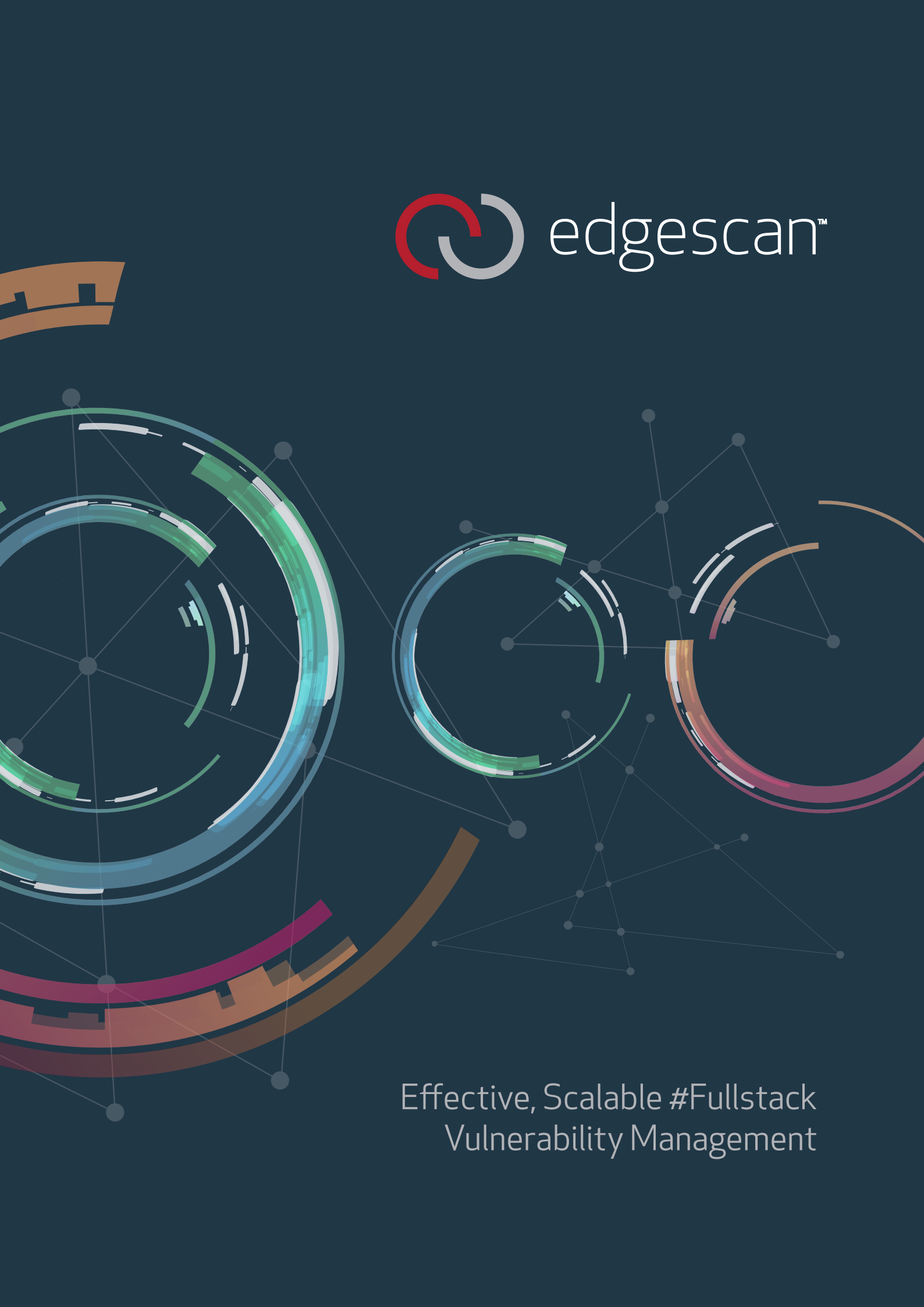
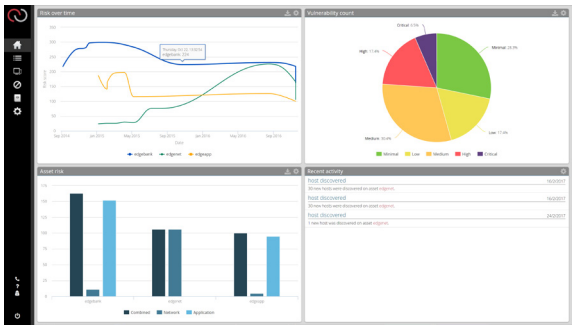
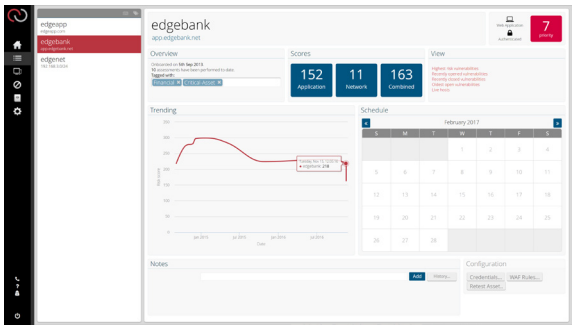
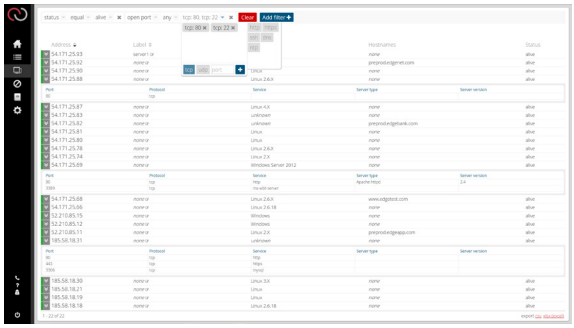
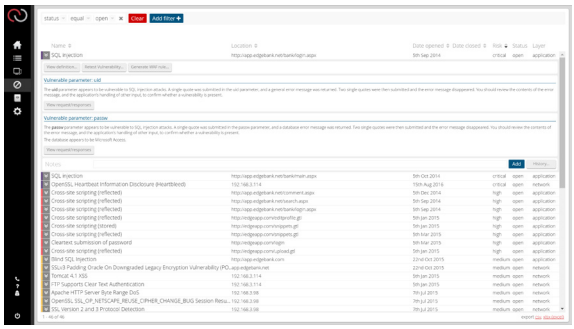

edgescan™
Effective, Scalable #Fullstack
Vulnerability Management

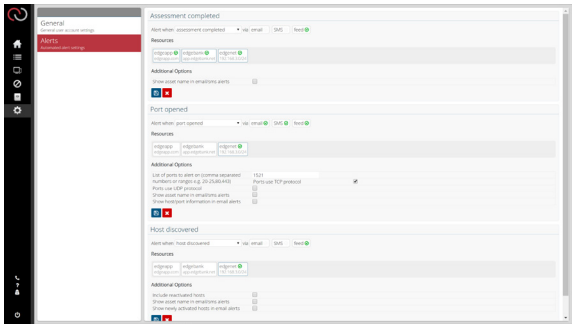
edgescan™ Portal











About edgescan™

SaaS: edgescan™ is a Software-as-a-Service (SaaS) vulnerability management service which helps detect vulnerabilities in both web application and hosting servers alike.

Hybrid Scalable Assessments: edgescan™ detects both known (CVE) vulnerabilities and also web application vulnerabilities unique to the application being assessed due to 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 systems technical stack.

Coverage: edgescan™ provides "full-stack" vulnerability management covering both hosting environments, component & frameworks and developer written code. Our **edgescan advanced™** license even covers business logic and advanced manual testing techniques.

Accuracy/Human Intelligence: All vulnerabilities discovered by **edgescan™** are verified by our engineering team to help make sure they are a real risk and highlighted appropriately to our clients.

API: The API makes it very easy to plug edgescan into your ecosystem in order to correlate and reconcile, providing integration with both GRC and Bug Tracking Systems alike.

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

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

Scale: Managing estates from one web application to hundreds, from a single hosting environment to thousands, edgescan delivers continuous and on demand security assessments.

edgescan

Gartner

2016 Tech Excellence Awards Winner

Red Herring Finalist 100 Europe

SME Finalist

amazon web services Partner Network Technology Partner

What is edgescan™?

edgescan™ is a managed security solution which identifies technical vulnerabilities and provides clients with the power to understand, prioritise and fix them.

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 to logical testing and cover all OWASP vulnerabilities, WASC threat classification and CWE known vulnerabilities. **edgescan™** also aligns and surpasses PCI compliance requirements.

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 a false positive free vulnerability intelligence for all assets.

The **edgescan™** online portal provides 24/7 visibility of security metrics, trending data, key performance indicators (KPI's) 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.

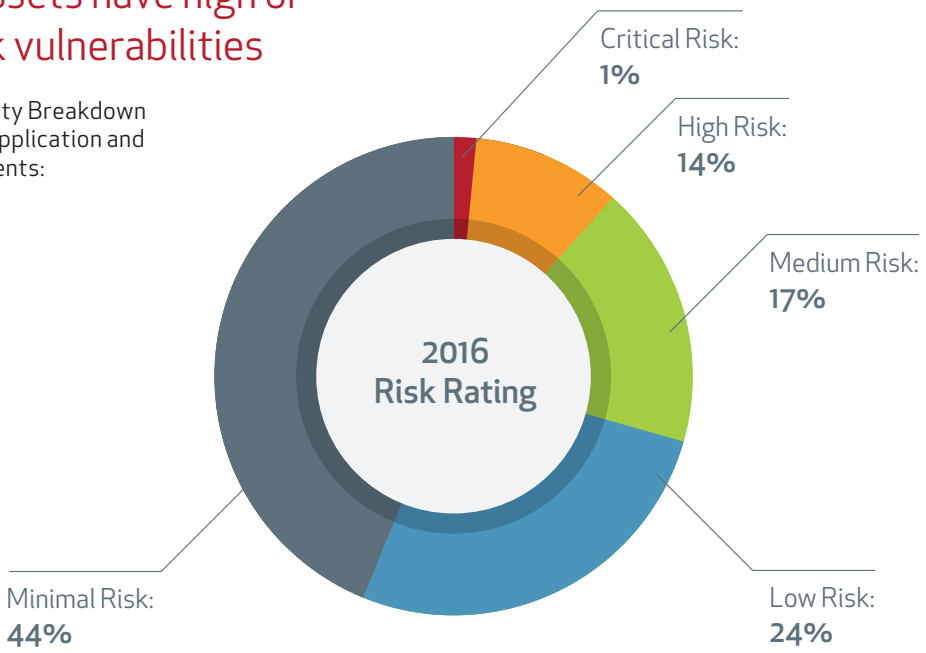
edgescan™ is unique, being the only hybrid full-stack security solution of its kind in Europe, Middle East and Africa "EMEA". This involves unlimited security assessments in both networks and applications coupled with manual verification of findings by **edgescan™** security analysts.

The Threat is Real

- **15%** of all Hosting and web application environments combined have a high or critical risk
- **95%** of Critical risks are in the web application layer
- **82%** of High Risks are in the web application layer
- **65%** of all vulnerabilities discovered are in the Hosting Layer

15.1% of Assets have high or critical risk vulnerabilities

Overall vulnerability Breakdown across both web application and hosting environments:



High or critical vulnerabilities are defined as:

- Easily exploitable
- Usually remote from the public Internet
- Application and Network layers combined
- Root Cause: Coding errors, configuration flaws and out-of-date or no patching applied

Remediation: Even though patch management is less than glamorous it still needs to be consistently performed. Security patches are a result of security bugs being discovered in application component and server systems provided by third parties.

In relation to web application security we still talk about Secure Application Development. It's our view that security touch points and developer education is a good starting place to correct the problem.

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.

Cost Savings

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

Robust API

Connect to our API and consume your local generated data to avail of our awesome graphs and reporting tools.

edgescan™

Experts in Vulnerability Management

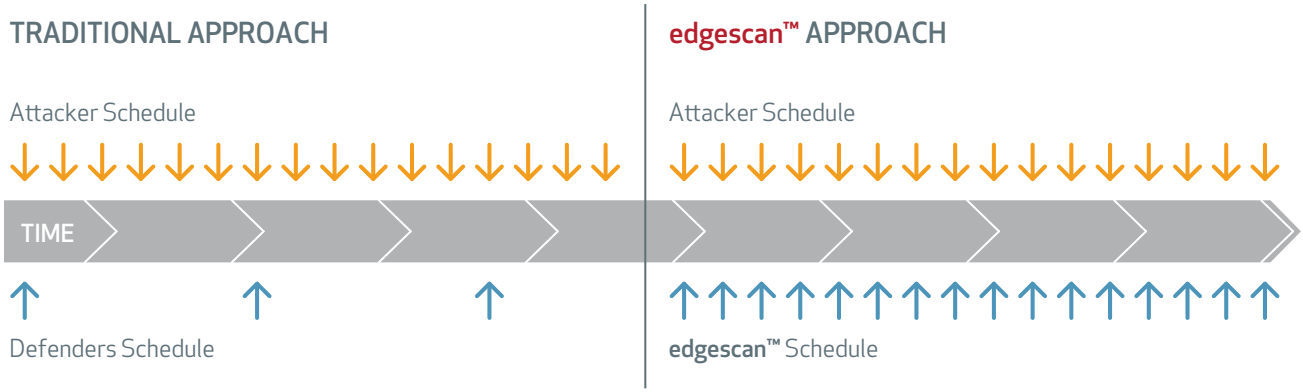
edgescan™ Fullstack Vulnerability Management helps companies to get the most from their vulnerability scanning and management requirements.

You get a service tailored to your specific needs and can be sure that you are following best practices by using experts in their own field. You can focus your efforts on your core business while experts take care of vulnerability management.

edgescan™

HELPS COMPANIES IN THREE WAYS:

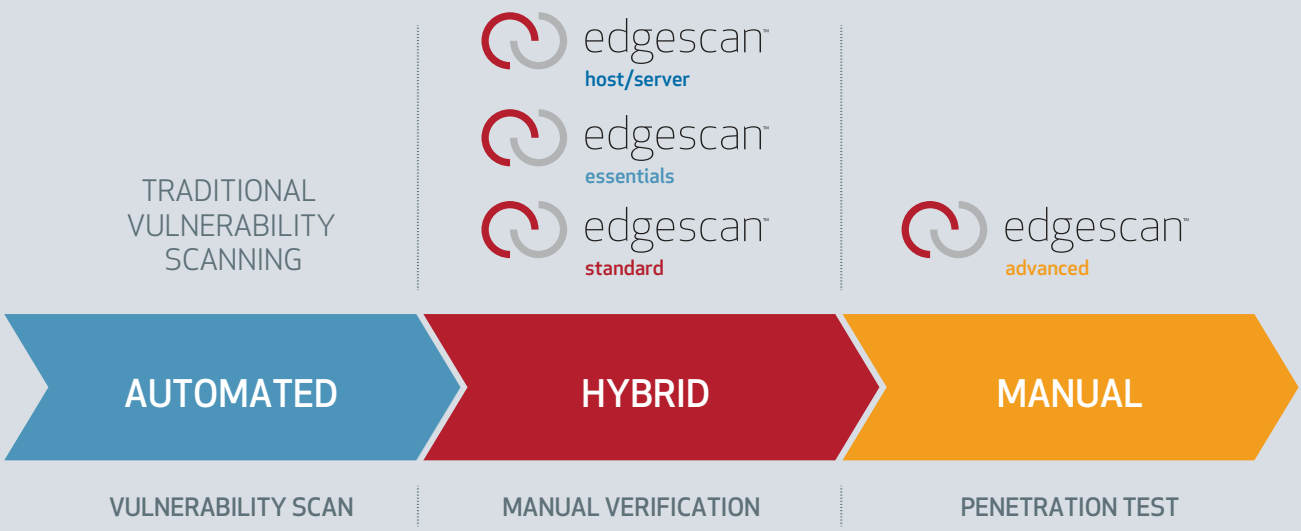
edgescan™ Approach



edgescan

Detecting Vulnerabilities with Expertise

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



Leading #FullStack Vulnerability Management

Continuous Asset Profiling:

edgescan™ Continuous Asset Profiling is a feature for all edgescan licenses. With fast network host discovery and asynchronous port scanning to help you identify and monitor assets and network changes.

Continuous Asset Profiling supports service and OS detection and can generate alerts based on what you need to know.

Host/Server Security Assessment:

Server Vulnerability Assessment covering over 90,000 CVE's. 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™ exceeds requirements of the PCI DSS by providing continuous, verified vulnerability assessments for both internal , public Internet facing websites and hosting environments.

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

edgescan™ integration with Web Application Firewalls (WAFs) supports the creation of virtual patches to fix vulnerabilities while providing the reports needed to pass auditor inspections.

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.

edgescan™ Approaches / Licenses

edgescan essentials

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

edgescan standard

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

edgescan advanced

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

edgescan host/server

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 (IP's)
- 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:** URL's for applications, Server IP's & 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

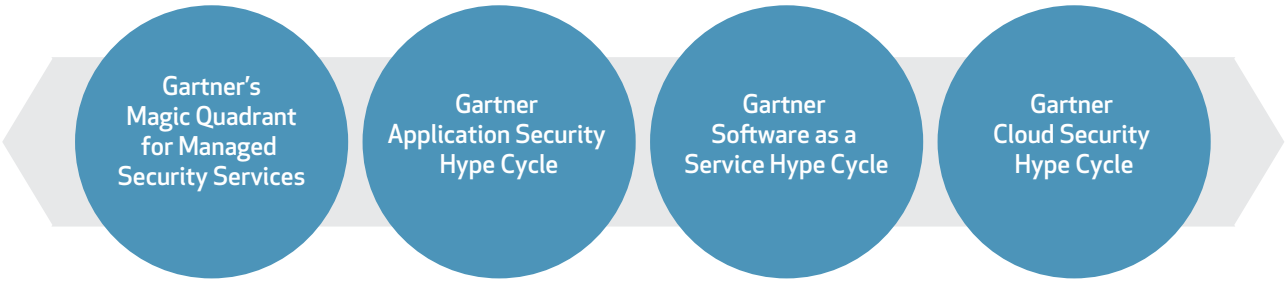
- 1-2 weeks to on-board entire estate and commencement of continuous testing.
- Associated Servers/Hosts (up to 350 IP's) are also included for fullstack security coverage.
- **Requirements:** URL's for applications

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 rating in the Gartner Peer Review Portal

https://www.gartner.com/reviews/market/application-security-testing/vendor/edgescan

edgescan™ Standard

"The implementation was simple and straightforward as a Managed Service solution."

Gartner Peer Insights, 2016

edgescan™ Standard

"Great tool, great team – helped shrink attack surface and protect our users."

Gartner Peer Insights, 2016

edgescan™ Standard

"Complete features, implementation easy, great for regulated sectors, hassle free vendor."

Gartner Peer Insights, 2016

edgescan™ Advanced

"Fantastic Product, quickly and efficiently deployed, with outstanding support."

Gartner Peer Insights, 2016

What is 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.

edgescan™ gives you:

- Manual threat verification and accuracy of all issues reported - false positive free
- Unbeatable price-performance ratio
- Prioritisation of security risks and remediation advise from our experts
- Continuous Asset profiling and Alerting
- 24/7 dashboard access and customisable reporting
- Continuous vulnerability assessment across both web and hosting layers
- Integration via API to GRC/ Bugtracking/JIRA/Slack & Automatic WAF Rule integration

edgescan™
DIGITAL SECURITY RADAR

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."

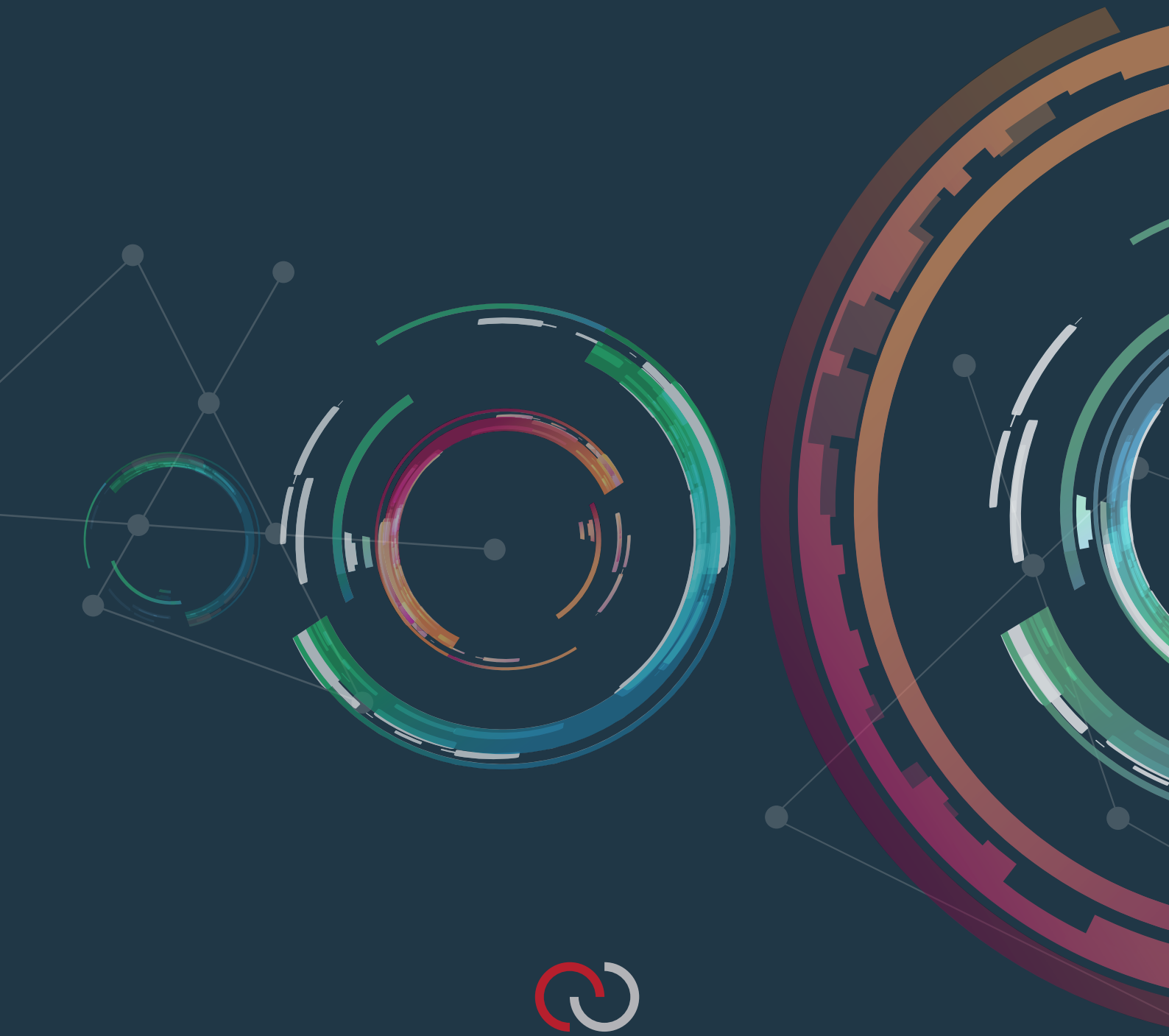
Gaming Client, EU

2016 Tech Excellence Awards Winner

Gartner

edgescan™
www.edgescan.com

 www.bccriskadvisory.com



edgescan™

CONTINUOUS VULNERABILITY MANAGEMENT

Telephone: IRL: +353 (0) 1 6815330 UK: +44 (0) 203 807 3933 US: +1 646 506 4977
Email: info@edgescan.com

www.edgescan.com