edgescan™

DATASHEET

AI Insights

Utilize Edgescan AI Insights to analyze vulnerability data in real-time.

In today's rapidly evolving digital landscape, organizations face an array of growing and diversified cyber threats. Their security teams face difficult questions:

"What vulnerabilities should we focus on?"

"What type of training for our developers would help improve our security posture?"

"Which assets are potentially exposed to ransomware attack?"

The answers are more complex than ever, and more specific to each individual organization. Traditional methods often fall short in providing timely and actionable advice, but AI Insights by Edgescan leverages cutting-edge machine-learning technology to empower an organization's information-security team to make informed decisions in real time and strengthen their security posture on a continuous basis.

By analyzing vulnerability data with Amazon Bedrock and a tuned version of Anthropics Claude, Edgescan delivers personalized, tactical recommendations for mitigating risk, prioritizing remediation efforts, and maintaining compliance.

Real-Time Analysis

The Edgescan engine instantly a nalyzes vulnerability data to provide immediate insights.

Personalized Insights

The engine delivers strategic analysis tailored to your organization's specific vulnerability data and systems architecture while incorporating Edgescan's deep knowledge of the prevailing cyber threat environment.

Dynamic and Scalable

The solution analyzes a vast data landscape of over 15,000,000 verified vulnerabilities to generate actionable insights and trending information, and can adapt to your organization's needs with insights specific to one unit of your business or across multiple.

These insights will continuously update as your business grows and your security posture evolves, and reports are directly linked to live vulnerabilities within your systems so you can take prompt action with full context.

Threat-Based Prioritization

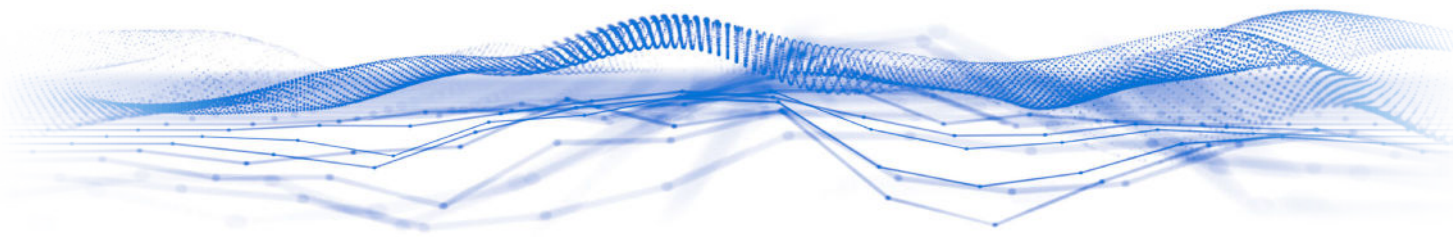
Address the most critical issues first with insights that draw on real-world threat analysis, ransomware intelligence, and a vast reservoir of metadata.

Ransomware Risk Assessment

The Edgescan engine evaluates vulnerabilities when they're uncovered to specifically assess the risk that they could be exploited by ransomware.

Compliance Guidance

This cutting-edge intelligence provides guidance as you move into full compliance with regulatory frameworks such as CIS, PCI-DSS, DORA, HIPAA, ISO, SOC2, GDPR, and more.



Training Focus

Get sharp insight into where you can best allocate resources for developer education and technical training based on trends in the vulnerability landscape, the current and future rate at which a specific vulnerability might occur, and the associated risk profile of that vulnerability with respect to your organization.

With this informed view of the landscape, you can guide your investments in training and education to reduce vulnerability recurrence, improve overall security expertise, and maximize value for your dollar.

Exploitable Vulnerabilities

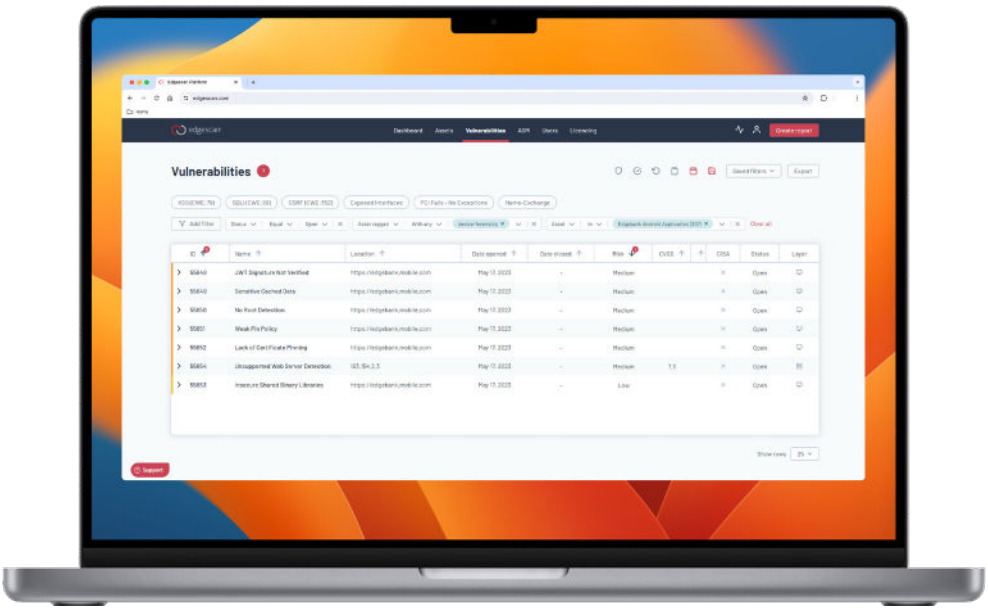
What are your current open vulnerabilities, and what are the associated exploit codes to look out for as you go about prioritization and remediation? AI Insights by Edgescan has the answers.

Anomaly Detection

Identify unusual patterns in in your data with AI Insights, including vulnerability clustering, frequent exposure types, and trends across your entire cyber estate or one particular business unit.

Your Data is Safe with AI Insights

Edgescan does not pass any identifiable data to our AI. This approach is designed to ensure privacy and data security, a common issue with AI based services. AI Insights can also be disabled if AI based insights “are not your thing.”



For more information on how Edgescan can help secure your business, contact: *sales@edgescan.com*

edgescan

IRELAND | Unit 701 Northwest Business Park, Ballycoolin, Dublin 15, D15 CH26
UNITED STATES | 445 Park Avenue, 9th Floor, New York, NY 10022