

Attack Surface Management (ASM) DATASHEET

Continuous Visibility Across your Estate

Visibility is the cornerstone of a robust security posture. You can't secure what you don't know about. With today's cloud enabled and rapid development environment, Edgescan keeps you informed of changes and exposures. Edgescan delivers external Attack Surface Management (ASM) which provides you the ability to see all services exposed to the public internet across your global estate. As new systems are deployed, decommissioned or a system changes, Edgescan can inform you of the event.

Keep informed – Edgescan Events

Edgescan keeps you informed as events happen. Using our simple customisable events feature you can be notified in multiple ways about anything that matters to you. Such as:

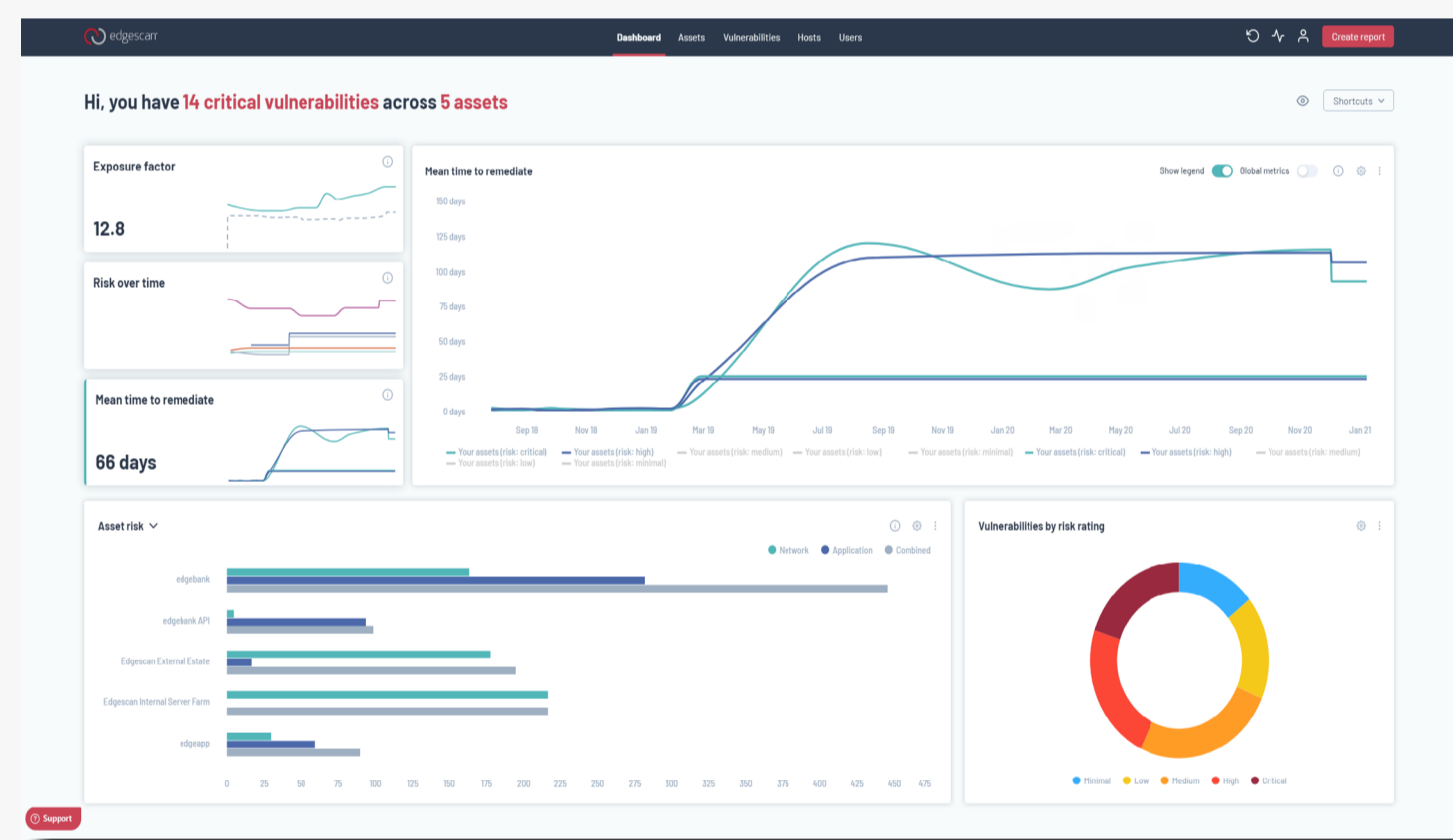
- Shadow, Lost, Forgotten and legacy assets
- Human Error resulting in exposed services
- Vulnerable and outdated software
- Rogue deployments
- Rogue API's, unknown API's
- IoT detection
- Application / DNS discovery

Notifications can be through Webhooks/API integrations, Ticketing systems, Instant Messaging, Risk Platforms, Bug Tracking, Asset Management and SIEM systems.

Know your Attack Surface

Changes to firewalls, exposed services and rogue deployments are all avenues of attack for any Enterprise. With Edgescan External IP Monitoring you are informed in real-time of change which may increase your attack surface and introduce additional risk.

In addition to External IP Monitoring, Edgescan uniquely offers API Discovery Service, which identifies and detects the presence of API's on the external IP range of the enterprise.



Features

Supported

Fast network host discovery and asynchronous port scanning across your whole global perimeter.



Allowing the identification of networking devices, platforms, operating systems, databases and applications.



Determine which service ports are present and listening for transactions.



Customizable scan profiling – be specific about the services you want to test for.



OS Detection – Discovery of known OS types based on response fingerprints.



Perform live retests on exposed ports.



Historical host information for point in time reads of endpoints.



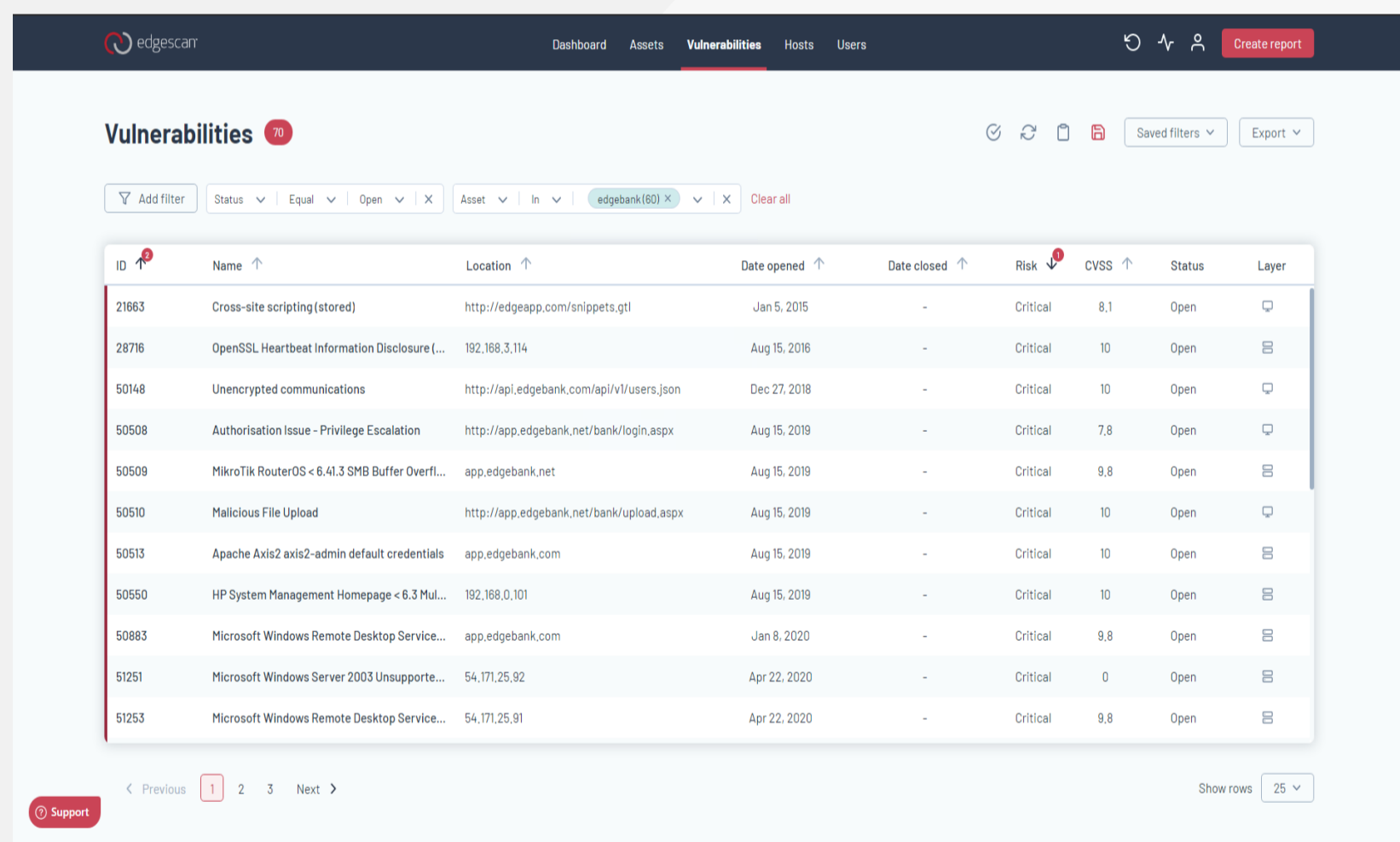
Identification of services running on the exposed layer.



Detect exposed services, ports and endpoints on a continuous basis.



Customizable targeted alerting, which notifies you automatically of any potential exposures (e-mail, webhook, SMS).

ID	Name	Location	Date opened	Date closed	Risk	CVSS	Status	Layer
21863	Cross-site scripting (stored)	http://edgesapp.com/snippets.gtl	Jan 5, 2015	-	Critical	8.1	Open	
28776	OpenSSL Heartbeat Information Disclosure [...]	192.168.3.114	Aug 15, 2016	-	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 < 6.41.3 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	



FULLSTACK VULNERABILITY MANAGEMENT

IRL: +353 (0) 1 6815330
 UK: +44 (0) 203 769 0963
 US: +1 646 630 8832

Sales and general enquiries:
sales@edgescan.com

View our latest
2021 Vulnerability Statistics Report
 at edgescan.com