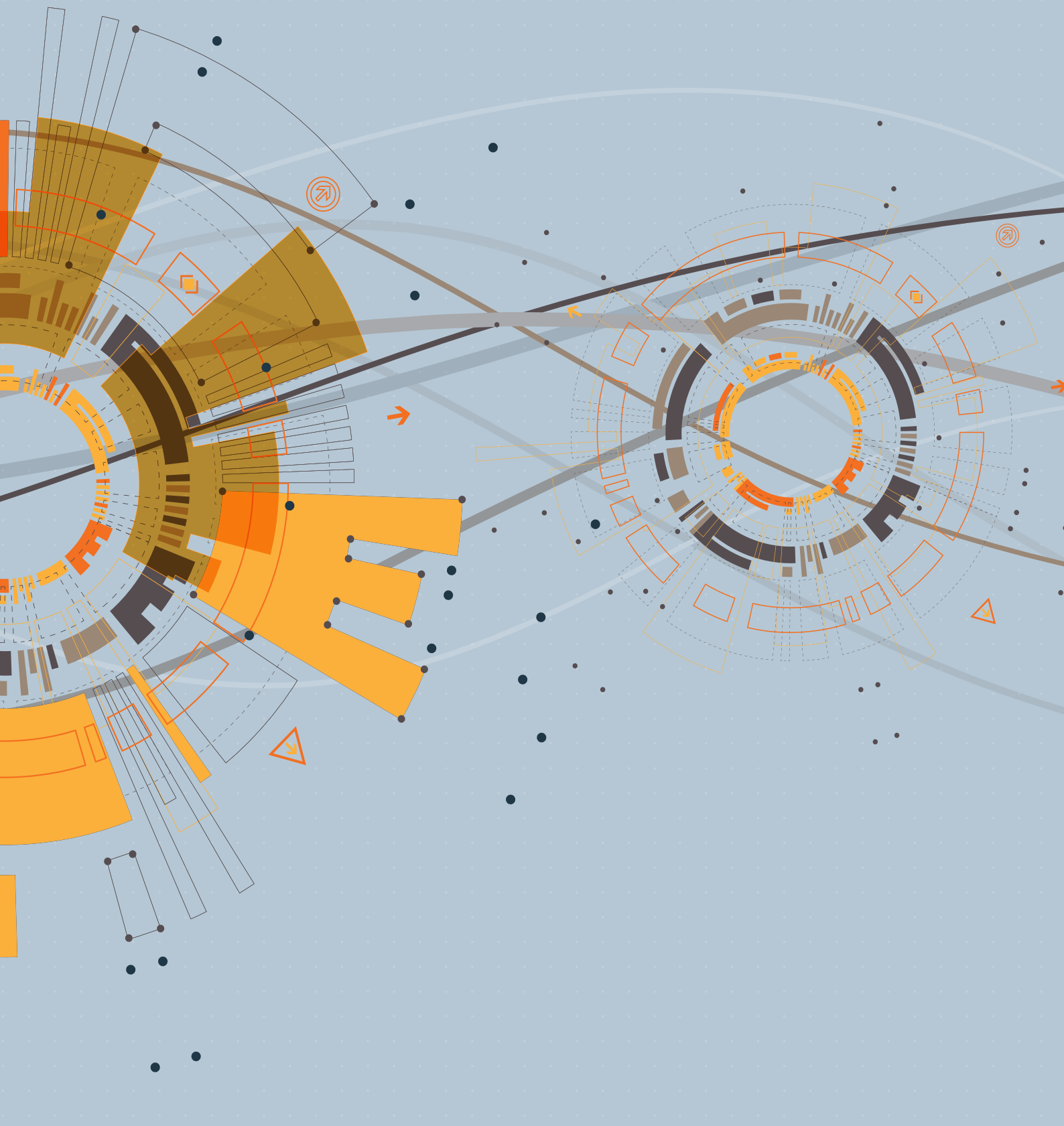
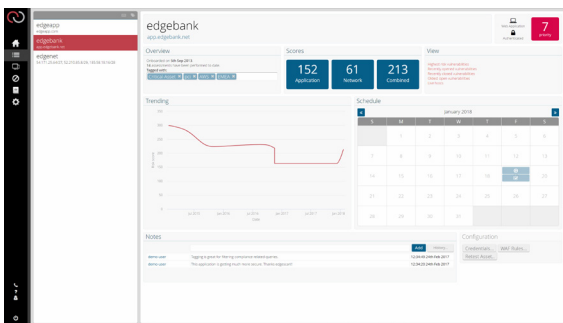
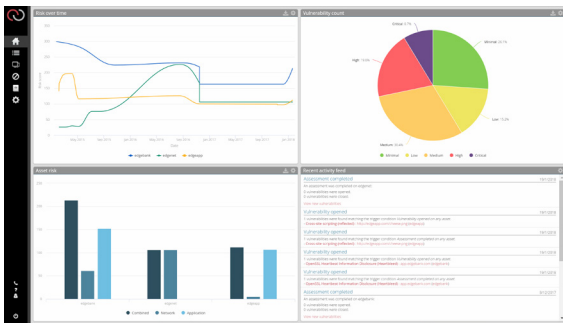
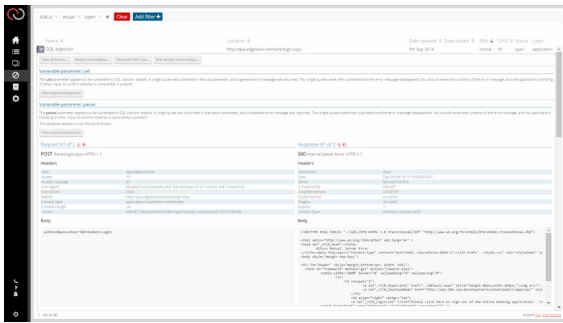




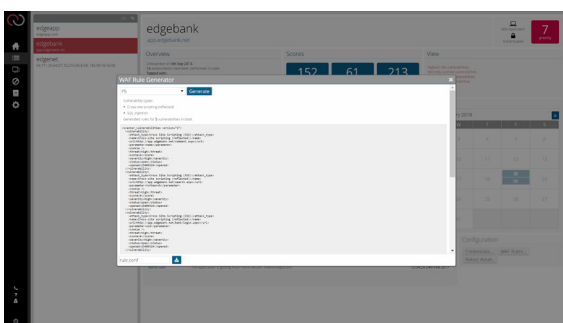
EFFECTIVE, SCALABLE, #FULLSTACK VULNERABILITY MANAGEMENT



edgescan™ Portal



IP	Host	OS	Applications	Network	Content	Score	Severity	Asset Name
141.171.25.80	www.e	Linux 3.10	Apache/2.4.18 (Ubuntu)	none	none	0.0	None	www.e
141.171.25.81	www.e	Linux 3.10	Apache/2.4.18 (Ubuntu)	none	none	0.0	None	www.e
141.171.25.82	www.e	Linux 3.10	Apache/2.4.18 (Ubuntu)	none	none	0.0	None	www.e
141.171.25.83	www.e	Linux 3.10	Apache/2.4.18 (Ubuntu)	none	none	0.0	None	www.e
141.171.25.84	www.e	Linux 3.10	Apache/2.4.18 (Ubuntu)	none	none	0.0	None	www.e
141.171.25.85	www.e	Linux 3.10	Apache/2.4.18 (Ubuntu)	none	none	0.0	None	www.e
141.171.25.86	www.e	Linux 3.10	Apache/2.4.18 (Ubuntu)	none	none	0.0	None	www.e
141.171.25.87	www.e	Linux 3.10	Apache/2.4.18 (Ubuntu)	none	none	0.0	None	www.e
141.171.25.88	www.e	Linux 3.10	Apache/2.4.18 (Ubuntu)	none	none	0.0	None	www.e
141.171.25.89	www.e	Linux 3.10	Apache/2.4.18 (Ubuntu)	none	none	0.0	None	www.e
141.171.25.90	www.e	Linux 3.10	Apache/2.4.18 (Ubuntu)	none	none	0.0	None	www.e
141.171.25.91	www.e	Linux 3.10	Apache/2.4.18 (Ubuntu)	none	none	0.0	None	www.e
141.171.25.92	www.e	Linux 3.10	Apache/2.4.18 (Ubuntu)	none	none	0.0	None	www.e
141.171.25.93	www.e	Linux 3.10	Apache/2.4.18 (Ubuntu)	none	none	0.0	None	www.e
141.171.25.94	www.e	Linux 3.10	Apache/2.4.18 (Ubuntu)	none	none	0.0	None	www.e
141.171.25.95	www.e	Linux 3.10	Apache/2.4.18 (Ubuntu)	none	none	0.0	None	www.e
141.171.25.96	www.e	Linux 3.10	Apache/2.4.18 (Ubuntu)	none	none	0.0	None	www.e
141.171.25.97	www.e	Linux 3.10	Apache/2.4.18 (Ubuntu)	none	none	0.0	None	www.e
141.171.25.98	www.e	Linux 3.10	Apache/2.4.18 (Ubuntu)	none	none	0.0	None	www.e
141.171.25.99	www.e	Linux 3.10	Apache/2.4.18 (Ubuntu)	none	none	0.0	None	www.e
141.171.25.100	www.e	Linux 3.10	Apache/2.4.18 (Ubuntu)	none	none	0.0	None	www.e



ABOUT EDGESCAN™

SaaS: edgescan™ is a ‘Security-as-a-Service’ (SaaS) vulnerability management service which detects vulnerabilities in both web application and hosting infrastructure alike.

Hybrid Scalable Assessments: edgescan™ detects both known (CVE) vulnerabilities and also web application vulnerabilities unique to the application, by using our hybrid approach.

Analytics & Depth: Coupling leading edge risk analytics, production-safe automation and human intelligence, **edgescan™** provides deep authenticated and unauthenticated vulnerability assessment across all layers of a system’s technical stack. Historical data to measure your risk profile over time. Effortless visibility into your fullstack security posture at-a-glance – Vulnerability Intelligence.

Coverage: edgescan™ provides “fullstack vulnerability management” covering hosting environments, frameworks and developer-written code. Our **edgescan advanced™** license even covers business logic and advanced manual testing techniques, akin to a full penetration test.

Support: Dedicated expert support from seasoned penetration testers and developers, to provide advice and remediation guidance.

Vulnerability Intelligence: edgescan™ delivers validated and risk-rated vulnerability data. Validated using a combination of correlation technology and human expertise, **edgescan™** delivers virtually false positive free vulnerability intel.

Rich API Integration: Our API makes it simple to plug **edgescan™** into your ecosystem in order to correlate and reconcile, providing integration with GRC, bug tracking and DevSecOps systems alike.

One-click WAF: Rule generation supporting a variety of firewalls is also supported, helping you “virtually patch” discovered vulnerabilities.

Alerting: Customise Alerting via email, SMS, Webhooks, Slack, API etc, based on custom criteria.

Continuous Asset Profiling: Continuous profiling of the entire Internet-facing estate detecting changes in estate profile and eliminating blind spots.

Scale: Vulnerability intelligence, from a single web application/endpoint to thousands, **edgescan™** delivers continuous and on-demand security assessments.

Compliance: edgescan™ is a certified PCI ASV and delivers testing covering the OWASP Top 10, WASC threat classification, CWE/SANS Top 25, etc.

WHAT IS EDGESCAN™?

edgescan™ is a vulnerability management service (SaaS) which continuously identifies cyber security vulnerabilities across the #fullstack, provides continuous system visibility and provides support to understand, prioritise and mitigate cyber security risks on a continuous basis.

How edgescan™ works

Our expert security analysts on-board, enumerate and prioritise your assets (e.g. websites, mobile applications, web applications, cloud applications, endpoints & hosting servers) into edgescan™.

We perform continuous vulnerability assessments of all assets, as much or as little as you require. edgescan™ assessments cover both technical and logical testing, including all OWASP vulnerabilities, WASC threat classification and CWE known vulnerabilities. edgescan™ also aligns and surpasses PCI (Payment Card Industry) compliance requirements. In fact, edgescan™ is a certified PCI Approved Scanning Vendor (PCI ASV).

False Positive Free: Manual verification by our expert security analysts ensures that all application and network vulnerabilities found are verified as real and ranked by security risk. This procedure allows for false positive free vulnerability intelligence for all assets.

The edgescan™ online portal provides 24/7 visibility of security metrics, trending data, key performance indicators (KPIs) and enables users to generate custom reports to manage and remediate cybersecurity risk. Our fully extensible API provides users with the ability to integrate edgescan™ vulnerability intelligence into any GRC or bug tracking system.

Ultimately, edgescan™ users benefit from continuous vulnerability management and penetration testing, security visibility and security intelligence.

edgescan™ is unique, being the only hybrid full-stack security solution of its kind in Europe, Middle East and Africa (EMEA). This involves unlimited security assessments of both networks and applications coupled with manual verification of findings by edgescan™ security analysts.

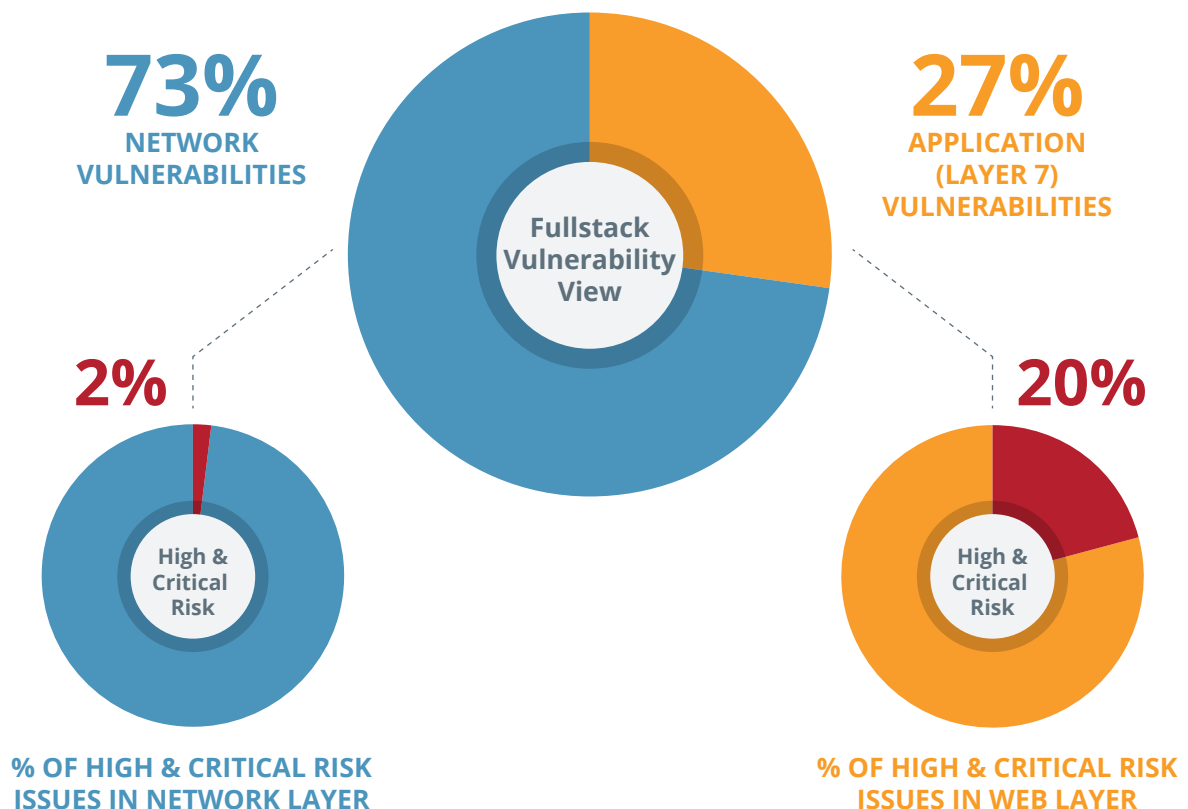


THE THREAT IS REAL: BASED ON EDGECAN™ VULNERABILITY STATISTICS (2018)

- Application Layer: 20% of all vulnerabilities discovered are High or Critical Risk.
- 73% of all vulnerabilities discovered were in the host/network layer.
- 8% of all vulnerabilities had a CVSS 2.0 score of more than 4.0 which is a PCI DSS fail.
- 32% of all application layer vulnerabilities had a CVSS 2.0 score of more than 4.0 which is a PCI DSS fail.

FULLSTACK VULNERABILITY VIEW

In 2017 we discovered that on average, 27% of all vulnerabilities were associated with web applications and 73% were network vulnerabilities.



Did you know? We are proud contributors of statistical data for the Verizon Data Breach Investigations Report (DBIR)

THOUSANDS OF VULNERABILITIES: ONE MANAGEMENT SOLUTION



Accuracy

edgescan™ security analysts are experts in vulnerability management and penetration testing. They manually verify all discovered security vulnerabilities, so our clients benefit from accurate (false positive free) vulnerability intelligence.



Cost Benefits

edgescan™ is a managed security service provider (MSSP) that can save your business significant costs. With **edgescan™**, there is no need for hiring and training additional security staff, and no need to purchase further hardware or software licenses.



Continuity

edgescan™ provides continuous or on-demand security assessments in a production safe manner so you can be assured your business is getting the coverage as required.

edgescan™ vulnerability assessment and management consists of a sophisticated platform and multiple tuned web scanning engines. This is coupled with a powerful, easy-to-use, web-based vulnerability management and reporting platform and extensive integration capabilities through the **edgescan™** API.

edgescan™ provides a flexible licensing scheme and allows unlimited assessments across the full technology stack. Clients that find **edgescan™** an invaluable service include financial, gaming and medical firms, including many leading brands globally.

COMPLETE VULNERABILITY MANAGEMENT



Progress Tracking

Tracking your vulnerability history so you can measure your security posture and improvement over time.



Manual Validation

No time wasted on figuring out next steps, as all findings are verified to be real, accurate and risk rated by our security engineers.



Awesome Reports

Deeply customisable reporting, from executive summary to deep technical data and remediation advice.



Time Saving

The information you need to prioritise your security issues and help you focus your efforts - maximize your time.



Flexibility

Did you change your codebase?
Did you just spin up a new server?
Assessments - scheduled when you want them.



Expertise

Significant global experts have been the architects of our practices, approach and overall solution.



Security Insights

Verification of security improvements and information on any new threats or emerging threats.



Advanced API

Connect using the API and consume vulnerability intelligence from the **edgescan™** cloud into GRC, Bug Tracking, SIEM & MSSP systems. Our API provides you with the capability to invoke assessments, assign scan targets, download metrics, tag assets, generate custom reports and integrate to custom data analytics engines.



Cost Savings

Save money and time by understanding what risks are faced by your systems and how to fix them.

SIMPLIFYING SECURITY



Industry recognition:

edgescan™ is a leading application security testing platform and leads the pack in Gartner “Peer Insights”.

edgescan™ is a certified Amazon partner, certified Payment Card Industry Approved Scanning Vendor (PCI ASV) and a leader in global #fullstack vulnerability management.



WAF Integration:

Auto generation of Web Application Firewall (WAF) rules in one click. “Virtually patch” web application vulnerabilities, helping you mitigate risks faster. Support for F5, Citrix, Imperva, ModSecurity and many more.



edgescan™ CloudControl:

Using **edgescan™** CloudControl, internal non-Internet facing systems can be assessed on an on-demand or scheduled basis. CloudControl also provides the ability to integrate with DevSecOps environments for pre-production assessments.



API Testing:

API ecosystems are no problem for **edgescan™**. We have pioneered a robust approach to API continuous security assessment, with the same depth and rigour as a traditional web application estate.



edgescan™ and IoT:

edgescan™ offers continuous visibility, service identification, port scanning and DNS querying for IoT systems, helping you get continuous security and visibility on-demand with a single dashboard for coordination and vulnerability intelligence.



Alerting and Events:

edgescan™ can deliver alerts to you any way you require. Be it via the API, Webhooks, SMS, email or instant messaging (e.g. #slack), **edgescan™** can inform you of an event that is meaningful to you.



edgescan™ WiFi SaaS:

Remote WiFi assessments can be delivered using the **edgescan™** “PicoBox”. Assess branch WiFi, Wireless PoS (Point of Sale), and corporate wireless network systems via the **edgescan™** cloud. Manage the security of hundreds of Wifi networks from a unified dashboard, to get ultimate visibility.

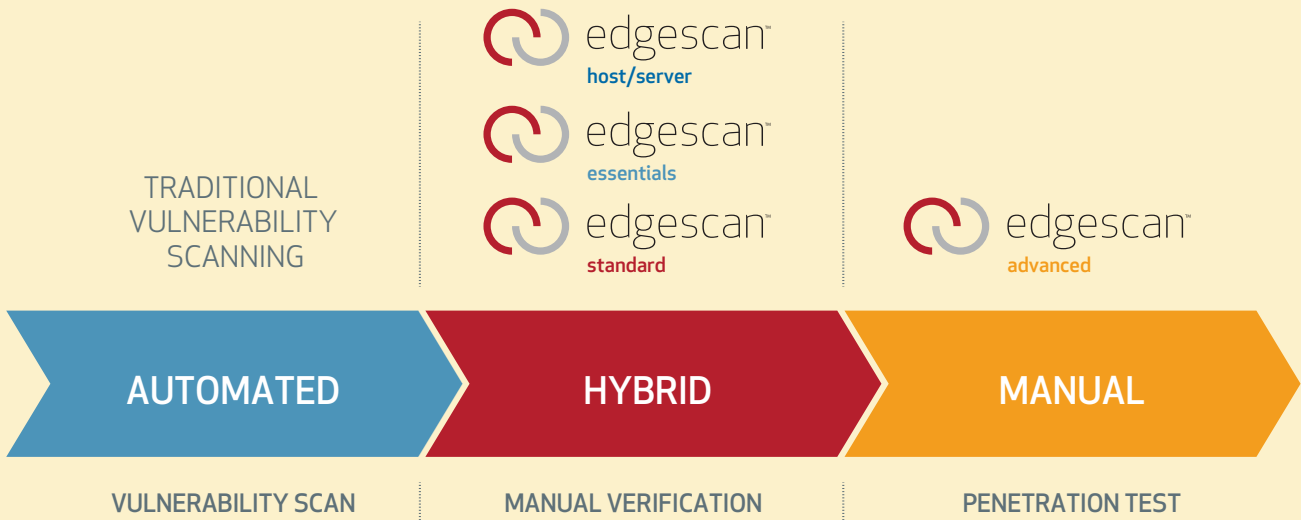


Asset Tagging:

“Tag” assets with anything you want. Group and search assets by tags. An easy way to manage multiple assets with similar attributes across an enterprise estate.

DETECTING VULNERABILITIES WITH EXPERTISE

edgescan™'s approach to cyber security can be compared to traditional security testing in the following way:



LEADING #FULLSTACK VULNERABILITY MANAGEMENT



Continuous Asset Profiling:

edgescan™ Continuous Asset Profiling is a feature for all **edgescan™** licenses. It delivers continuous endpoint discovery and asynchronous port scanning to help you identify and monitor assets and network changes as they occur.

Continuous Asset Profiling supports service, DNS and OS detection and can generate alerts based on what you need to know using the events API or portal.



Host/Server Security Assessment:

Server Vulnerability Assessment covering over 90,000 CVEs. Designed to help ensure your deployment, be it in the cloud or on premise, is secure and configured securely.

All vulnerabilities are validated and risk rated by experts and available via the dashboard to track and report on when required.



PCI Compliance:

edgescan™ is a certified Payment Card Industry Approved Scanning Vendor (PCI ASV).

edgescan™ exceeds requirements of the PCI DSS by providing continuous, verified vulnerability assessments for both internal, public Internet facing websites and cloud environments.

edgescan™ Advanced includes business logic and penetration testing required by the PCI DSS standard.



Web Application Security Assessment:

Validated web application security assessments on demand when you want them and scheduled as often as you need them.

Recording of risk ratings, trending data and other metrics on a continuous basis, all available via our rich dashboard for superior security intelligence.

EDGECAN™ APPROACHES / LICENSES



Foundational assessment for less critical applications

- Can be used across an enterprise to estimate basic security posture
- Massively scalable
- Validated results
- Very cost effective

ESSENTIALS

WEB APPLICATION
DISCOVERY & VULNERABILITY
MANAGEMENT



Includes all edgescan™ Basic features but also includes authenticated testing to simulate a “logged in” attacker

- Recommended for use on permanent applications with authentication enabled
- Massively scalable
- Validated results

STANDARD

WEB APPLICATION
VULNERABILITY MANAGEMENT



Includes all the features of edgescan™ Standard but also includes business logic testing on-demand to help detect complex security flaws

- Recommended for use on business critical and complex applications
- For applications with rigorous compliance requirements

ADVANCED

WEB APPLICATION
PENETRATION TESTING
VULNERABILITY MANAGEMENT



For scanning hosts and servers located in data centres or cloud-based deployments

- Detects over 90,000 known vulnerabilities (CVE)
- Assessment across IP ranges or single IP's
- Massively scalable, extremely flexible and cost effective
- One license supports up to 256 hosts

HOST/SERVER

HOST/SERVER
VULNERABILITY MANAGEMENT

Licenses Explained

	edgescan™ essentials	edgescan™ standard	edgescan™ advanced	edgescan™ host/server
Verified & Risk rated results	●	●	●	●
On-Demand testing	●	●	●	●
PCI Compliance	●	●	●	●
Highly Scalable	●	●	●	●
Support and access to analysts	●	●	●	●
Continuous Asset Profiling	●	●	●	●
API Access	●	●	●	●
Host/Server Vulnerability Analysis	●	●	●	●
Web Application Testing	●	●	●	
WAF/Firewall Rule Generation	●	●	●	
Authenticated Testing		●	●	●
Business Logic Testing			●	

EDGESCAN™ EXAMPLE DEPLOYMENT

Example Client Engagement Use Case 1

Scope

- 1000 Hosts/Servers (IPs)
- 10 Web Applications:
3 critical, 3 authenticated,
4 basic (brochure)

Suggested Approach

Initial Licenses Required:

- 6 edgescan™ Standard + 4 edgescan™ Essentials
+ 4 edgescan™ Host/Server

Onboarding

- 1 week to on-board entire estate and commence continuous testing of all web applications and hosts.
- **Requirements:** URLs for applications, Server IPs & Login credentials where required.

3-6 months later, client may wish to upgrade from edgescan™ Standard to edgescan™ Advanced for 3 critical applications. This provides on-demand deep testing of the 3 critical applications in addition to the continuous testing via edgescan™ standard.

Example Client Engagement Use Case 2

Scope

- 0 Hosts/Servers (IP's)
- 350 Web Applications

Suggested Approach

Initial Licenses Required:

- 350 edgescan™ Essentials

Onboarding

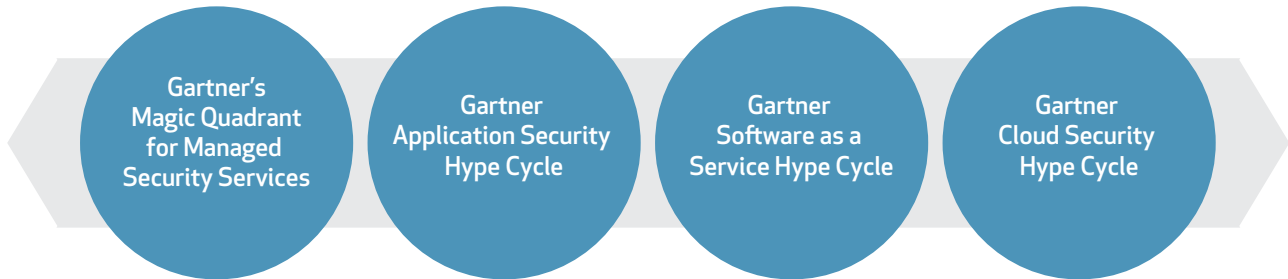
- 1-2 weeks to on-board entire estate and commencement of continuous testing.
- Associated Servers/Hosts (up to 350 IPs) are also included for fullstack security coverage.
- **Requirements:** URLs for applications

After the initial onboarding the client may choose to upgrade the licenses from edgescan™ Essentials to Standard or Advanced licenses for specific web applications.

An upgrade path is provided to easily upgrade required licenses to either Standard or Advanced. This provides additional on-demand deep testing of selected applications in addition to the continuous testing via edgescan™ Essentials.

RECOGNITION AND SUCCESS

Gartner With over 90,000 Assets under vulnerability management, **edgescan™** is listed in:



edgescan™ is one of the highest rated security testing platform's in the Gartner Peer Review Portal
<https://www.gartner.com/reviews/market/application-security-testing/vendor/edgescan>

"Best of breed product that allows my organization to scale to an enterprise level."

Manager of Application Security in the Media Industry,
Gartner Peer Insights 2018.

"The time to identify & respond to our risk has been significantly reduced."

Information Security Specialist in the Services Industry,
Gartner Peer Insights 2017.

"Easy to implement and even easier to use. The level of detail is outstanding."

CISO in a Government Organisation,
Gartner Peer Insights 2017.

"Excellent customer focus and consistent delivery."

Security Architecture Manager in the Finance Industry,
Gartner Peer Insights 2017.

"edgescan's customer focused approach acts as a significant differentiator. They have introduced a fresh perspective on our pen testing methodology and I would have no hesitation in recommending them."

Security Architecture Manager in a Professional Services firm, Gartner Peer Insights 2017.

"Assurance from engaging edgescan allows us to focus scarce InfoSec resources elsewhere."

Managing Director in the Services Industry,
Gartner Peer Insights 2016.

WHY EDGESCAN™?

edgescan™ is a managed security service which identifies and provides vulnerability intelligence on an on-going basis. It detects technical vulnerabilities in both internal and Internet facing systems and provides you with the power to understand, prioritise and fix.

It provides you the ability to manage both network and web application security issues for tens, hundreds or even thousands of your systems.

edgescan™ conducts Application & Server vulnerability management with manual validation to help ensure your application / server security.

edgescan™ reports are virtually False Positive free due to our hybrid approach of combining automated testing with manual validation.

edgescan™ provides continuous asset profiling letting you see what systems and services are live and available at any point in time and provides alerting to let you detect rogue, APT or delinquent systems within your asset estate.



False Positive Free, Full-Stack, Continuous Penetration Testing.

"Very useful and helpful – helped us find a lot of issues quickly and very cost effective for the benefit delivered for us."

CISO Financial Services, UK

"Great customer focused service, and the clear explanation of the results from pen tests has certainly made our life easier."

IT Architect, Legal Firm, UK&I

"Excellent service, quick response, efficient and unobtrusive. Highly recommended."

CISO Media Organisation, USA

"Apart from a strong technical platform, the key advantage Edgescan seems to have over competitors is an ability to relate knowledge of the subject matter to real world actions..."

Head of Application Security
(Medical Organisation), Dublin, Ireland



"...very successful service for us and has provided a focus to our teams to ensure we are constantly improving our security posture. Most importantly, being regular, it's no longer just a once a year focus."

Gaming Client, EU





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

[@edgescan](#)

www.edgescan.com