edgescan™

2025 Mid-Year Snapshot: Vulnerability Statistics Report

Executive Summary & Welcome

Welcome to the 2025 Mid-year Vulnerability Stats Report for Edgescan.

This is based on the last 6 months of delivering adversarial and offensive testing across hundreds of clients globally—more than 40,000 assessments, and 1000+ penetration tests across a split of Assets Network/Cloud: 47%, Web Applications: 32%, APIs: 21%.

From a market standpoint we're certainly seeing a move from traditional consultancy based penetration testing to continuous automated PTaaS (Penetration Testing as a Service). This is due to the lower friction, rapid results and guaranteed accuracy delivered by such a model. It also saves organizations significant spend. Such approaches save out clients significant budget, resource allocation to offensive security is reduced and reliance on high quality vulnerability and exposure intelligence is increased. (In the first half of 2025, we saved a North American client in excess of one million dollars as a result of employing Edgescan during a due diligence phase of an M&A project!)

Be mindful, automated penetration testing is still just a scan. The "devil is in the detail," and business logic and logical cyber security testing still need human intelligence to verify and exploit. Most penetration testers would agree the best "hacks" they've ever successfully exploited were in the business logic space with the ability to easily demonstrate data or financial theft. Automated penetration testing alone frankly does not deliver such results. We've employed the best of AI, analytics, clever automation and a human touch to deliver deep, high-quality, continuous vulnerability and exposure detection and management.

Visibility of ones landscape is nothing new, but a feature called Attack Surface Management (ASM) combined with bonafide exposure and weakness assessment has been proven to keep pace with constant change.

The introduction of clever AI for prioritization and validation combined with our unique data lake to analytical validation and triage has proven to deliver accuracy without scale and speed suffering.

Hope you enjoy this short report.

Best,

Eoin Keary
Founder/CEO, Edgescan

How does Edgescan measure Security?

Edgescan discovers and validates all exposures and vulnerabilities to remove false positives, false alarms and make our users lives a little easier. The data in this report is based on thousands of penetration tests and continuous scans across hundreds of organizations globally.

1. Risk Analytics

Edgescan employs advanced risk analytics to prioritize vulnerabilities based on the level of risk they pose to an organization. This helps in focusing remediation efforts on the most critical issues first.

2. Human Touch

In some cases, vulnerabilities cannot be validated or confirmed using automation. This may be due to complexity, the multi-step nature of the exploit or a business contextual exposure. Edgescan uses our team of experts to ensure high and critical severity vulnerabilities are real. There is nothing more disruptive than receiving a critical severity alert based on a false positive.

3. Data-Driven Decisions

By analyzing historical data and trends, Edgescan provides insights into the most common vulnerabilities and their impact. This data-driven approach helps organizations make informed decisions about their security posture.

4. Continuous Monitoring

Edgescan continuously monitors the security environment to identify new vulnerabilities and changes in the exposure landscape.

Smart Vulnerability Management™

Automated Validation

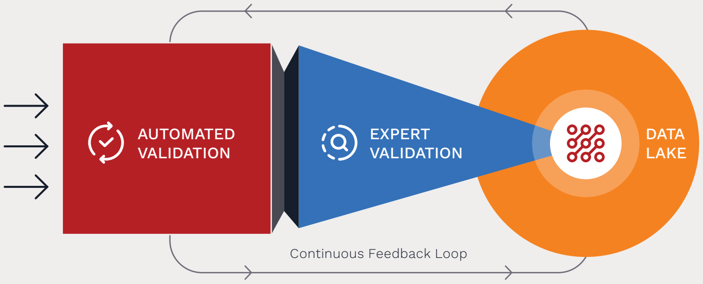
- Utilises **analytics to query millions of vulnerability examples** from data lake
- **Strong analytical models** determine if discovered vulnerability is a true positive
- Model then **determines if a vulnerability is real (automatically commit) or needs expert validation**

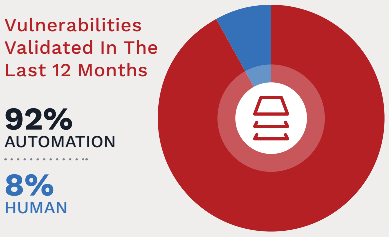
Expert Validation

- Required when a **vulnerability** is:
  - Critical or High Severity
  - PCI Fail, or
  - Confidence interval is outside the Edgescan Risk Parameters
- Validated by highly qualified experts **(OSCP/CREST Certified)**

Data Lake

- **True and false positives from both automated and expert validation** are fed into the data lake to **optimise automated validation accuracy**





Methodology

Edgescan was built to deliver an end-to-end, continuous testing and offensive security assessment platform.

VISIBILITY, COVERAGE, AND DEPTH

Our platform spans the full security lifecycle:

1. Asset Discovery and Visibility—via *Attack Surface Management (ASM)*

2. Vulnerability Scanning—using *Dynamic Application Security Testing (DAST)* and *Network Vulnerability Management (NVM)* across web applications, APIs, mobile apps, cloud, and network environments

3. Penetration Testing—full-scale testing of web applications, APIs, mobile applications, and infrastructure

Our philosophy is simple:

- **Speed and scale should not reduce accuracy**
- **Complexity should not limit coverage or depth**

Validation Process

Every vulnerability reported by Edgescan is validated by expert analysts. This eliminates false positives and significantly reduces noise, enabling teams to focus on what matters.

Data Scope

The statistics in this report are based on thousands of full-stack assessments. All findings are validated and prioritized using a proprietary data lake containing millions of triaged vulnerabilities, enhanced with human expertise where required.

Timeframe of Metrics

Vulnerability prioritization is dynamic and evolves as exploitability changes over time. The data presented reflects the threat landscape and prioritization logic as of the time this report was written.

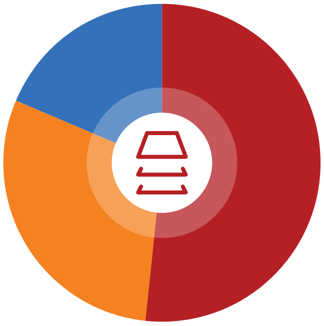
Detailed Insights

VULNERABILITY TYPES

47%
NETWORK / CLOUD

33%
WEB APPLICATION

20%
API



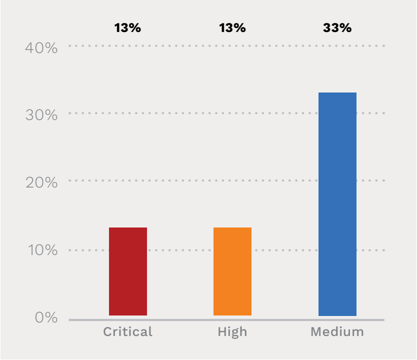
THE SPLIT ACROSS THE FULL STACK IS DEPICTED HERE WITH 47% OF DISCOVERED VULNERABILITIES LOCATED IN THE NETWORK/CLOUD LAYER.

33% OF VULNERABILITIES DISCOVERED EMANATE FROM THE WEB APPLICATION LAYER AND 20% FROM THE API LAYER.

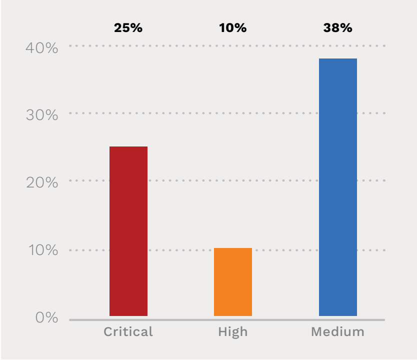
THIS SPLIT DEPICTS THE VULNERABILITY LANDSCAPE AND HENCE THE ATTACK SURFACE IS SPREAD ACROSS THE FULL STACK. FOCUS ON A SINGLE LAYER ALONE RESULTS IN POTENTIAL EXPOSURE POINTS WHICH CANT BE IGNORED.

SEVERITY BREAKDOWN

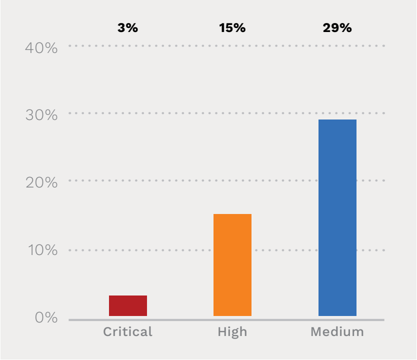
Full Stack



Web / API

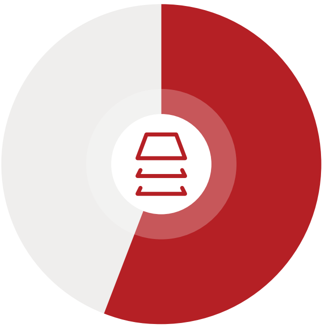


Network / Cloud



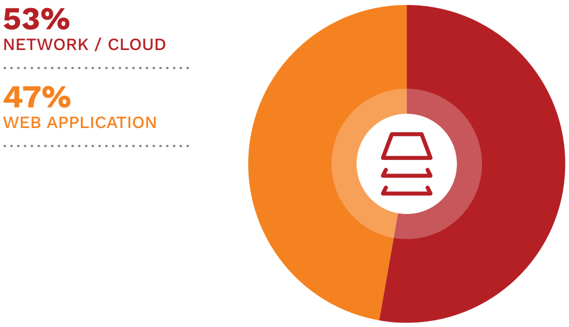
CLOSURE RATES

56%
CLOSURE RATE



56% OF VULNERABILITIES DISCOVERED WERE RETESTED AND VERIFIED AS CLOSED BETWEEN JANUARY AND JUNE 2025

FULL STACK VULNERABILITY DISPERSION

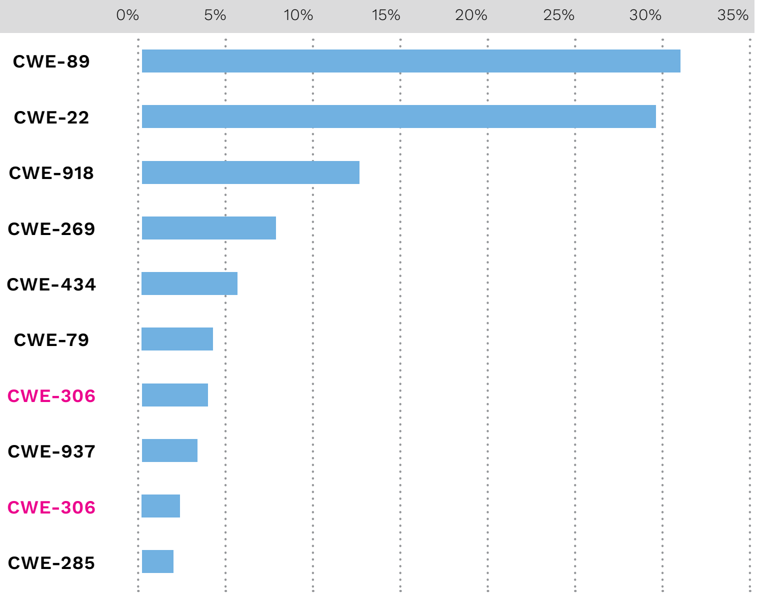


AS DISCUSSED PREVIOUSLY THE “LAYER 7” (WEB APPLICATION / API COMBINED) LAYER VERSUS THE CLOUD AND NETWORK LAYERS VULNERABILITY DISPERSION IS NEAR EQUAL.

A FULL STACK VIEW OF ONES ATTACK SURFACE IS KEY TO DISCOVERING EXPOSURES AND WEAKNESSES. PRIORITIZATION OF SUCH IS ALSO KEY AS WE CANT FIX ALL THE VULNERABILITIES. LEVERAGING FRAMEWORKS LIKE EPSS, CISA KEV COUPLED WITH ROBUST VALIDATION PROVIDE HUGE BENEFITS TO FOCUSING ON WHAT MATTERS.

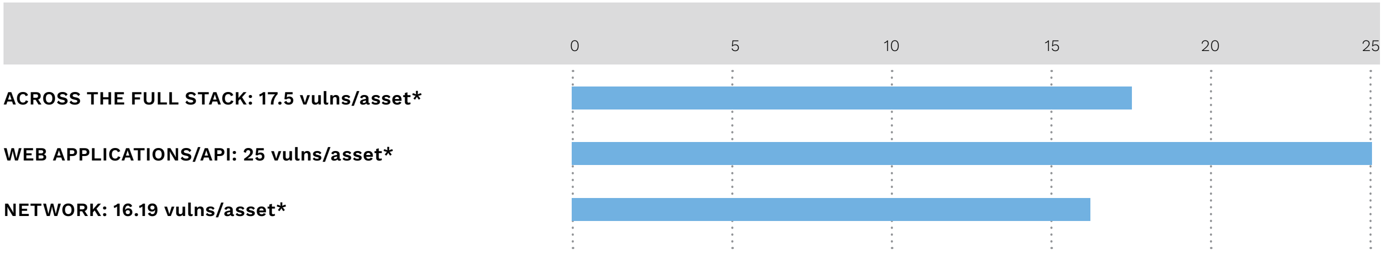
Most Common Critical Web Application Vulnerabilities Discovered

% of Total	CWE	Name
31.4%	CWE-89	SQL injection
29.6%	CWE-22	File Path Traversal
12.5%	CWE-918	Out-of-Band Resource Load
7.7%	CWE-269	Authorization Issue: IDOR/BOLA/Bypass
5.5%	CWE-434	Malicious / Arbitrary File Upload
4.09%	CWE-79	Cross-site Scripting (Stored)
3.8%	CWE-306	API Accessible without Authentication
3.18%	CWE-937	Vulnerable Software Detected
2.2%	CWE-306	Information Disclosure
1.8%	CWE-285	Unauthorized Admin Access



Full Stack Vulnerability Density

Average vulnerability count per asset.

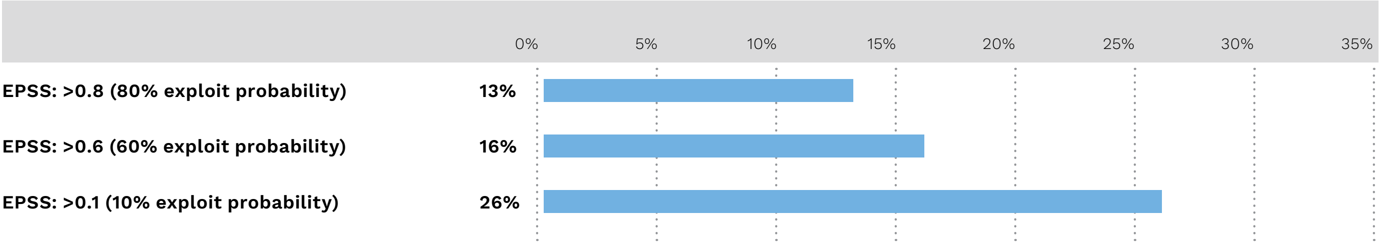


*Asset: An asset can be a web application, an API, a CIDR range, an IP range. IP/CIDR ranges can vary dramatically in size.

Exploit Prediction Security Score (EPSS)

EPSS (Exploit Prediction Scoring System) estimates the likelihood a software vulnerability will be exploited in the next 30 days (as per date of publication of this document) https://www.first.org/epss/

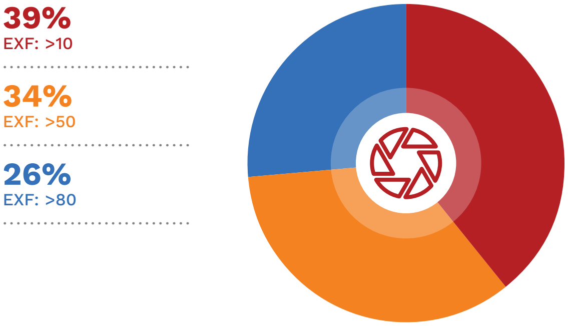
Percentage of vulnerabilities with an EPSS score within various probabilities of exploitation:



Percentage of vulnerabilities with EXF scores within specific bands

The Xposure Factor is determined through a blend of external scoring systems; Common Vulnerability Scoring System (CVSS), Exploit Prediction Scoring System (EPSS), CISA KEV. https://kb.edgescan.com/knowledge/what-is-edgescan-xposure-factor-exf

EDGESCAN EXPOSURE FACTOR



THE EXF SPLIT BETWEEN MEDIUM, HIGH AND CRITICAL VULNERABILITIES IS FAIRLY EVEN.

VULNERABILITIES WITH THE EXF >80 WOULD BE THE FIRST PORT OF CALL IN TERMS OF MITIGATION FOCUS.

TAKING INTO ACCOUNT THE CRITICALITY OF THE ASSET WHERE THE VULNERABILITY RESIDES IS ALSO KEY TO GOOD PRIORITIZATION.

What Is Edgescan

WHAT MAKES US TICK

Verified vulnerability intelligence

Real data. Actionable results.

During an assessment, the Edgescan validation engine queries millions of vulnerability examples stored in our data lake; our data is sourced from thousands of security assessments and penetration tests performed on millions of assets utilizing the Edgescan Platform. Vulnerability data is then run through our proprietary analytics models to determine if the vulnerability is a true positive. If it meets a certain numeric threshold it is released to the customer; we call this an auto-commit vulnerability.

If the confidence level falls below the threshold, the vulnerability is flagged for expert validation by an Edgescan security analyst. This hybrid process of automation and combined human intelligence is what differentiates us from scanning tools and legacy services providing real and actionable results.

Accurate data

Really accurate data.

Since 2015 Edgescan has annually produced the Vulnerability Statistics Report to provide a global snapshot of the overall state of cybersecurity using intelligence obtained from the Edgescan data lake.

This yearly report has become a reliable source for approximating the global state of vulnerability management and enterprises security postures. This is exemplified by our unique dataset being part of the Verizon Data Breach Report (DBIR), which is the de facto standard for insights into the common drivers for incidents and breaches today.

Happy customers

95% renewal rate.

Edgescan is a true white glove service that eliminates the need for tool configuration, deployment, and management. By providing vulnerability intelligence and remediation information along with human guidance and vulnerability verification, we help our customers prevent security breaches, safeguarding their data and IT assets.

Customer satisfaction is seen in our retention rate of 95% and the amazing product reviews on Gartner Peer Insights and G2, as well as our stellar customer testimonials.

> *"The accuracy that comes with human validation, paired with the efficiency of automatic, continuous scanning, means that my team now knows that whenever a vulnerability is flagged, the vulnerability is there, and they can continue working until they find it and fix it."*
>
> **CISO – Global Life Sciences Firm**

Edgescan Reviews

Customer First

by Edgescan in Application Security Testing

4.7 ★★★★★ 44 Ratings

The Edgescan Platform

ONE PLATFORM FOR CONTINUOUS TESTING AND EXPOSURE MANAGEMENT

Comprehensive visibility into your cyber footprint with continuous automated security testing, exposure management and Penetration Testing as a Service (PTaaS)

Enjoy Continuous Threat and Exposure Management (CTEM) – from visibility and scope to continuous testing, and prioritization to PTaaS.

- Discover assets requiring protection with Edgescan Attack Surface Management (ASM)
- Assess the "full stack" for vulnerabilities and exposures with intelligent human backed assessment (full stack vulnerability management) and penetration testing as a service (PTaaS)
- Enjoy 100% validated results using technology and human expertise
- Risk-based prioritization to improve remediation capability

Unified best-in-class testing across networks, APIs, web applications, and mobile applications to clearly understand and track your risk posture. Contextualize your organization's risk with false-positive free validated vulnerability intelligence, traditional scoring and reference systems for compliance, and Edgescan's proprietary validated risk and breach rating systems to prioritize the most important vulnerabilities first.

Full-stack continuous testing coupled with human expertise ensure you can have a true understanding of your attack surface, and the vulnerabilities within. Edgescan gives your team everything they need to maintain a proactive and robust, risk-based exposure management program.

Key features and benefits:

Edgescan AI Insights (New)
Designed to leverage GenAI technology to analyze your vulnerability data in real-time. Using vulnerability metrics it determines tactical and strategic activities designed to benefit your organization in relation to ransomware, remediation prioritization, compliance advice, training focus, exploitable vulnerabilities and anomalies across your estate.

Hybrid approach
Automated continuous testing and exposure management, risk of breach and proven exploits validated by experts, consultancy-grade penetration testing combining CREST, OSCP leading practice.

On-Demand and Unlimited Retesting
Retest any vulnerability, anytime without cost associated with traditional penetration testing offerings.

Unlimited Exposure Management
For both public and private network infrastructure, APIs, and web applications.

Validated Vulnerabilities
Near 100% accurate and false positive-free vulnerability and exposure intelligence verified by experts.

Consultancy-Grade Penetration Testing
Delivered as a service by certified security experts.

Edgescan eXposure Factor (EXF)
Leverage a combination of EPSS, CISA KEV and Edgescan expertise designed to prioritize vulnerability remediation.

Cloud-Based CTEM Platform
Near 100% accuracy coupled with expert remediation guidance and support from a team of OSCP, CREST and CEH certified penetration testers based in Europe and the USA.

Core Edgescan Products

THE EDGESCAN CTEM AND CONTINUOUS TESTING PLATFORM

Penetration Testing as a Service (PTaaS)

We started by addressing the limitations of traditional penetration testing by offering continuous security testing. Edgescan revolutionized the industry by on-demand penetration testing with unlimited retests, expert remediation guidance, proven exploits, validated risk, streamlined reports, and unlimited vulnerability assessments.

Dynamic Application Security Testing (DAST)

Recognizing the gaps in automated vulnerability scanning alone, we added a human layer to our service. This ensured our clients received accurate vulnerability risk, minimizing false positives and helping customers prioritize fixes with proven exploits.

Network Vulnerability Management (NVM)

The need for full-stack visibility became clear. Edgescan expanded into network vulnerability intelligence, offering a single validated source of the truth, for better prioritization and mitigation across the entire tech stack.

API Security Testing

As APIs became a major attack vector, clients demanded a better way to secure these assets. We added specialized API discovery and testing, giving customers vital protection for this increasingly critical component of the modern application.

Mobile Application Security Testing (MAST)

The explosion of mobile devices in enterprise environments meant security couldn't be neglected. Edgescan now includes comprehensive mobile application security testing to address the unique threats that mobile apps often present.

Attack Surface Management (ASM)

Proactive security requires real-time awareness of potential exposure points. We developed ASM to empower clients with continuous visibility into shadow IT and rogue assets. Newly discovered assets can be security tested immediately from the Edgescan Platform.

edgescan™

IRELAND | Unit 701 Northwest Business Park, Ballycoolin, Dublin 15, D15 CH26
UNITED STATES | 445 Park Avenue, 9th Floor, New York, NY 10022 030124