, die alle IT-Assets und Endpunkte in einem Unternehmen finden, verwalten und schützen. Mehr als 40.000 Kunden, darunter 88 der Fortune-100-Unternehmen, haben sich bereits für Ivanti entschieden, um ihren Mitarbeitenden eine hervorragende digitale Erfahrung zu bieten sowie die Produktivität und Effizienz ihrer IT- und Sicherheitsteams zu verbessern. Unser Ziel bei Ivanti ist, ein Umfeld zu schaffen, in dem alle Meinungen gehört, respektiert und geschätzt werden. Und wir setzen uns für eine nachhaltigere Zukunft für unsere Kunden, Partner, Mitarbeitenden und unseren Planeten ein. Weitere Informationen finden Sie unter ivanti.com.

ivanti

Für weitere Informationen oder zur Kontaktaufnahme mit Ivanti besuchen Sie bitte ivanti.com.

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