

The 2021 Verizon DBIR Edgescan Analysis



DBIR

2021 Data Breach Investigations Report

Intro

The 2021 Verizon Data Breach Investigations Report (DBIR) was recently released and it is a great snapshot of the information security ecosystem as a whole.

A portion of the report covers **Web Application Hacking** and **System intrusion**, both which Edgescan provides **protection** against by continuous detection and **vulnerability intelligence**.

Edgescan is a noted contributor (amongst many others) to the DBIR. We've provided curated vulnerability data for the last 3 years to the report.

Our team analyzed the DBIR report and compared with the Edgescan 2021 Vulnerability Stats Report.

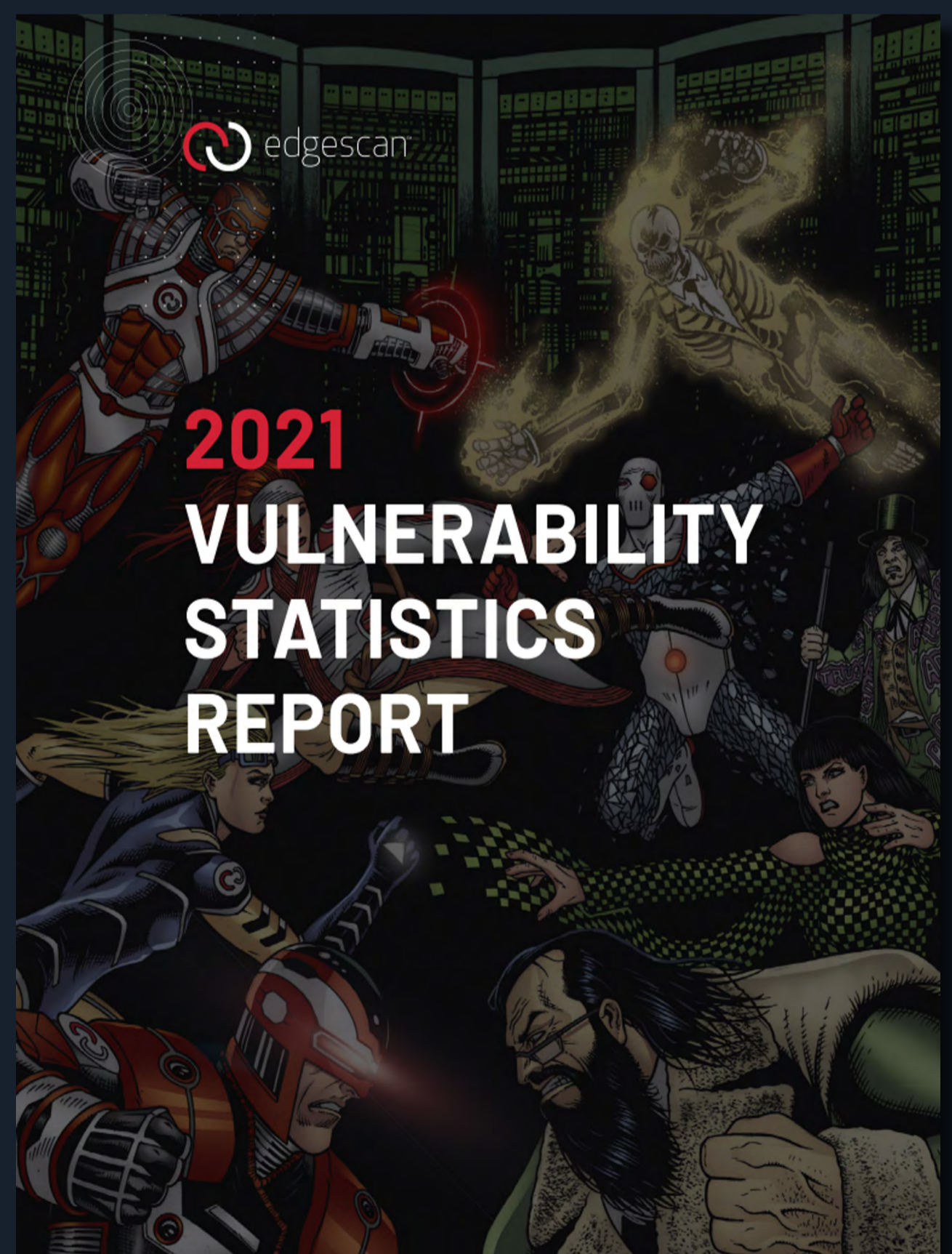
"We're pretty happy to see so much correlations between the statistical models and have taken the liberty to put our spin on this industry leading document, The Verizon DBIR report..."

Verizon DBIR 2021:

<https://www.verizon.com/business/resources/reports/dbir/>

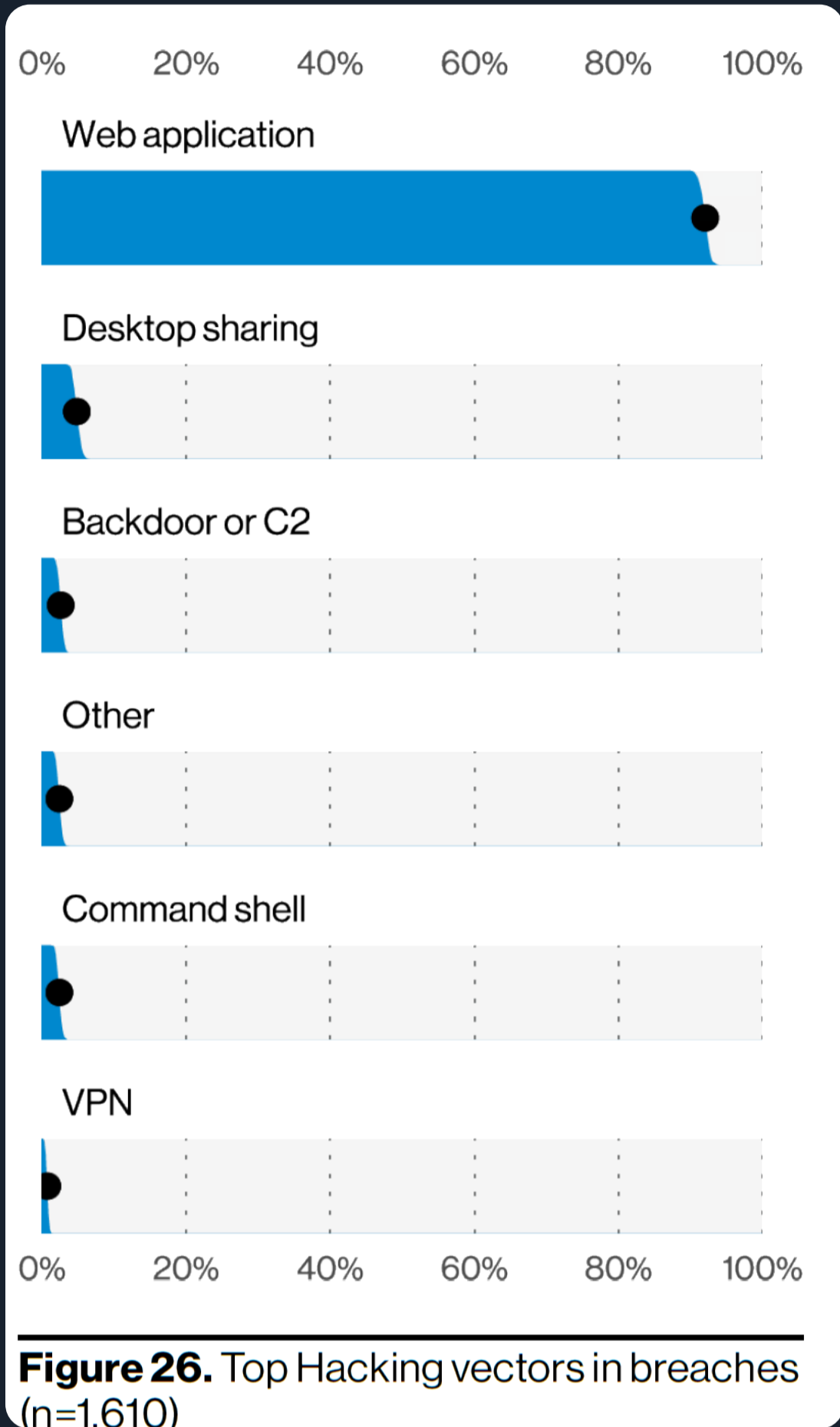
Edgescan Vuln Stats 2021:

<https://info.edgescan.com/vulnerability-stats-report-2021>





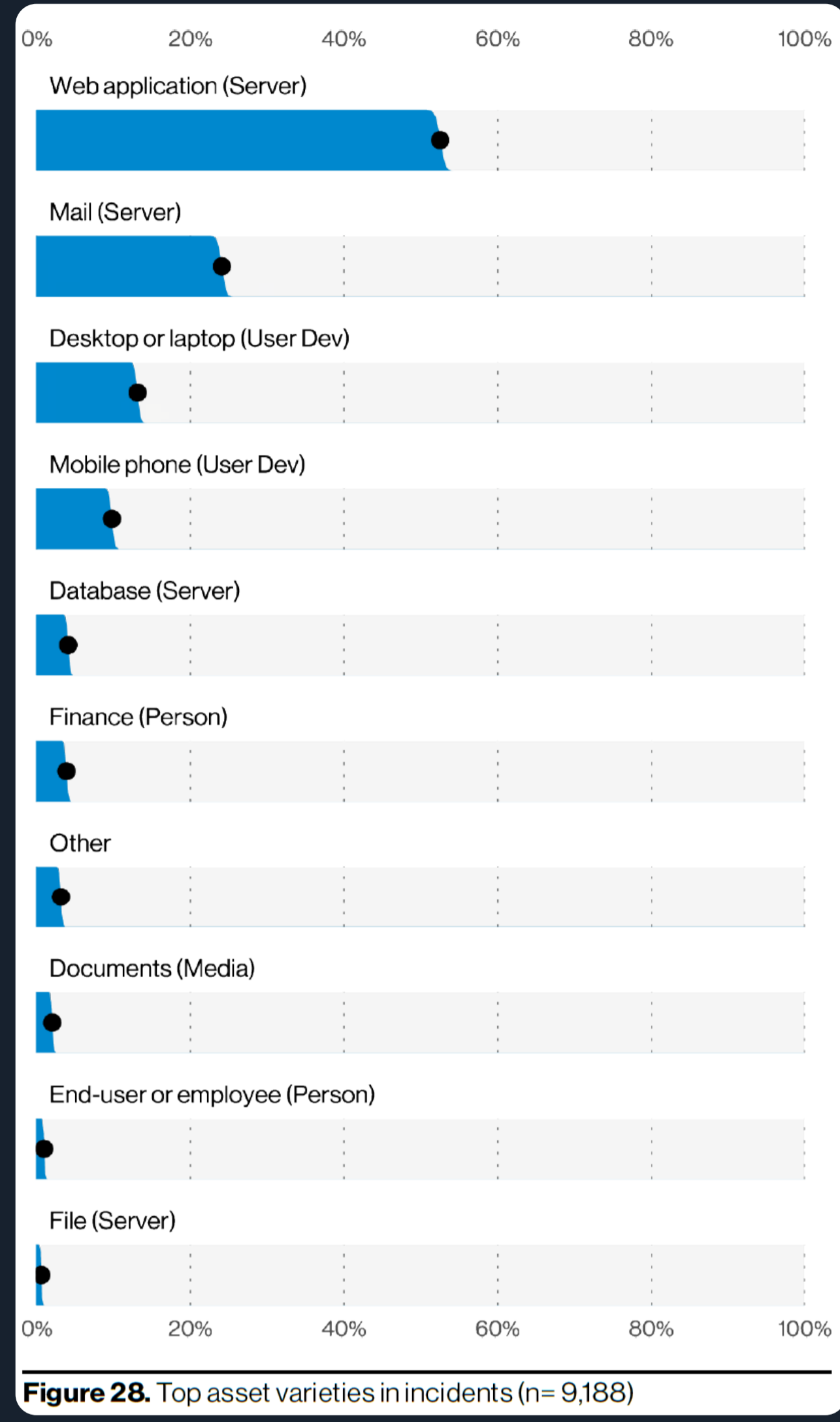
Top Targets



Web applications are top targets. Desktop sharing attacks have increased which aligns to the 2021 Edgescan Stats report.

“...60% of the Ransomware cases involving direct install or installation through desktop sharing apps...”

Edgescan sees a similar trend such that the majority of initial attack steps involve hacking to gain unauthorized access. Once a system is compromised malware etc. can be deployed...



“...Servers are still dominating the Asset landscape due to the prevalence of web apps and mail services involved in incidents...”

Edgescan’s data correlates with this...Internet facing web applications still have a significantly higher Risk Density, with 32% of vulnerabilities discovered rated as High or Critical Risk whilst Internet facing servers and hosts have a risk density of 21%

Don't sweat the zero days, focus on the basics.

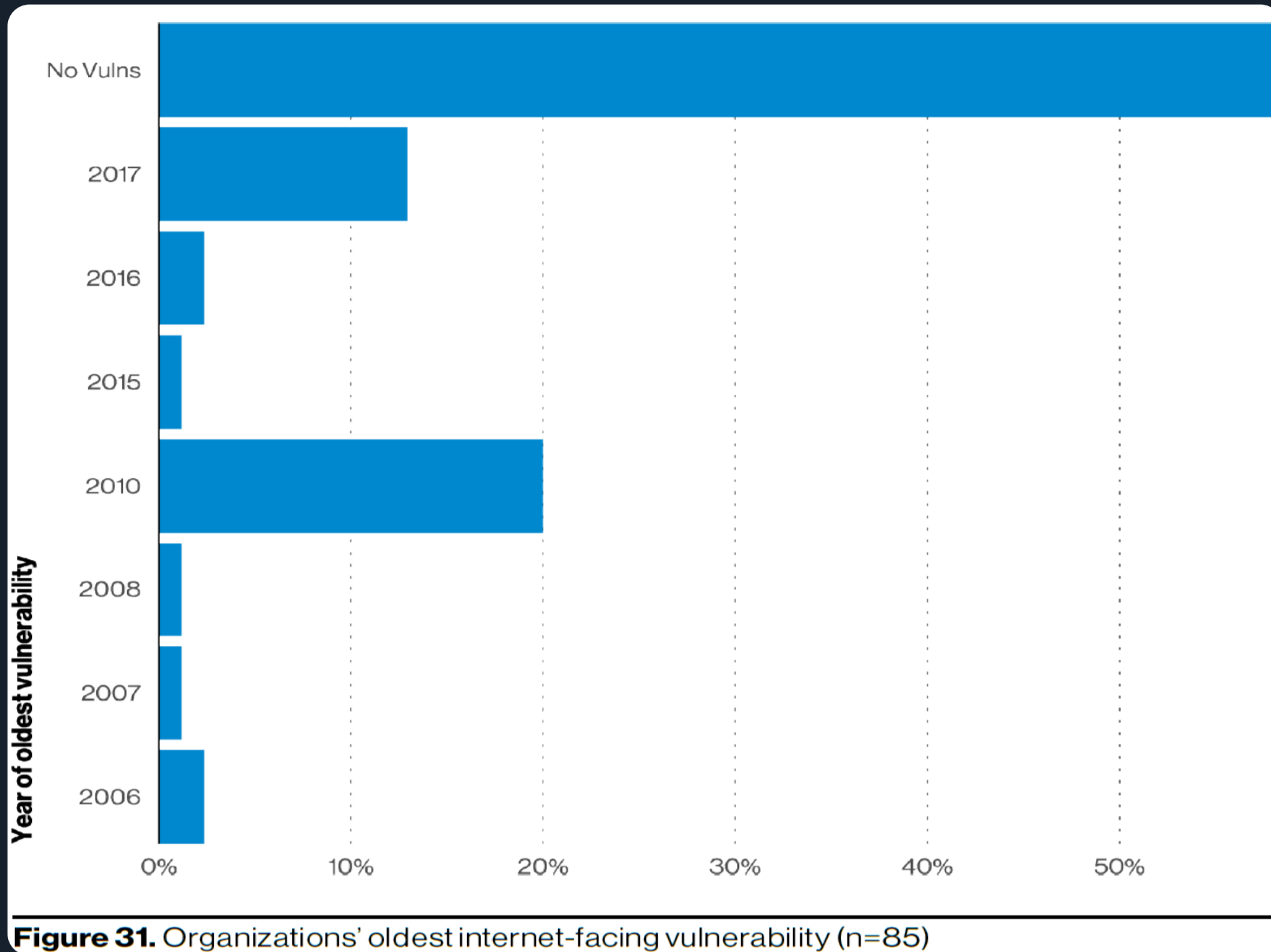
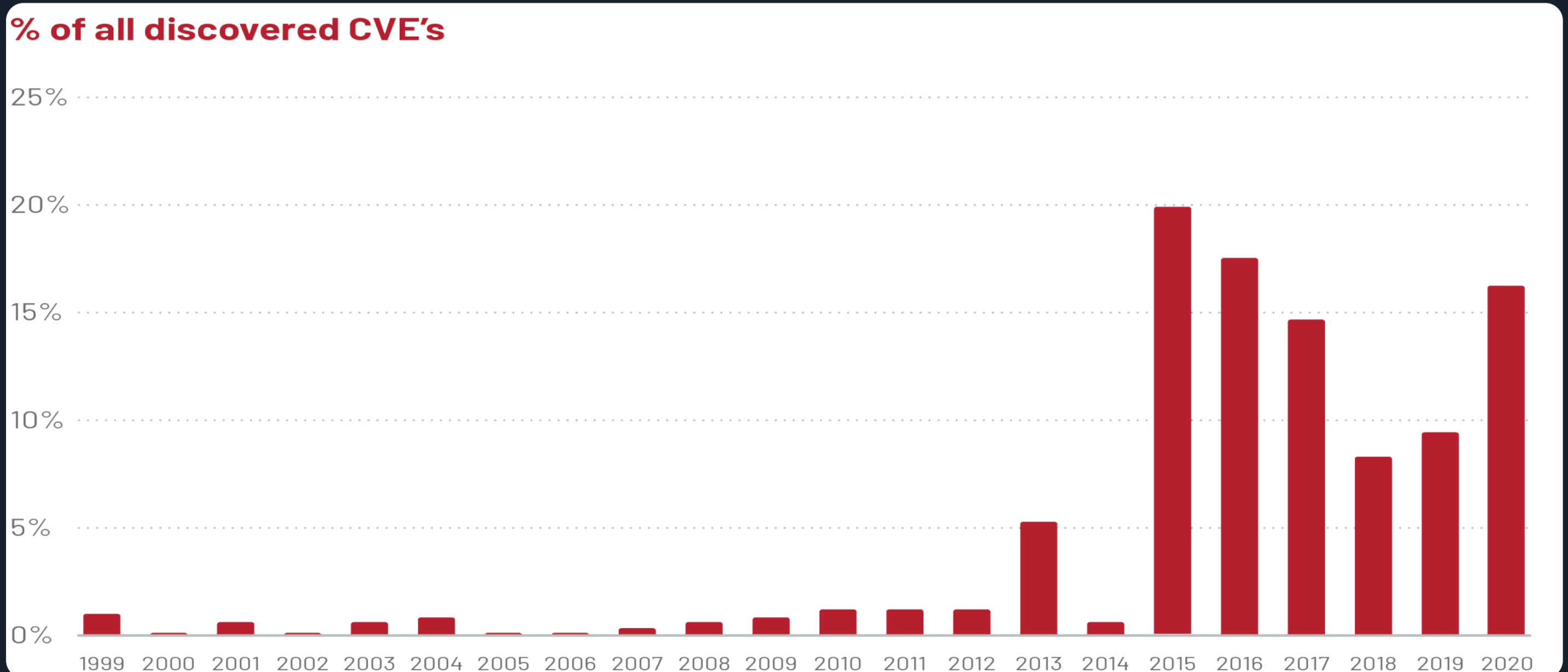


Figure 31. Organizations' oldest internet-facing vulnerability (n=85)

“...However, as we saw last year, it is actually the older vulnerabilities that are leading the way..”

Older vulnerabilities lead the pack. 20% of internet facing vulnerabilities are 11 years old.

Edgescan also has observed this trend over previous years...The most common malware toolkits are using older vulnerabilities very successfully.



Malware/Ransomware has become a huge issue. Hacking as a first step is not uncommon

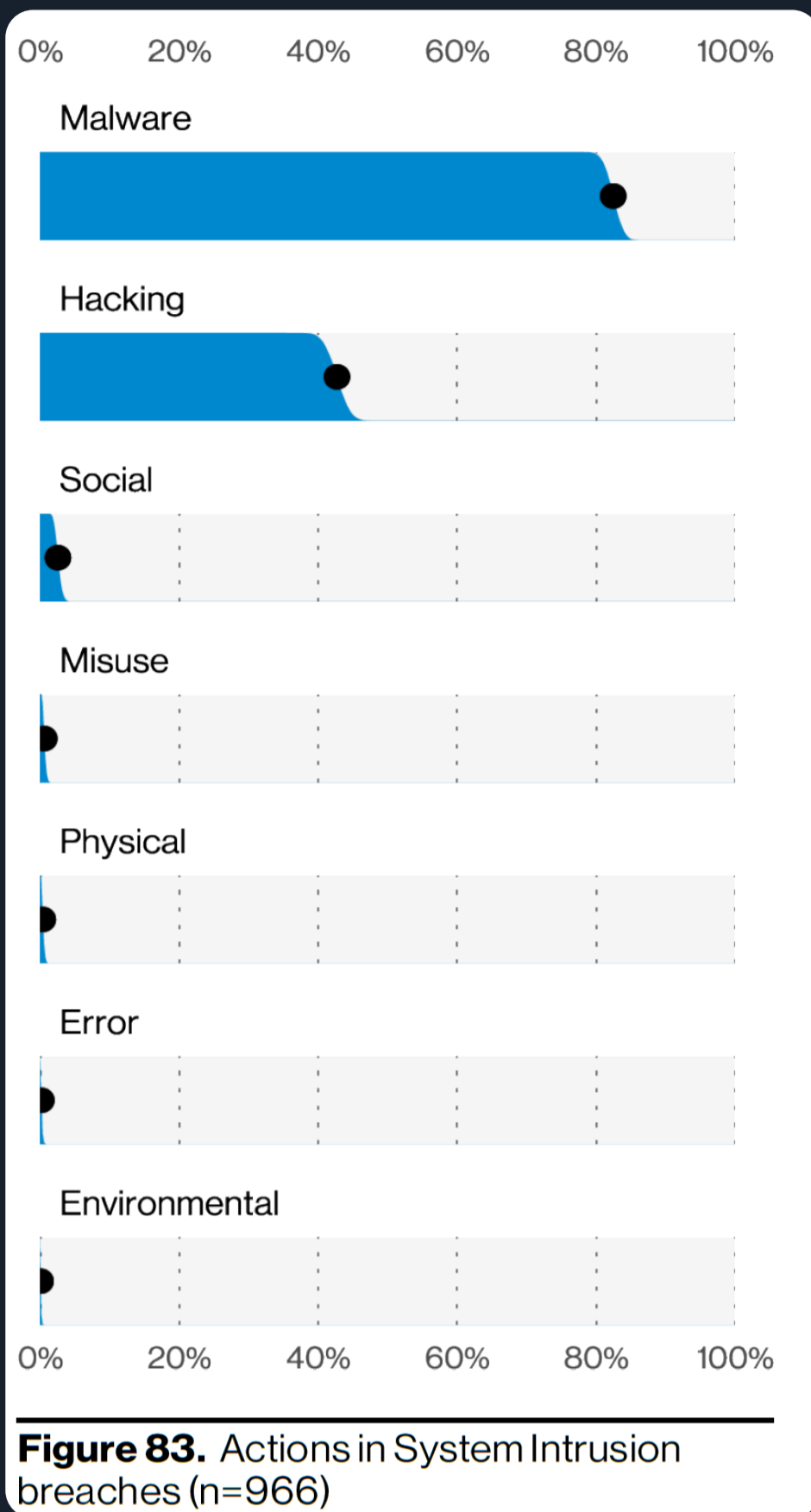


Figure 83. Actions in System Intrusion breaches (n=966)

“...As we have pointed out in previous reports, Credentials remain one of the most sought-after data types....”

- Finance, Healthcare, Information Technology, Professional Services were the most common industry verticals subject to **web application breach**
- Manufacturing, Professional Services, and Healthcare were the most common verticals subject to **system intrusion** (complex full stack attacks)
- **Web application attacks** and **system intrusion** were the most common variants in top patterns associated with breach in nearly all **industry verticals**

“...The majority of Web App hacking attacks used stolen credentials. “Credential Stuffing” was a very common attack vector against web applications....” - Theft of credentials is due to web hacking and system intrusion patterns..

“The most common system intrusion was via malware (>70%) followed by Hacking (>40%).....

.....the Actor will be focused on repurposing the web app for malware distribution, defacement or installing malware for future DDoS attacks.....

....30% of the malware was directly installed by the actor, 23% was sent there by email and 20% was dropped from a web application.

....it does highlight the importance of having a robust defense to cover these three major entry paths for Malware...”

“...80% of basic Web application attacks resulted in credential compromise
100% of the attacks were external Threat actors...”

“...7.8% of organizations attempted to download at least one piece of known Ransomware last year...”

“...Attackers are less likely to purely target Payment data and are more likely to broadly target any data that will impact the victim organization’s operations.

This will increase the likelihood that the organization will pay up in a Ransomware incident...”

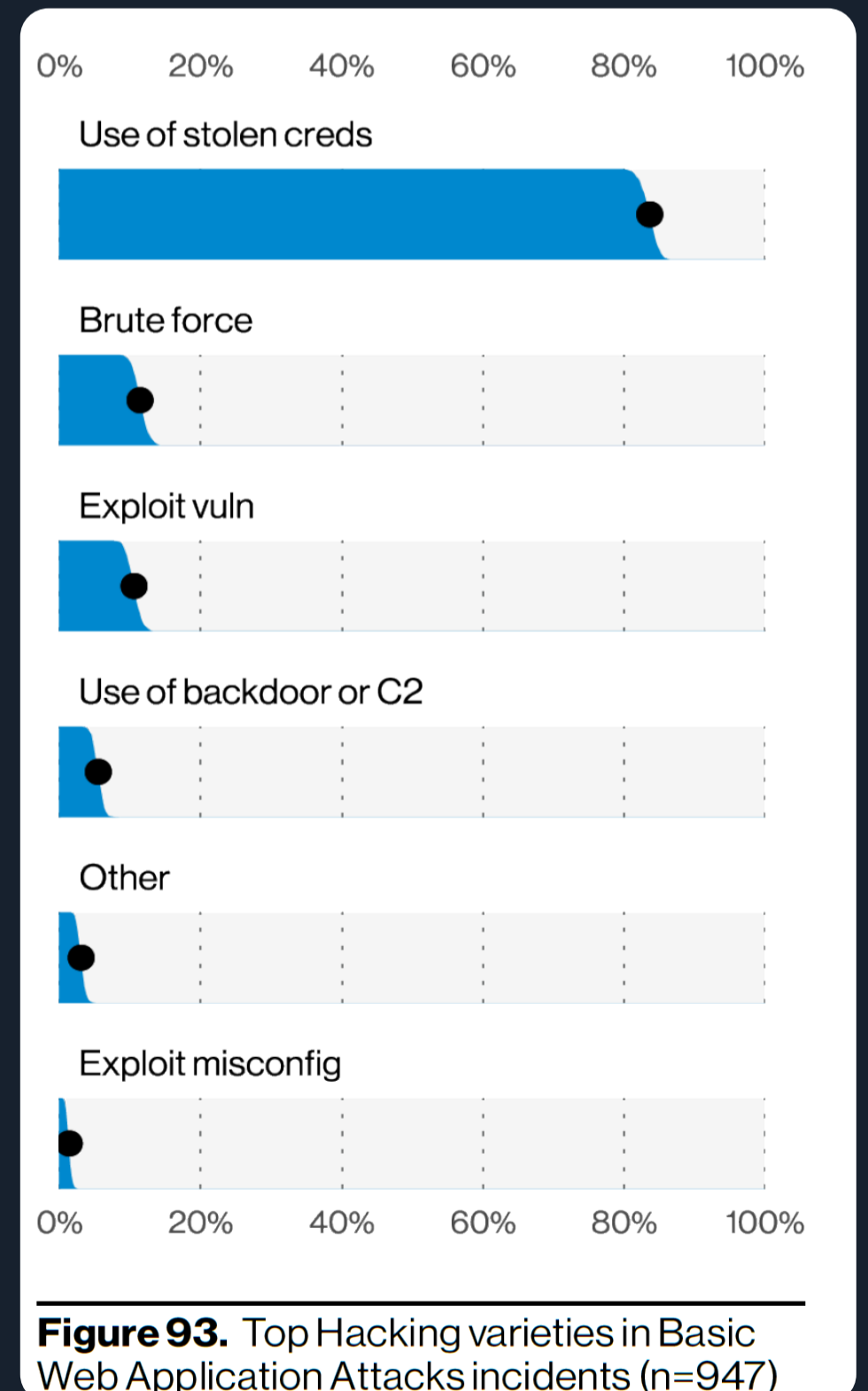


Figure 93. Top Hacking varieties in Basic Web Application Attacks incidents (n=947)

What is Edgescan?

Application Security

- Continuous Application/API vulnerability assessment.
- Pentesting as a Service. (PTaaS)
- API Security assessment and Pentesting.
- Alerting and integration

Host Security

- Continuous External /Internal Vulnerability Assessment.
- Pentesting as a Service (PTaaS).
- Alerting and integration

Continuous Monitoring

- Live system and service 24/7 discovery
- Alerting and integration
- Exposed service alerting

API Discovery

- Continuous API discovery and enumeration.
- Eliminate blind spots
- Alerting and integration

What does Edgescan do?

Simply, we detect & validate cyber vulnerabilities in your IT systems Web, Network, API, CI/CD, IoT, Internal, external – fullstack! We provide continuous visibility to help you maintain security.

We provide on-demand Pen Testing as a Service (PTaaS)

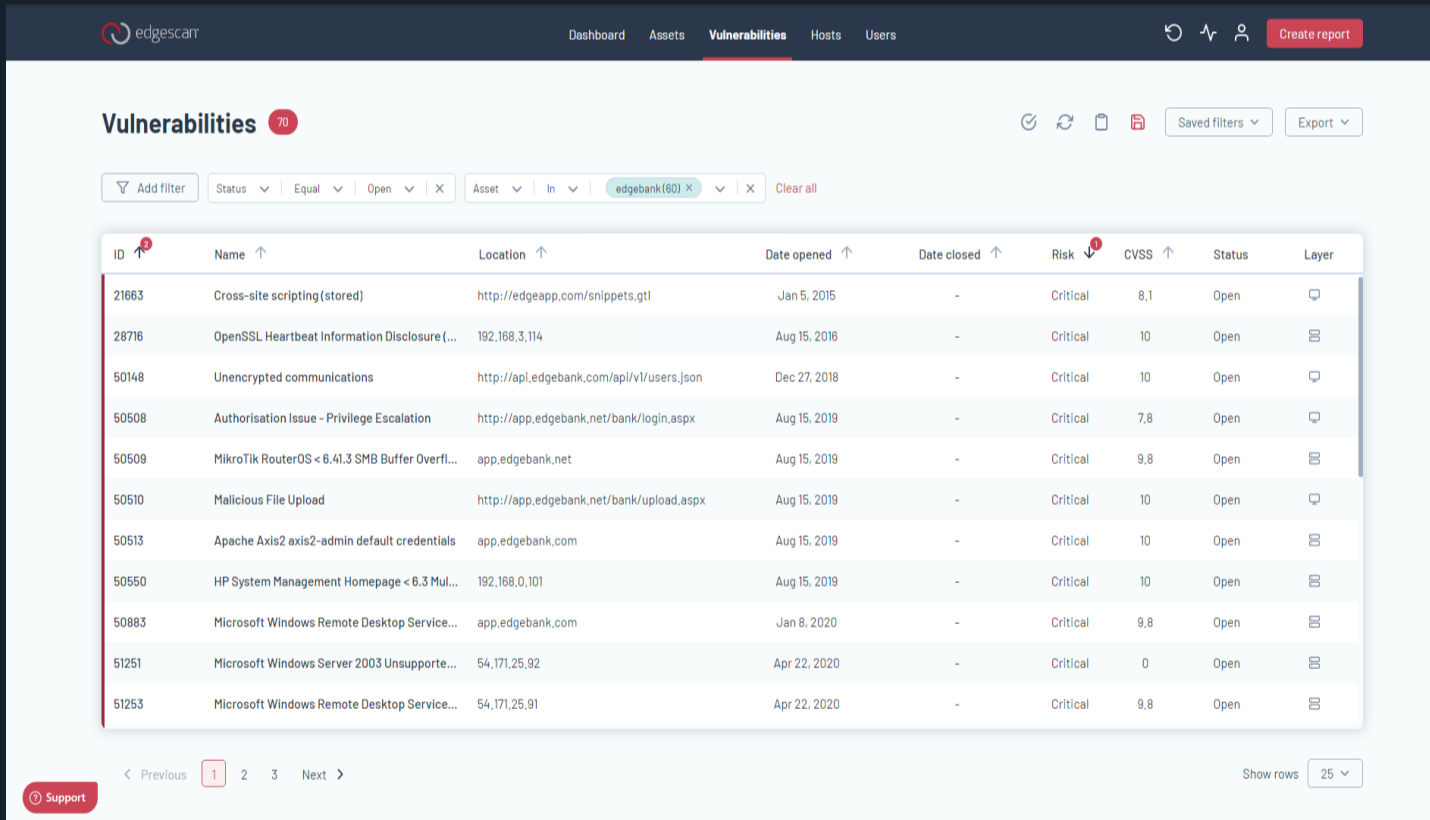
Why should I use Edgescan?

We deliver a dedicated vulnerability detection solution (SaaS). We're extremely accurate and provide support to guide you through your journey.

We deliver a comprehensive and cost effective solution.

We're PCI Approved Scanning Vendors.

- Fullstack coverage
- Validated by experts
- Mitigation Support
- On-demand



ID	Name	Location	Date opened	Date closed	Risk	CVSS	Status	Layer
21863	Cross-site scripting(stored)	http://edgeapp.com/snippets.gtl	Jan 5, 2015	-	Critical	8.1	Open	
28776	OpenSSL Heartbeat Information Disclosure L...	192.168.3.114	Aug 15, 2018	-	Critical	10	Open	
50148	Unencrypted communications	http://api.edgescan.com/api/v1/users.json	Dec 27, 2018	-	Critical	10	Open	
50508	Authorisation Issue - Privilege Escalation	http://app.edgescan.net/bank/login.aspx	Aug 15, 2019	-	Critical	7.8	Open	
50509	Mikrotik RouterOS < 6.43.3 SMB Buffer Overfl...	app.edgescan.net	Aug 15, 2019	-	Critical	9.8	Open	
50510	Malicious File Upload	http://app.edgescan.net/bank/upload.aspx	Aug 15, 2019	-	Critical	10	Open	
50513	Apache Axis2 axis2-admin default credentials	app.edgescan.com	Aug 15, 2019	-	Critical	10	Open	
50550	HP System Management Homepage < 6.3 Mul...	192.168.0.101	Aug 15, 2019	-	Critical	10	Open	
50883	Microsoft Windows Remote Desktop Service...	app.edgescan.com	Jan 8, 2020	-	Critical	9.8	Open	
51251	Microsoft Windows Server 2003 Unsupporte...	54.171.25.92	Apr 22, 2020	-	Critical	0	Open	
51253	Microsoft Windows Remote Desktop Service...	54.171.25.91	Apr 22, 2020	-	Critical	9.8	Open	

40%

Reduce Mean Time To Remediation (MTTR) by 40%

2.1+

Save on average the equivalent of 2.1 full time staff members per month using Edgescan

What is Edgescan?

What's different?

- All vulnerabilities are validated for accuracy and risk.
- We're a fullstack cyber SaaS (Web applications and Network security).
- We support our clients to help understand and fix with our certified penetration testing team.
- We can scale to thousands of assessments.
- Fixed monthly fee, unlimited assessments.

What are the main features?

- Continuous fullstack security testing
- Automatic assessments of new endpoints as they are discovered
- Validation and support for all issues discovered
- Continuous asset and API monitoring and detection
- Internal and External Assessments
- On-demand assessments and penetration testing.
- Alerting and Integration customizable for you.

Does this help me?

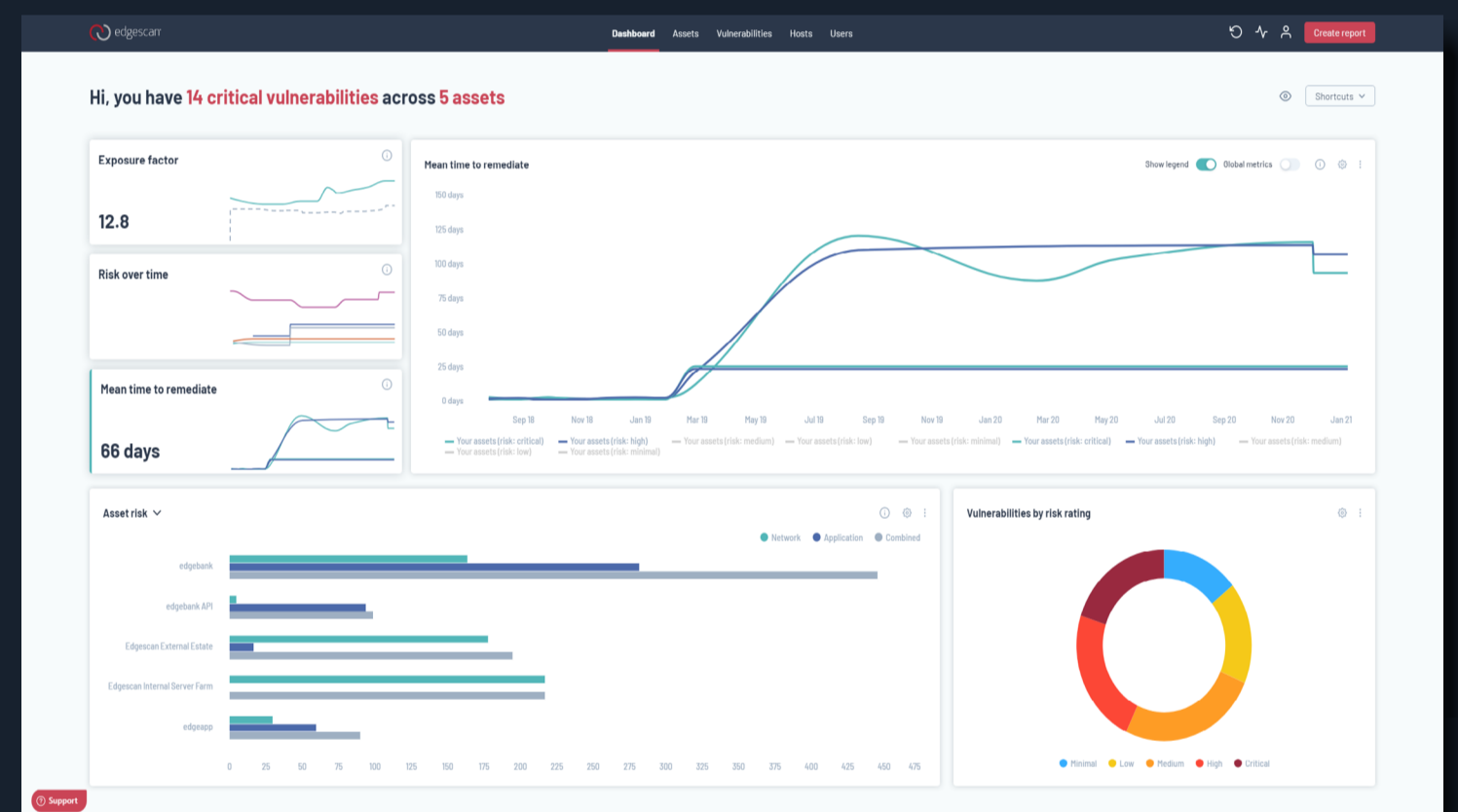
The Edgescan Team are experts at vulnerability detection. We save you time and money by helping you focus on items that matter.

How?

We deliver a cyber assessment service from our cloud which provides continuous and on-demand detection.

Why?

Finding weaknesses in IT Systems helps prevent a data breach or cyber attack.



If you think Edgescan can help your organisation increase its security posture, get in touch with our sales team for a trial at sales@edgescan.com

100%

Full OWASP Application Security Coverage

24/7/365

Continuous asset profiling and discovery

Gartner

SC Awards
EUROPE
WINNER
Best Vulnerability
Management Solution

aws partner
network

Pci Security
Standards Council
APPROVED SCANNING
VENDOR

Contributor
Version 2019
Data Breach
Investigation Report

ISO
27001
CERTIFICATION
EUROPE

Tech
EXCELLENCE
AWARDS
Managed Security Service
Provider of the Year
Edgescan

CREST

2020 Computing
Security Awards
WINNER
Penetration Testing Solution
of the Year

The Irish
Advantage