



2025

Vulnerability Statistics Report

10TH EDITION



Contents

Welcome & Synopsis	3
Year in Review	5
How does edgescan measure Security?	6
Vulnerability Severity	7
Risk Density – Full Stack	8
Risk Density – Network/Host	9
Risk Density – Application/API	10
Complex Web & API Vulnerabilities	11
Payment Card Industry (PCI) Failures	12
Vulnerabilities Discovered By Age	13
Public Facing Systems	14
Non Public Facing Systems	15
Known Exploited Vulnerabilities (CISA KEV)	16
Remediation Speed (MTTR)*	17
Remediation Speed by Industry	18
Vulnerability Backlog	19
Conclusion	20
What is Edgescan	21
The Edgescan Platform	22
Core Edgescan Products	23

***MTTR**

Mean Time to Remediation

Welcome & Synopsis

Welcome to the 10th edition of the Edgescan Vulnerability Stats Report 2025.

This report demonstrates the state of full stack security based on thousands of security assessments and penetration tests on millions of assets that were performed globally from the Edgescan Cybersecurity Platform in 2024.

This is an analysis of vulnerabilities detected in the systems of hundreds of organizations across a wide range of industries – from the Fortune 500 to medium and small businesses.

The report provides a statistical model of the most common weaknesses faced by organizations to enable data-driven decisions for managing risks and exposures more effectively.

We hope this report will provide a unique by-the-numbers insight into trends, statistics and a snapshot of the overall state of cybersecurity for the past year, from the perspective of vulnerabilities discovered and remediated, as well as penetration testing success rates.

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

This year we delve into quantification of attack surface management exposures & risks, Mean Time To Remediate (MTTR) critical vulnerabilities and also into Risk Density, to describe where critical severity vulnerabilities and exposures are clustered in the IT technical stack.

Our statistical models are split across layers of the technology stack (i.e. Full Stack), such as Web Application, API, and Device/Host layers.

Additionally, we make a distinction in the data, highlighting if discovered known vulnerabilities (CVEs) have associated exploit code freely available.

Unfortunately, we still see high rates of known (patchable) exploitable vulnerabilities, with working exploits in the wild being used by nation states and cyber criminal groups against organizations who are slow to patch.

As Edgescan employs a number of risk prioritization scoring mechanisms, we take a deeper look at the most common risks faced by organizations and also look at correlation of the various risk scoring methodologies.

Some of the results are surprising and we hope you will stay to the end to learn more!

Given Edgescan also maps validated vulnerabilities automatically to CVSS¹ (Common Vulnerability Scoring System), CISA KEV² (Cyber Security & Infrastructure Security Agency Known Exploited Vulnerability Catalogue), EPSS³ (Exploit Prediction Scoring System) and our own EVSS (Edgescan Validated Security Score), we have leveraged this information to provide a qualitatively better guide to what the most common risks are, as faced by modern enterprises.

CISA KNOWN EXPLOITED VULNERABILITIES (KEV) CATALOG CONTAINS 1,275 VULNERABILITIES. IN 2024, 320 WERE ADDED TO THE CISA KEV.

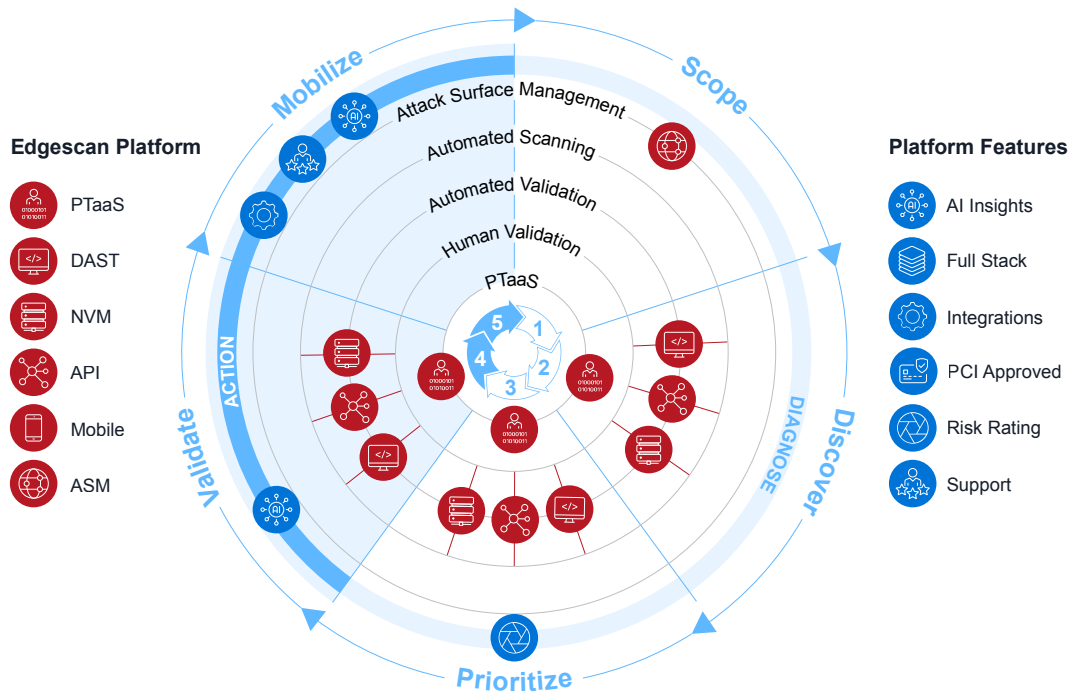
IN 2024, A RECORD-BREAKING 40,009 COMMON VULNERABILITIES AND EXPOSURES (CVEs) WERE PUBLISHED.

IN 2024, 768 CVEs WERE PUBLICLY REPORTED AS EXPLOITED FOR THE FIRST TIME IN THE WILD, 2% OF ALL DISCOVERED IN 2024 AND A 20% INCREASE ON 2023.

1. www.first.org/cvss/

2. www.cisa.gov/known-exploited-vulnerabilities

3. www.first.org/epss/



Statistically some vulnerabilities have a very low frequency of occurrence compared to the total number of vulnerabilities discovered, but many will result in a breach with an outsized impact, which we can call an intensive rather than extensive risk.

Looking at prioritization and risk models such as EPSS, CISA KEV, CVSS & SSVC*, they are very useful in an attempt to determine areas of focus, but they vary dramatically and can't be relied on individually.

For example, vulnerabilities may have a high CVSS score, a low EPSS score and a SSVC score of "Act", making it difficult to prioritize issues based on one scoring system alone.

Similarly to the 2024 report, patching and maintenance is a challenge and we still find that it is not trivial to patch production systems.

The MTTR (Mean Time to Remediation) statistics also reflect on this issue. Continuous detection and assessment needs improvement and as I've always said, visibility is paramount.

Internal (non-public) cyber security posture is significantly lacking in terms of resilience and ease of exploit. Combining vulnerabilities across the stack, often results in the potential impact being much more severe, than the sum of the individual discovered vulnerabilities.

Oddly, CVEs dating from 2015 are still being discovered and are being used by ransomware and malware toolkits, to exploit systems when found.

Attack Surface Management (Visibility) is a key driver to cybersecurity best practices. Based on our continuous asset profiling, we have observed how common it is that sensitive and critical systems are exposed to the public Internet.

The assumption here is that enterprises simply do not have systems, people and processes in place, to make them aware of exposures in a manner that facilitates remediation actions.

This report provides a global snapshot across dozens of industry verticals and how to prioritize what is important, as not all vulnerabilities are created equal.

Best regards,



Eoin Keary
Founder/CEO, Edgescan

*STAKEHOLDER-SPECIFIC VULNERABILITY CATEGORIZATION (SSVC)

<https://www.cisa.gov/stakeholder-specific-vulnerability-categorization-ssvc>

Year in Review

APPLICATION SPECIFIC VULNERABILITIES VS CVEs

Understanding the relationship between data breaches, Common Vulnerabilities and Exposures (CVEs), and application security vulnerabilities is crucial for effective cybersecurity strategies. Here is an overview based on available data.

Application Security Vulnerabilities and Data Breaches

In the 2024 Verizon Data Breach Investigations Report (DBIR), **vulnerability exploitation** was identified as the initial point of entry in **14% of all breaches**, marking a significant increase from previous years.

While the report does not specify the exact percentage of breaches directly linked to application security vulnerabilities, it highlights that **basic web application attacks** are among the top three patterns associated with data breaches.

The report emphasizes the critical need for organizations to address vulnerabilities promptly, as delays in patching can leave systems exposed to attacks.

Implementing robust security measures, conducting regular vulnerability assessments, and ensuring timely patch management are essential steps in mitigating the risk of breaches stemming from both application and infrastructure vulnerabilities.

Application breaches, often involving stolen credentials and vulnerabilities, accounted for 25% of all breaches in 2024 based on multiple sources.

CVEs and Data Breaches

Here is an overview based on available data.

- Application breaches, often involving stolen credentials and vulnerabilities, accounted for 25% of all breaches in 2024, based on multiple sources.
- As of 31st May 2024, approximately 6% of all published CVEs had been exploited in the wild
- The average CVSS score for CISA KEV listed vulnerabilities, was 8.4
- 53% of scored CVEs discovered in 2024 were of High and Critical Severity

Unpatched vulnerabilities, many of which are catalogued as CVEs, have been implicated in a significant number of data breaches. One report suggests that unpatched vulnerabilities were involved in 60% of data breaches.

Key Considerations

- **Exploitation Rates:** Not all CVEs are exploited in the wild. The exploitation rate is relatively low compared to the total number of published CVEs. However, when exploited, they can lead to significant security incidents.
- **Importance of Patching:** Unpatched vulnerabilities, whether they are application-specific or broader system flaws, pose substantial risks. Regularly updating and patching systems is essential to mitigate these threats.

This report is based on the dataset of all vulnerabilities found by the Edgescan platform in 2024.

<https://www.verizon.com/about/news/2024-data-breach-investigations-report-vulnerability-exploitation-boom>

<https://www.comparitech.com/blog/information-security/cybersecurity-vulnerability-statistics/>

<https://cvedata.com/>

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

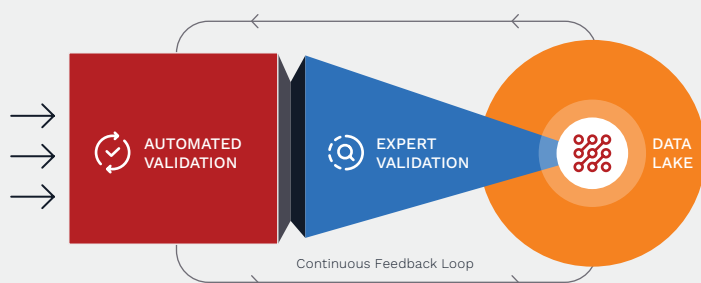
- Utilises **analytics** to query millions of **vulnerability examples** from data lake
- Strong analytical models** determine if discovered vulnerability is a true positive
- Model then **determines if a vulnerability is real (automatically commit) or needs expert validation**

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)

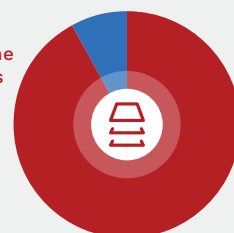
Data Lake

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



Vulnerabilities Validated In The Last 12 Months

92%
AUTOMATION
8%
HUMAN





Vulnerability Severity

EPSS, CISA KEV, EVSS & EXF

What is EPSS?

The Exploit Prediction Scoring System (EPSS) is an open, data-driven effort for estimating the likelihood (probability) that a software vulnerability will be exploited in the wild. The EPSS model produces a probability score between 0 and 1 (0 and 100%). The higher the score, the greater the probability that a vulnerability will be exploited.

<https://www.first.org/epss/>

What is CISA KEV?

CISA (Cybersecurity & Infrastructure Security Agency) maintains the authoritative source of vulnerabilities that have been exploited in the wild: the Known Exploited Vulnerability (KEV) catalog. CISA strongly recommends all organizations review and monitor the KEV catalog and prioritize remediation of the listed vulnerabilities to reduce the likelihood of compromise by known threat actors.

<https://www.cisa.gov/known-exploited-vulnerabilities>

Edgescan Validated Security Score (EVSS)

Every vulnerability discovered by Edgescan is validated via a combination of advanced “big-data” analytics and human expertise, resulting in near false positive-free vulnerability intelligence. Once a vulnerability is validated it is mapped to both the CISA KEV and EPSS to assist with prioritization. All vulnerabilities in Edgescan (where applicable) have an EPSS, CISA KEV, CVSS and EVSS risk score.

<https://www.edgescan.com/solutions/risk-based-vulnerability-management-rbvm/>

Edgescan eXposure Factor (EXF)

The Edgescan eXposure Factor combines EPSS, CVSS, CISA KEV and EVSS to reach a simple priority score which, taken in relevance with other vulnerabilities, provides a simple way to prioritize discovered and validated vulnerabilities.

<https://www.edgescan.com/edgescan-exposure-factor-exf/>

What is Stakeholder-Specific Vulnerability Categorization (SSVC)?

CISA uses its own SSVC decision tree model to prioritize relevant vulnerabilities into four possible decisions. Edgescan has mapped:

Track: The vulnerability does not require action at this time.

Track*: The vulnerability contains specific characteristics that may require closer monitoring for changes.

Attend: The vulnerability requires attention from the organization's internal, supervisory-level individuals.

Act: The vulnerability requires attention from the organization's internal, supervisory-level and leadership-level individuals.

<https://www.cisa.gov/stakeholder-specific-vulnerability-categorization-ssvc>

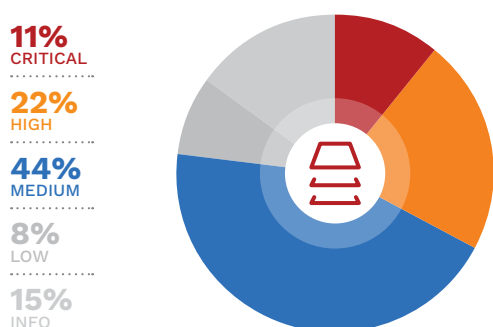
Risk Density

The following is a breakdown of vulnerabilities by severity, discovered across the full stack; Web Applications, APIs and Network/Host deployments.

It also depicts the risks associated with potential PCI (Payment Card Industry) failures – not every vulnerability results in a PCI fail.

Severity is defined via the Edgescan Validated Security Score (EVSS). Later in the report we draw upon CVSS, CISA KEV and EPSS Risk and Probability scores.

SEVERITY DISPERSION ACROSS THE FULL STACK (NETWORK, WEB, API COMBINED)



ACROSS THE FULL STACK MORE THAN 33% OF DISCOVERED VULNERABILITIES WERE OF A CRITICAL OR HIGH SEVERITY

SEVERITY IS BASED ON EDGESCAN EVSS (EDGESCAN VALIDATED VULNERABILITY SCORE)

EVSS IS APPLIED TO WEB APPLICATION VULNERABILITIES AND IS BASED UPON LIKELIHOOD & IMPACT WHEN A VULNERABILITY IS UNDERGOING VALIDATION, ADDRESSING QUESTIONS SUCH AS EXPLOITABILITY, IMPACT AND LIKELIHOOD

How EVSS Works

1. Automated Scanning: The platform continuously scans your digital assets for vulnerabilities using various tools and techniques.

2. Data Science & Human Validation: Analytics is used to estimate the confidence interval of a vulnerability and whether it is a true or false positive. This is based on comparison with millions of previously validated vulnerabilities to get an accurate estimate. Security experts review the automated findings, specifically High and Critical Severity issues, to eliminate false positives and ensure accuracy.

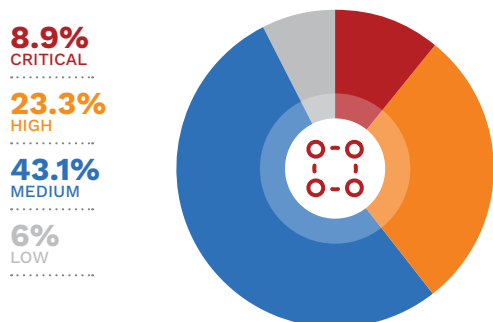
3. Risk-Based Data: Each vulnerability is assessed using multiple risk-based data points, including:

- **EPSS (Exploit Prediction Scoring System):** Predicts the likelihood of a vulnerability being exploited
- **CISA KEV (Known Exploited Vulnerability catalogue):** Identifies vulnerabilities that are known to be exploited in the wild
- **CVSS (Common Vulnerability Scoring System):** Provides a standardized severity score
- **EXF:** The above scores are combined and weighted to produce the Edgescan eXposure Factor (EXF) to assist with prioritization decisions

Benefits of EVSS

- **Prioritization:** Helps you focus on the most critical vulnerabilities first, improving your security posture efficiently
- **Accuracy:** Reduces the noise of false positives, allowing your team to concentrate on real threats
- **Efficiency:** Speeds up the remediation process by providing clear, actionable intelligence
- **Comprehensive Coverage:** Integrates with various security solutions to offer full-stack vulnerability management

NETWORK/HOST VULNERABILITY DISPERSION BY SEVERITY



32.2% OF DISCOVERED VULNERABILITIES IN THE INFRASTRUCTURE/HOSTING/CLOUD/NETWORK LAYER WERE OF A CRITICAL OR HIGH SEVERITY

19% HAD AN EPSS SCORE ABOVE 0.8 (PROBABILITY OF BREACH EXCEEDING 80%)

EPSS SCORES ARE DYNAMIC AND CHANGE OVER TIME. THE EPSS SCORES DEPICTED ARE AT TIME OF PUBLICATION (10TH JANUARY 2025)

The most common vulnerabilities with an EPSS score above 0.7 are listed here

OPEN SSL/CRYPTOGRAPHIC ISSUES REMAIN THE MOST COMMON

CVE	Vulnerability Name	Avg EPSS Score	On CISA KEV	SSVC Score	CVSS Score	*Exploit Code Available	Percentage of total above 0.7
CVE-2014-0224	OpenSSL 'ChangeCipherSpec' MITM Vulnerability	0.97539	Yes	Act	7.4	Yes	18.09
CVE-2023-44487	Eclipse Jetty HTTP/2 Protocol DoS Vulnerability (CVE-2023-44487) - Windows	0.8009	Yes	Act	7.5	Yes	6.73
CVE-2020-5377	Dell EMC OpenManage Server Administrator < 9.3.0.2, 9.4.x < 9.4.0.2 Directory Traversal Vulnerability (DSA-2020-172)	0.81873	No	Track	9.1	Yes	3.46
CVE-2020-9484	Apache Tomcat RCE Vulnerability (May 2020) - Windows	0.93186	Yes	Act	9.8	Yes	2.42
CVE-2020-1938	Apache Tomcat Multiple Vulnerabilities (Feb 2020) - Windows	0.97406	Yes	Act	7.5	Yes	2.16
CVE-2020-1147	Microsoft .NET Framework Multiple Vulnerabilities (KB4578969)	0.921	Yes	Act	7.8	Yes	1.83
CVE-2024-8926	PHP < 8.1.29, 8.2.x < 8.2.20, 8.3.x < 8.3.8 Multiple Vulnerabilities - Windows	0.95382	No	Track	9.8	Yes	1.76
CVE-2019-0232	Apache Tomcat RCE Vulnerability (Apr 2019) - Windows	0.97365	Yes	Act	9.8	Yes	1.7

Breach Probability	Dispersion
EPSS > 0.8 (>80%)	11%
EPSS 0.6 - 0.79 (60%-79%)	13%
EPSS 0.1-0.59 (10% - 59%)	7%
EPSS below < 0.1 (10%)	69%

*EXPLOIT CODE AVAILABLE

Addresses the question "Does code exist which is freely available on the public Internet?"

Searches of popular sites such as <https://github.com>, <https://www.exploit-db.com>, <https://vuldb.com>, <http://0day.today>, to assess if code to exploit a weakness can be easily obtained and used.

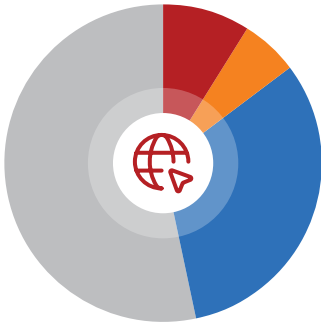
WEB APPLICATION & API (LAYER 7) VULNERABILITY DISPERSION BY SEVERITY

9%
CRITICAL

5.8%
HIGH

32%
MEDIUM

53.2%
LOW

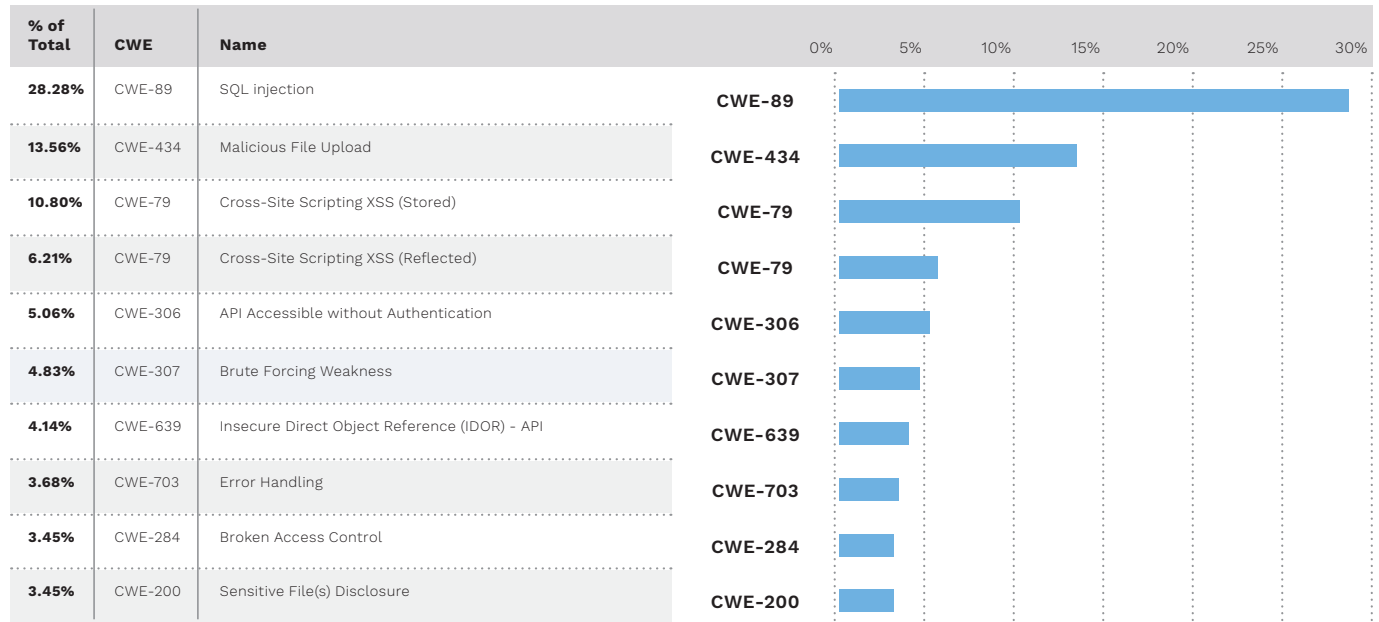


ACROSS THE WEB APPLICATION AND API LAYERS 14.8% OF DISCOVERED VULNERABILITIES WERE OF A CRITICAL OR HIGH SEVERITY. AS DEPICTED LATER IN THIS DOCUMENT CRITICAL AND HIGH SEVERITY VULNERABILITIES REMAIN VERY SIMILAR TO PREVIOUS YEARS

VULNERABILITIES SUCH AS SQL INJECTION (CWE-89) ARE READILY DISCOVERED AND ACCOUNT FOR 19.52% OF ALL CRITICAL AND HIGH SEVERITY VULNERABILITIES

VULNERABILITIES SUCH AS MALICIOUS FILE UPLOAD ARE NOT TESTED ADEQUATELY USING AUTOMATION AND ARE FREQUENTLY OVERLOOKED BY SCANNING SOLUTIONS DUE TO THE RISKS ASSOCIATED WITH SUCH TEST CASES

The Top 10 – High & Critical Severity



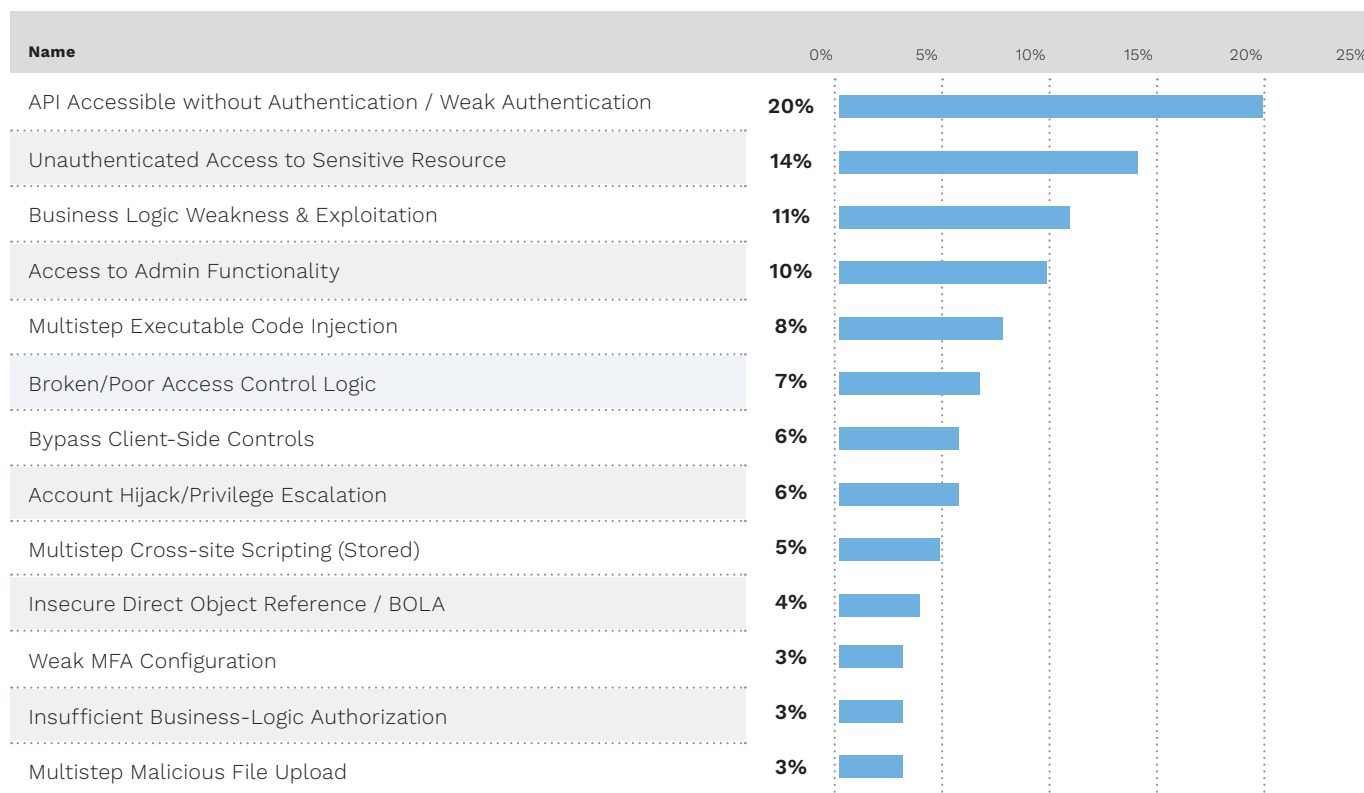
The Top 10 depicts the most common Critical and High Severity issues discovered by Edgescan over the past year. SQL Injection is still the main contender (as was in the 2024 report), which is interesting to note as we can easily develop code (or block vectors) to mitigate such attacks. Detection of such vulnerabilities is also trivial using the correct techniques.

Something which is overlooked quite frequently is "malicious file upload" at 9.37% of all High and Critical Severity vulnerabilities discovered. This can give rise to ransomware, malware and internal network breach pivot points for attackers.

API security weaknesses are also significant with Authentication and IDOR issues at 5% and 2.9% respectively.

Complex Web & API Vulnerabilities

MOST COMMON CRITICAL SEVERITY VULNERABILITIES DISCOVERED USING PTAAS* – NOT TYPICALLY FOUND USING AUTOMATION ALONE



Automated vs Hybrid web application security assessments

Automated scanning is a powerful approach for identifying vulnerabilities in software systems, but it has limitations:

- Firstly, automated scanners rely on predefined rules and signatures, which means they can miss novel or unique vulnerabilities that have not been documented yet.
- Secondly, these tools often struggle with complex logic flaws or business logic vulnerabilities that require human intuition and understanding to detect.

- Additionally, automated scans may not fully cover all aspects of a system, especially if the system is highly customized or uses obscure technologies.
- False positives and false negatives are also common, leading to either missed vulnerabilities or unnecessary alerts. Moreover, automated tools cannot assess the context or impact of a vulnerability in the same way a skilled security professional can.

Finally, attackers are constantly evolving their techniques, and automated tools may lag behind in recognizing new methods of exploitation.

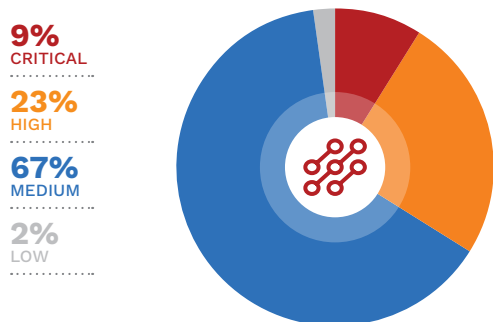
Therefore, while automation is a valuable component of a comprehensive security strategy, it should be complemented by manual reviews and expert analysis to ensure thorough vulnerability detection.

*PTAAS

Penetration Testing as a Service

Payment Card Industry (PCI) Failures

PCI Failures By Severity – Issues which will result in a failed compliance scan. PCI affected assets must pass 4 quarterly scans per year in order to be compliant with the PCI Data Security Standard (PCI DSS).



32% OF PCI FAILURES WERE OF HIGH & CRITICAL SEVERITY

RESEARCH INDICATES THAT MANY PCI FAILURES HAVE A VERY LOW CHANCE OF BEING EXPLOITED GIVEN THEY ARE NOT ON THE CISA KEV AND HAVE A LOW EPSS SCORE, ALBEIT THEY RESULT IN A PCI DSS COMPLIANCE FAIL

Most Common PCI Fails

Vulnerability Name	% of All PCI Fails	CVEs	On CISA KEV	EPSS	SSVC Score	*Exploit Code Available	CVSS	Risk (EVSS)
Prefix Truncation Attacks in SSH Specification (Terrapin Attack)	4.66	CVE-2023-48795	Yes	0.85	Act	Yes	5.9	3
TLS Version 1.0 Protocol Detection	3.50	CVE-2013-0169	Yes	0.02	Track	Yes	6.5	3
OpenBSD OpenSSH < 9.6 Multiple Vulnerabilities	3.46	CVE-2023-48795, CVE-2023-51384, CVE-2023-51385	No	0.85	Track	Yes	6.5	3
TLS Version 1.1 Protocol Detection	3.34	CVE-2013-0169	No	0.02	Track	Yes	6.5	3
Windows IExpress Untrusted Search Path Vulnerability	2.67	CVE-2018-0598	No	0.21	Track	No	7.8	4
Microsoft Windows HID Functionality Code Execution Vulnerability	2.67	CVE-2011-0638	No	0.06	Track	Yes	6.9	3
OpenBSD OpenSSH <= 9.6 Authentication Bypass Vulnerability	2.65	CVE-2023-51767	No	0.05	Track	No	7	4
Server Message Block (SMB) Protocol Version 1 Enabled	2.33	CVE-2020-1301	Yes	.02	Act	Yes	8.8	4
SSL/TLS: Weak Cipher Suites	1.97	CVE-2013-2566, CVE-2015-2808, CVE-2015-4000	Yes	0.056	Track	Yes	5.9	3

Highest EPSS	CVE
97%	CVE-2020-1938
97%	CVE-2014-0224
60%	CVE-2023-42795, CVE-2023- 44487, CVE-2023-45648
98%	CVE-2023-48795, CVE-2023-51384, CVE-2023-51385

*EXPLOIT CODE AVAILABLE

Addresses the question "Does code exist which is freely available on the public Internet?"

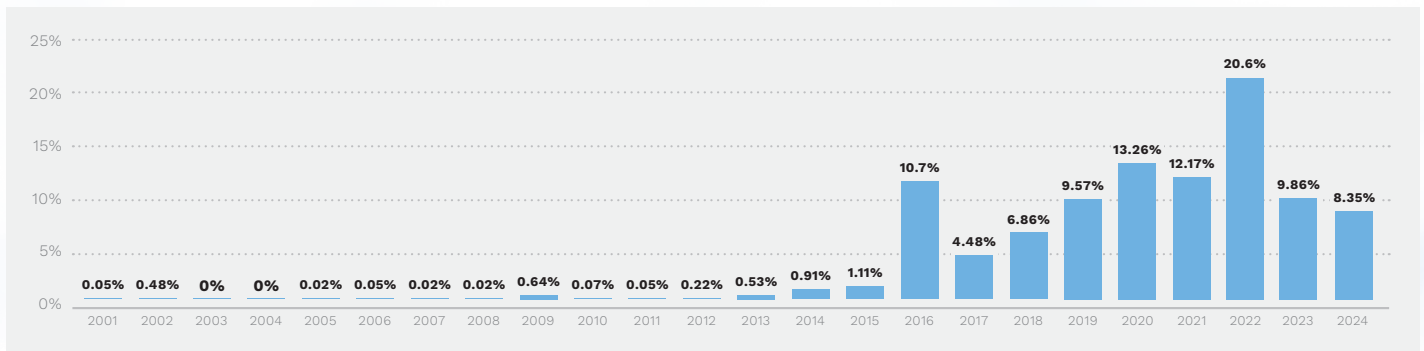
Searches of popular sites such as <https://github.com>, <https://www.exploit-db.com>, <https://vuldb.com>, <http://0day.today>, to assess if code to exploit a weakness can be easily obtained and used.

Vulnerabilities Discovered By Age

AGE DISPERSION OF VALIDATED KNOWN VULNERABILITIES (CVEs) PER YEAR

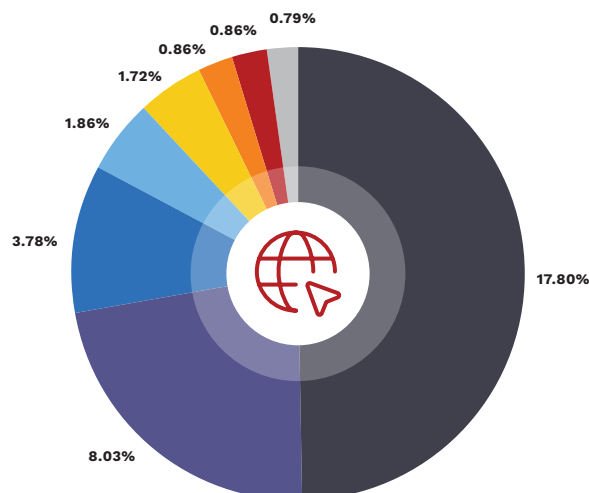
Common Vulnerabilities and Exposures (CVEs) are public disclosures of security vulnerabilities in software. Each CVE is assigned a unique number along with the year that it was disclosed. The below graph shows known vulnerabilities that were found across systems in 2024, organised by the age of when that CVE was first discovered.

CVEs Discovered by Age



Public Facing Systems

MOST COMMON HIGH AND CRITICAL SEVERITY CVEs DISCOVERED IN INTERNET-FACING SYSTEMS



Name	CVE(s)	EPSS	EVSS	On CISA KEV	CVSS (3.1) Base Score	SSVC Score	*Exploit code Available?	% of all High and Critical Severity
SSL 64-bit Block Size Cipher Suites Supported (SWEET32)	CVE-2016-2183	0.03984	4	Yes	7.5	Act	Yes	17.80%
OpenBSD OpenSSH <= 9.6 Authentication Bypass Vulnerability	CVE-2023-51767	0.00042	4	No	7.0	Track	No	8.03%
Exim <= 4.96.2 libspf2 RCE Vulnerability (Sep 2023)	CVE-2023-42118	0.00065	4	No	7.5	Attend	Yes	3.78%
Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSH, D(HE)ater)	CVE-2002-20001	0.01824	4	No	7.5	Track	Yes	1.86%
OpenBSD OpenSSH < 9.3p2 RCE Vulnerability	CVE-2023-38408	0.04294	5	Yes	9.8	Act	Yes	1.72%
Ivanti Endpoint Manager Mobile (EPMM) Multiple Vulnerabilities (Jul 2024)	CVE-2024-36130, CVE-2024-36131, CVE-2024-36132, CVE-2024-34788	0.00091	5	No	9.8	Attend/Track*	No	0.86%
OpenSSH 6.2 <= 8.7 Privilege Escalation Vulnerability	CVE-2021-41617	0.0005	4	Yes	7.0	Track	Yes	0.86%
OpenSSH <= 8.6 Command Injection Vulnerability	CVE-2020-15778	0.00587	4	Yes	7.8	Track	Yes	0.79%

CISA KEV

CISA KEV depicts if the vulnerability is listed on the Known Exploit catalogue managed by the Cyber Security and Infrastructure Agency (CISA)

<https://www.cisa.gov/>

EPSS

EPSS is the Exploit probability based on first.org data.

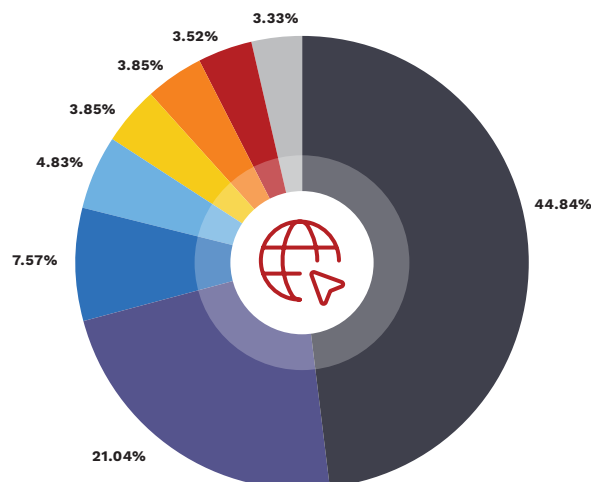
*EXPLOIT CODE AVAILABLE

Addresses the question "Does code exist which is freely available on the public Internet?"

Searches of popular sites such as <https://github.com>, <https://www.exploit-db.com>, <https://vuldb.com>, <http://0day.today>, to assess if code to exploit a weakness can be easily obtained and used.

Non Public Facing Systems

MOST COMMON HIGH AND CRITICAL SEVERITY CVEs DISCOVERED IN NON INTERNET-FACING SYSTEMS



Name	CVE(s)	EPSS	EVSS	On CISA KEV	CVSS (3.1) Base Score	SSVC Score	*Exploit code Available?	% of all High and Critical Severity
SSL 64-bit Block Size Cipher Suites Supported (SWEET32)	CVE-2016-2183	0.03984	4	Yes	7.5	Act	Yes	44.84%
SNMP Agent Default Community Names	CVE-1999-0517	0.45448	4	No	7.0	–	Yes	21.04%
Windows IExpress Untrusted Search Path Vulnerability	CVE-2018-0598	0.21443	4	No	7.8	Track	No	7.57%
Microsoft Malware Protection Engine Denial of Service Vulnerability (Apr 2023)	CVE-2023-24860	0.0006	4	No	7.5	Attend	No	4.83%
Trellix / McAfee Endpoint Security < 10.6.1 Build 2113, 10.7.x < 10.7.0 Build 2000 Multiple Vulnerabilities	CVE-2020-7319	0.0006	4	No	8.8	Track	No	3.85%
Trellix Endpoint Security < 10.7.0 Build 6149 Code Injection Vulnerability	CVE-2023-3665	0.0006	4	No	7.8	Track	No	3.85%
OpenSSL 'ChangeCipherSpec' MITM Vulnerability	CVE-2014-0224	0.97539	4	Yes	7.4	Act	Yes	3.52%
SUSE: Security Advisory (SUSE-SU-2022:4240-1)	CVE-2022-43995	0.00042	4	No	7.1	Track	No	3.33%

CISA KEV

CISA KEV depicts if the vulnerability is listed on the Known Exploit catalogue managed by the Cyber Security and Infrastructure Agency (CISA)

<https://www.cisa.gov/>

EPSS

EPSS is the Exploit probability based on first.org data.

*EXPLOIT CODE AVAILABLE





















Addresses the question "Does code exist which is freely available on the public Internet?"

Searches of popular sites such as <https://github.com>, <https://www.exploit-db.com>, <https://vuldb.com>, <http://0day.today>, to assess if code to exploit a weakness can be easily obtained and used.

Known Exploited Vulnerabilities (CISA KEV)

At the end of 2024, the Cybersecurity & Infrastructure Security Agency Known Exploited Vulnerabilities (CISA KEV) catalog contained a total of **1,238 vulnerabilities**. 185 vulnerabilities were added in 2024.

CISA KEV VULNERABILITY DISPERSION BY VENDOR

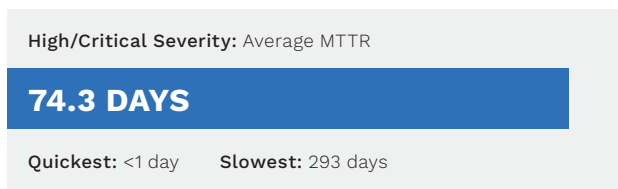
 Microsoft 321	 Apple 79	 CISCO 75	 Adobe 74	 Google 60
 Oracle 39	 Apache 36	 Vmware 26	 Ivanti 24	 D-Link 20
 Linux 18	 Citrix 16	 Fortinet 16	 Palo Alto Networks 13	 Android 13
 Atlassian 13	 SonicWall 12	 Zykel 12	 Mozilla 12	 Samsung 11

Remediation Speed (MTTR)

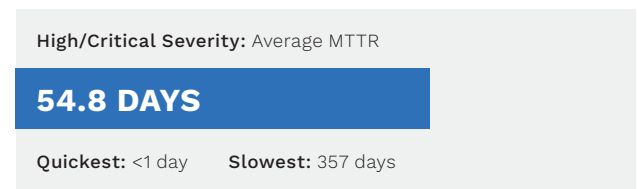
MEAN TIME TO REMEDIATE (MTTR)

MTTR measures how quickly a vulnerability can be remediated and validated as such, after it is first detected. It provides insights into the efficiency of remediation processes and an organisations ability to bounce back from incidents. A lower MTTR indicates faster recovery and better system reliability.

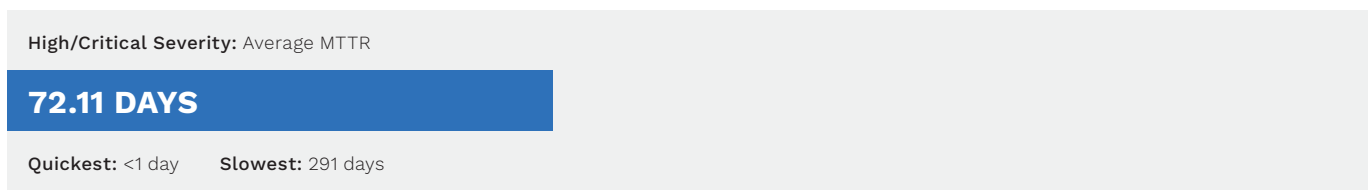
Application/API Vulnerabilities



Device/Network Vulnerabilities



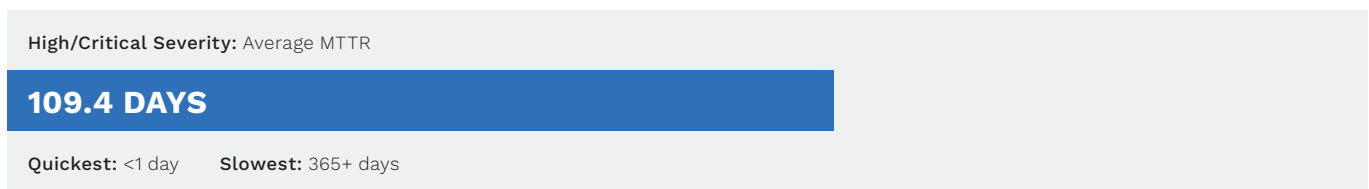
PCI Failures Across the Full Stack



Vulnerabilities EPSS >0.7 (70%)



Vulnerabilities EPSS <0.1 (10%)



It is clear, prioritization of vulnerabilities is not strictly based on EPSS, CISA KEV or SSVC scoring, but more heavily weighted to traditional CVSS scores. This is understandable as many compliance frameworks and traditional ways to measure the priority of a vulnerability is based on CVSS.

We expect to see a shift to exploit prediction score combined with other contextual information such as; if exploit code is available, is it actively tracked by government agencies, or other contextual metrics. CVSS is a rather "blunt instrument", albeit a good place to start in terms of measuring potential impact of a vulnerability.

Remediation Speed by Industry

During 2024 we examined 14 different industries to report on their average rates of MTTR within that vertical. We can see that the shortest MTTR can be seen in **Software**, at **63 days**, while the longest is the **Construction** industry, at **104 days**.



Vulnerability Backlog

A Vulnerability Backlog is the percentage of unclosed vulnerabilities an organization has within a 12 month period. This is typical of all organizations and most professionals agree that fixing all vulnerabilities is not a wise use of resources, nor practical. Prioritization of risk is now more important than ever – fix what matters.

17.4%

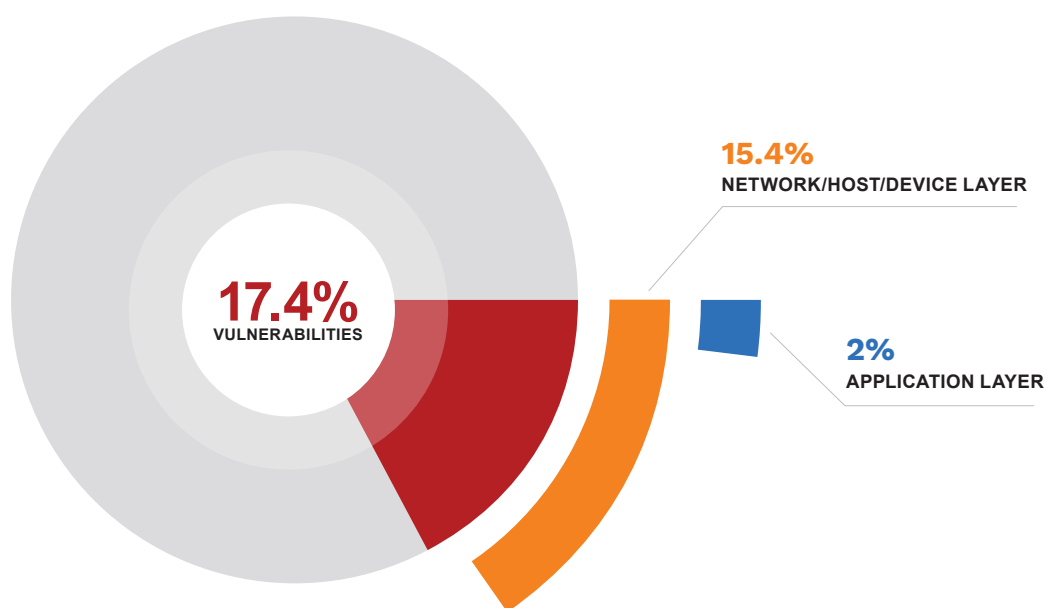
OF VULNERABILITIES IN AN ENTERPRISE'S BACKLOG ARE EITHER HIGH OR CRITICAL SEVERITY

15.4%

OF WHICH ARE ATTRIBUTED TO THE NETWORK/HOST/DEVICE LAYER

2%

OF WHICH ARE IN THE APPLICATION LAYER



For larger enterprises (1000+ employees), on average, 45.4% of vulnerabilities discovered in a 12 month period remain open – they have not been remediated.

It appears closure of web application and API vulnerabilities is more consistent, given the majority of high and critical severity vulnerabilities on average in a vulnerability backlog reside in the network/host/device layer.

Conclusion

THE VULNERABILITIES DISCOVERED WHICH SUPPORT THIS REPORT, DO NOT DRAMATICALLY DIFFER TO PREVIOUS YEARS.

What is changing however, is the approach to prioritization and discovery. Implementing a proactive approach, which includes Attack Surface Management (ASM) combined with continuous assessment and deep testing (PTaaS) on critical assets, helps one discover and detect more rapidly.

The ability to quickly and continuously map an organisations landscape, discover assets and exposures and act appropriately, is a bare minimum requirement. With the rise of powerful AI tools, the speed at which exploitation occurs, is only ever going to increase.

The most common critical and high severity vulnerabilities are well established, and can be detected using a combination of technology, along with deep assessments that utilize penetration testing (PTaaS) solutions. Deep testing to discover logical vulnerabilities is certainly becoming more automated, but still requires an experienced human “behind the wheel” for now.

Such vulnerabilities are being exploited by cyber criminals and ransomware groups, resulting in complex chained attacks, business compromise and headaches overall. Defending an organisation is asymmetric warfare, the attacker always has the advantage. For the defender, continuous vigilance and focus on what is important, is key to success.

Prioritization is evolving and a combination of EPSS, SSVC, CVSS & CISA KEV to name a few, can help focus on what matters. The scoring and values, albeit measuring different aspects of exposure, can give organisations a better grounding on what to focus on. Priority is also a function of what is being protected and how important the exposed asset is to the organisation. Accuracy of vulnerability intelligence is a cornerstone of a successful process (something edgescan was built on). This in turn feeds priority decisions and downstream activities.

Without accuracy, prioritization can amplify “white noise” which results in wasting an organisations time and resources, chasing false positives, and generating “ghost” critical alerts – a key contributor to alert fatigue!

It is of paramount importance that continuous assessment and robust prioritization approaches are implemented. We cannot fix all the vulnerabilities discovered all the time. And all vulnerabilities are not created equal.

Leveraging AI to process vulnerability data and discover anomalies is very powerful. In addition to vulnerability priority, anomaly detection can help with strategic decisions and preventative security activities.

For a successful cybersecurity programme the following must be implemented:

1. Understand your landscape, exposed services and attack surface
2. Have the ability to monitor change and act as the landscape changes
3. Be able to continuously assess your landscape for exposures and weaknesses with accuracy
4. Prioritize discovered validated vulnerabilities, such to focus on what matters
5. Have the ability to retest and validate quickly, to closeout discovered issues
6. Leverage continuous assessment and AI to generate trending metrics and detect anomalies
7. Rinse and Repeat

ASM

Attack Surface Management

PTAAS

Penetration Testing as a Service

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 EDGECAN 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 (EASM)

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.



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

edgescan.com | Copyright© 2025 Edgescan.
All rights reserved.