edgescan™

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.

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.

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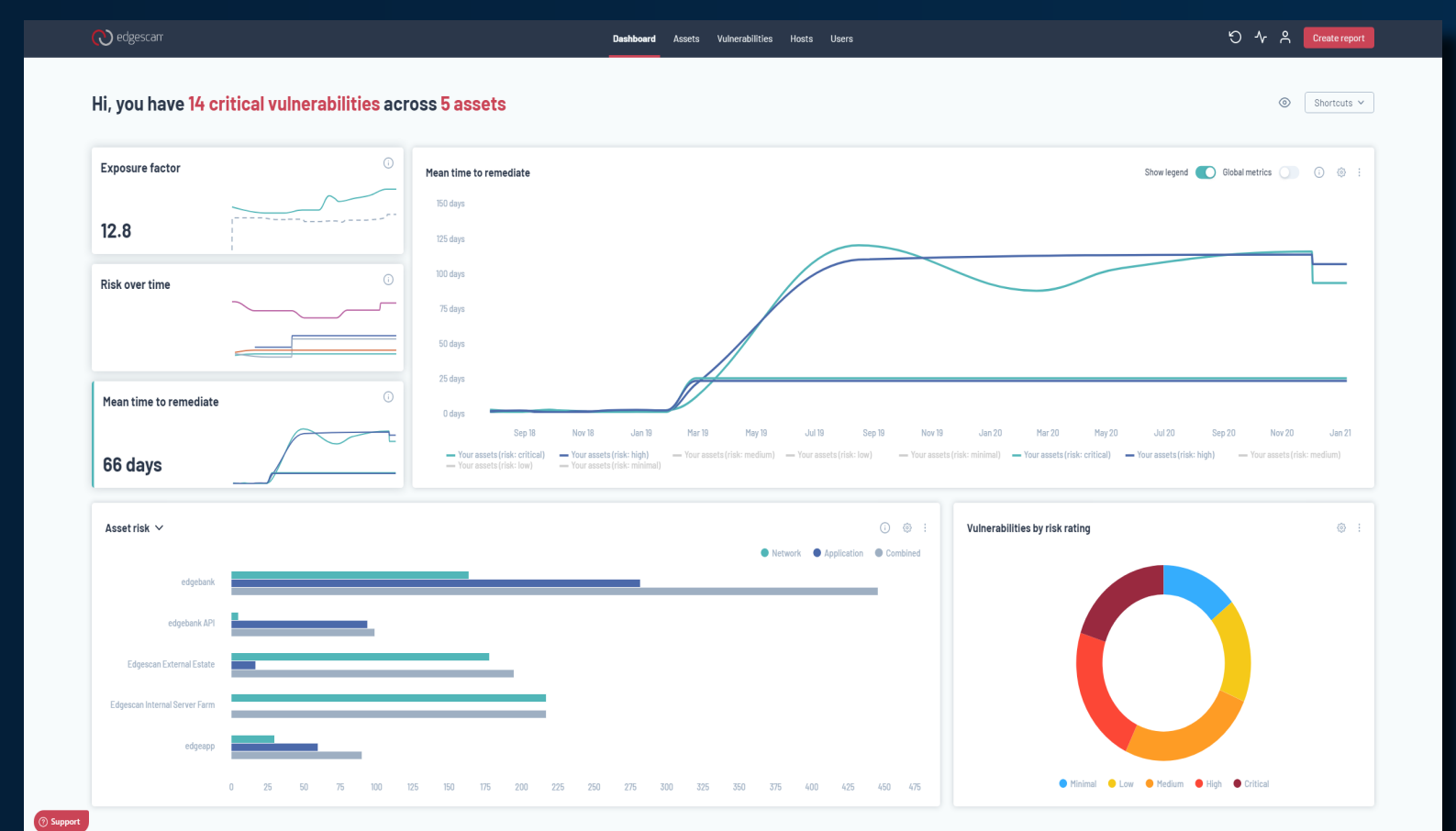
- Shadow, Lost, Forgotten and legacy assets
- Human Error resulting in exposed services
- Vulnerable and outdated software
- Rogue deployments
- Rogue API's, unknown API's
- IoT detection
- Application / DNS discovery

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

webhooks · RISKSENSE · Jira · AXONIUS

YARO · zapier · Teams · slack

edgescan™

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).	✔
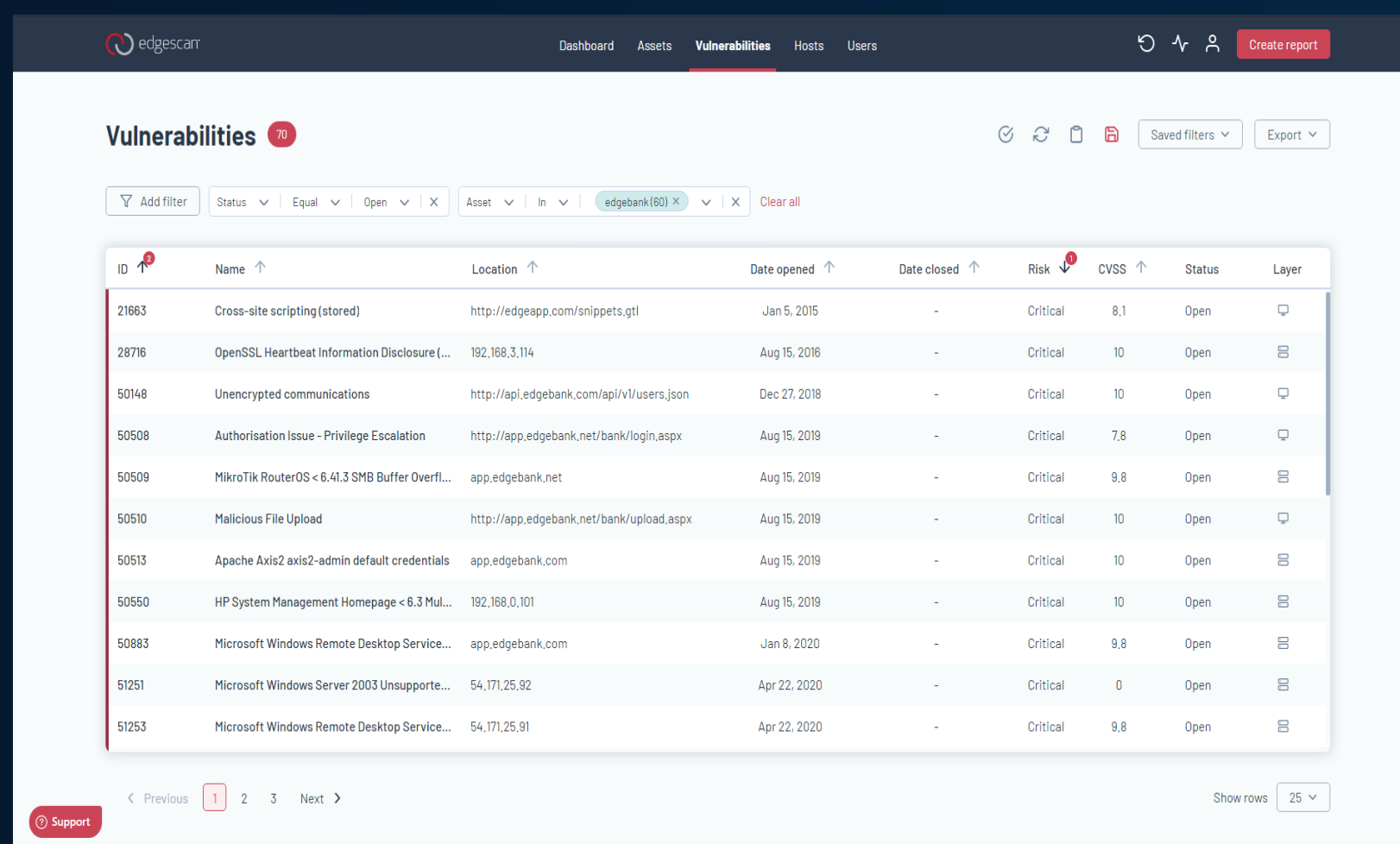
edgescan™
FULLSTACK VULNERABILITY MANAGEMENT

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