Barrier Networks Vulnerability Management Service and Penetration Testing (Edgescan)

G Cloud 11 Service Definition Document

Copyright

Barrier Networks Limited
272 Bath Street, Glasgow, G2 4JR
Tel: 0141 356 0101

1 Introduction

Barrier Networks Ltd is a privately-owned cybersecurity company who specialises in the integration of cybersecurity solutions. Established in 2006, the company work with all vertical markets that require specialist security advice. We are a partner with leading technology vendors including Fortinet, F5 Networks, Cisco, WhiteHat Security, Microsoft, AlienVault and Thales eSecurity.

Barrier Networks is committed to ensuring that our customers benefit from our years of experience within cybersecurity. Our consultants hold various levels of industry certifications right up to Cisco's prestigious expert-level CCIE Security. We are accredited to assess and certify against the National Cyber Security Centre Cyber Essentials scheme and work as an authorised "Trusted Partner" of the Scottish Business Resilience Centre

1.1 Barrier Networks Pedigree

At Barrier we believe that our skills, experience and technology are among the best in the industry and certainly the best in the region, some of our unique advantages include:

- Best of breed technology that is highly rated by Gartner Research.
- UK Based
- Detect advanced threats, malicious insiders and third-party supplier risk.
- Significant experience in full spectrum cybersecurity operations.
- Certified consultants and engineers who hold active security clearances.
- Flexible commercial models with options for Opex based solutions.

1.2 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.

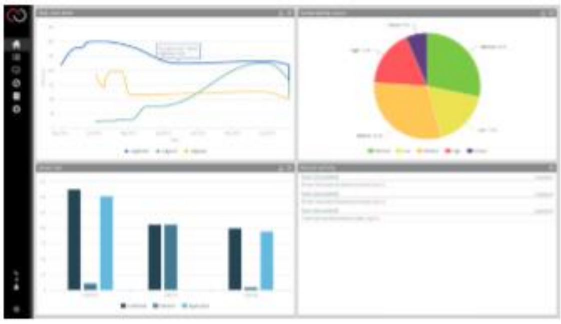
API: The API makes it very easy to plug edgescan into your ecosystem in order to correlate and reconcile, providing integration with both GRC and Bug Tracking Systems alike.

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.

1.3 edgescan™ Portal



1.4 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.

1.5 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™.

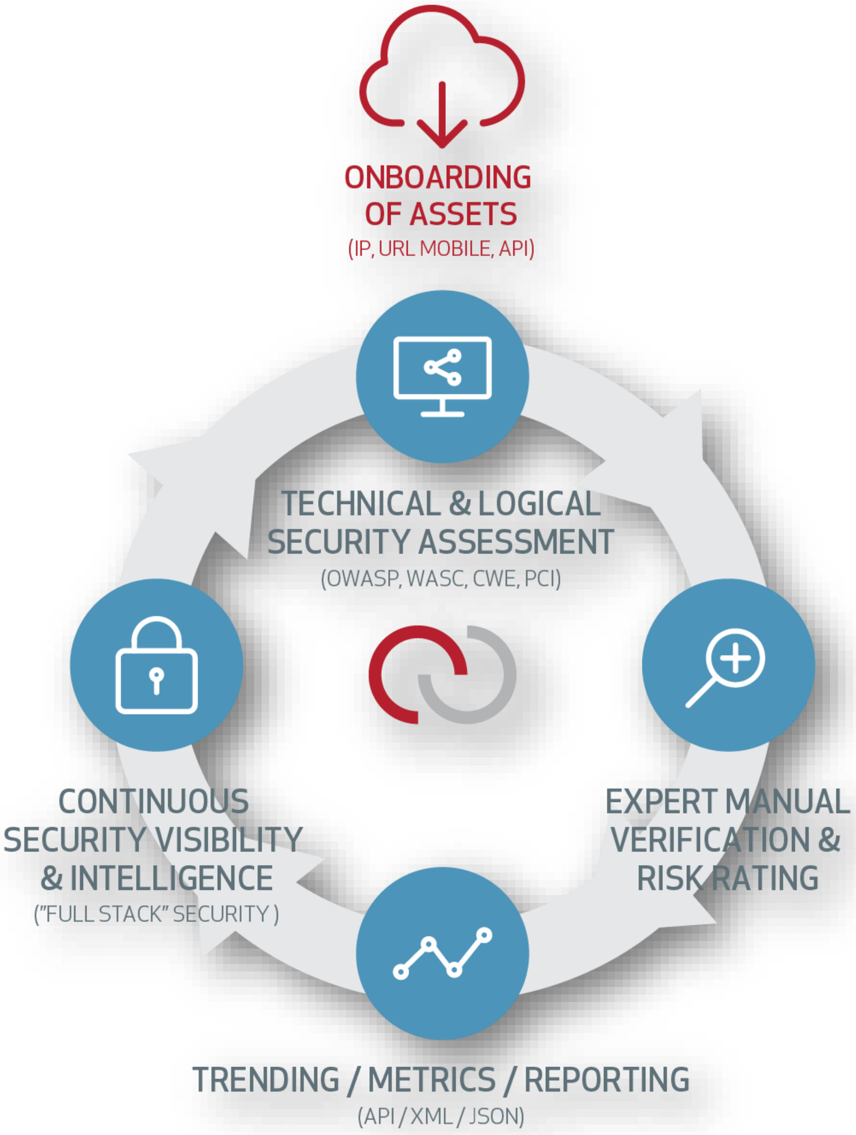
We perform continuous vulnerability assessments of all assets, as much or as little as you require. edgescan™ assessments cover both technical to logical testing and cover all OWASP vulnerabilities, WASC threat classification and CWE known vulnerabilities. edgescan™ also aligns and surpasses PCI compliance 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.

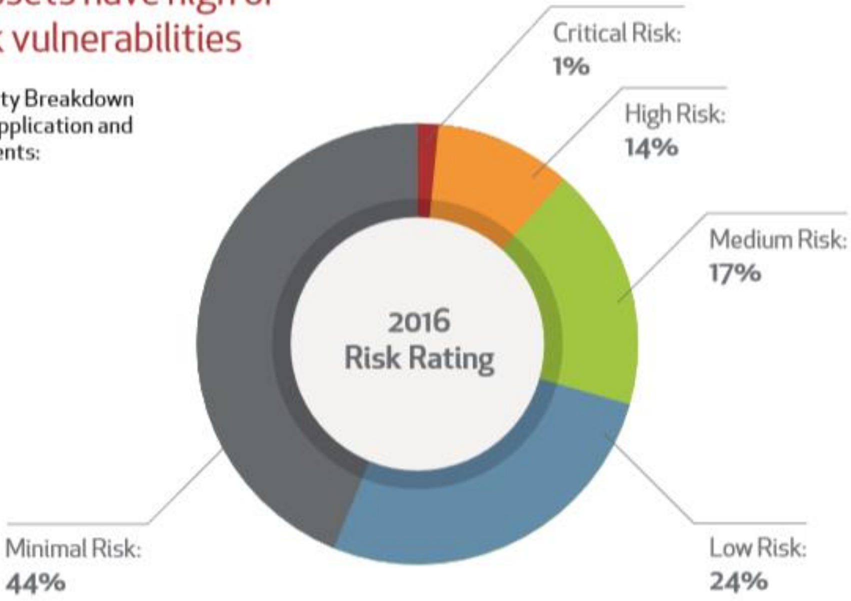

ONBOARDING OF ASSETS
(IP, URL MOBILE, API)
TECHNICAL & LOGICAL SECURITY ASSESSMENT
(OWASP, WASC, CWE, PCI)
EXPERT MANUAL VERIFICATION & RISK RATING
TRENDING / METRICS / REPORTING
(API / XML / JSON)
CONTINUOUS SECURITY VISIBILITY & INTELLIGENCE
("FULL STACK" SECURITY)

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:

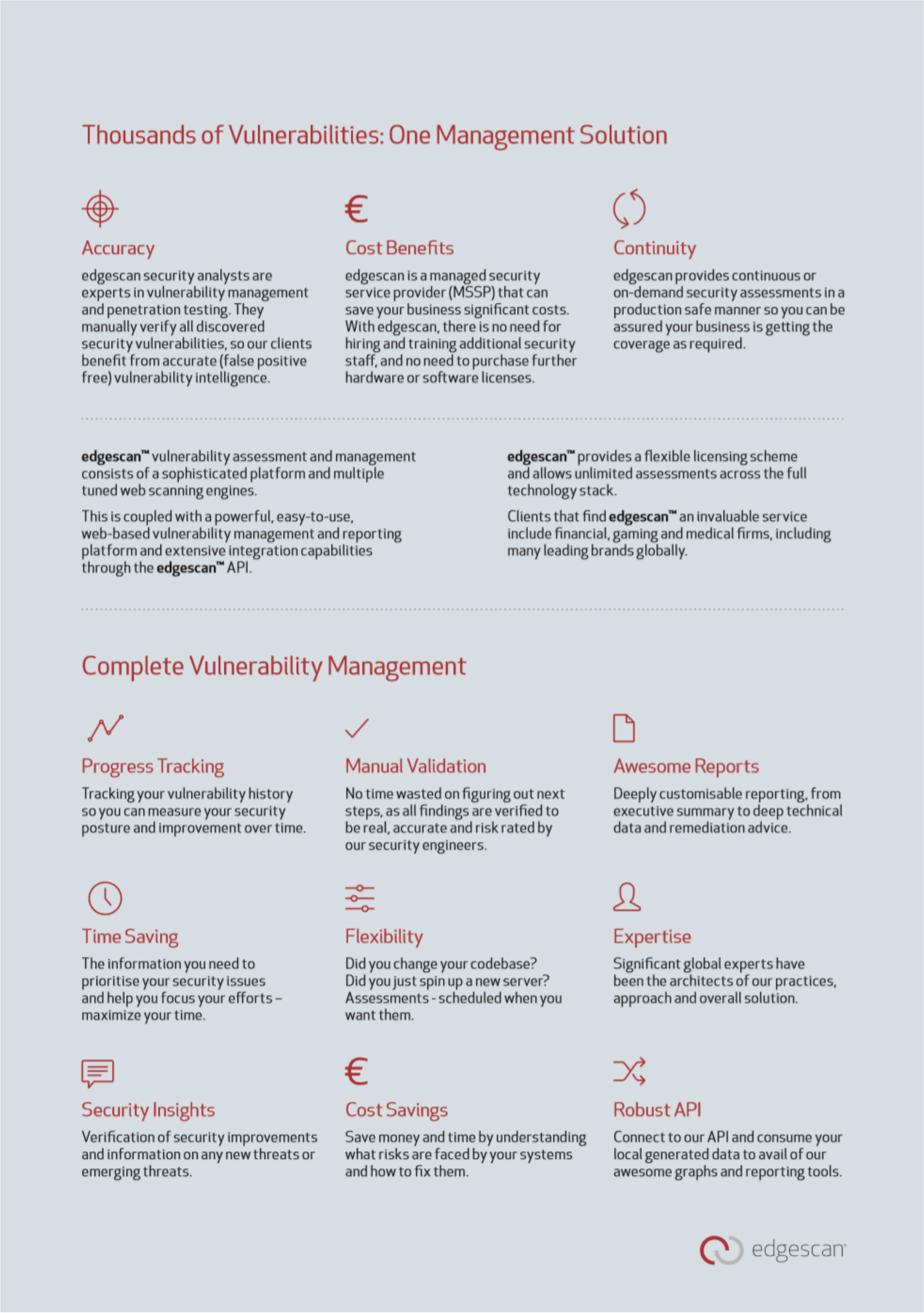


High or critical vulnerabilities are defined as:

- 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

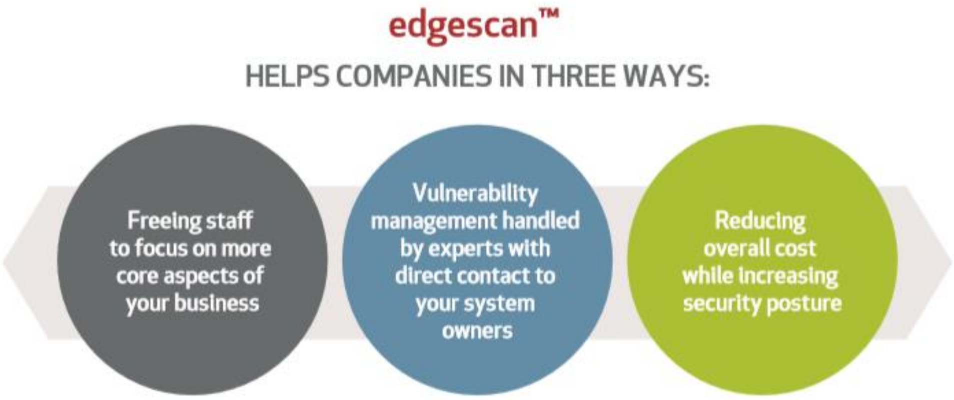
Connect to our API and consume your local generated data to avail of our awesome graphs and reporting tools.

edgescan™

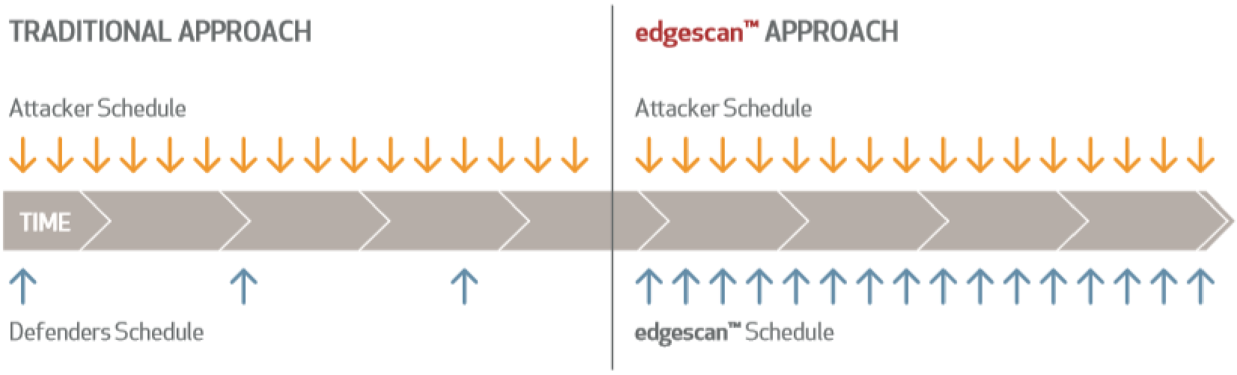
1.6 Experts in Vulnerability Management

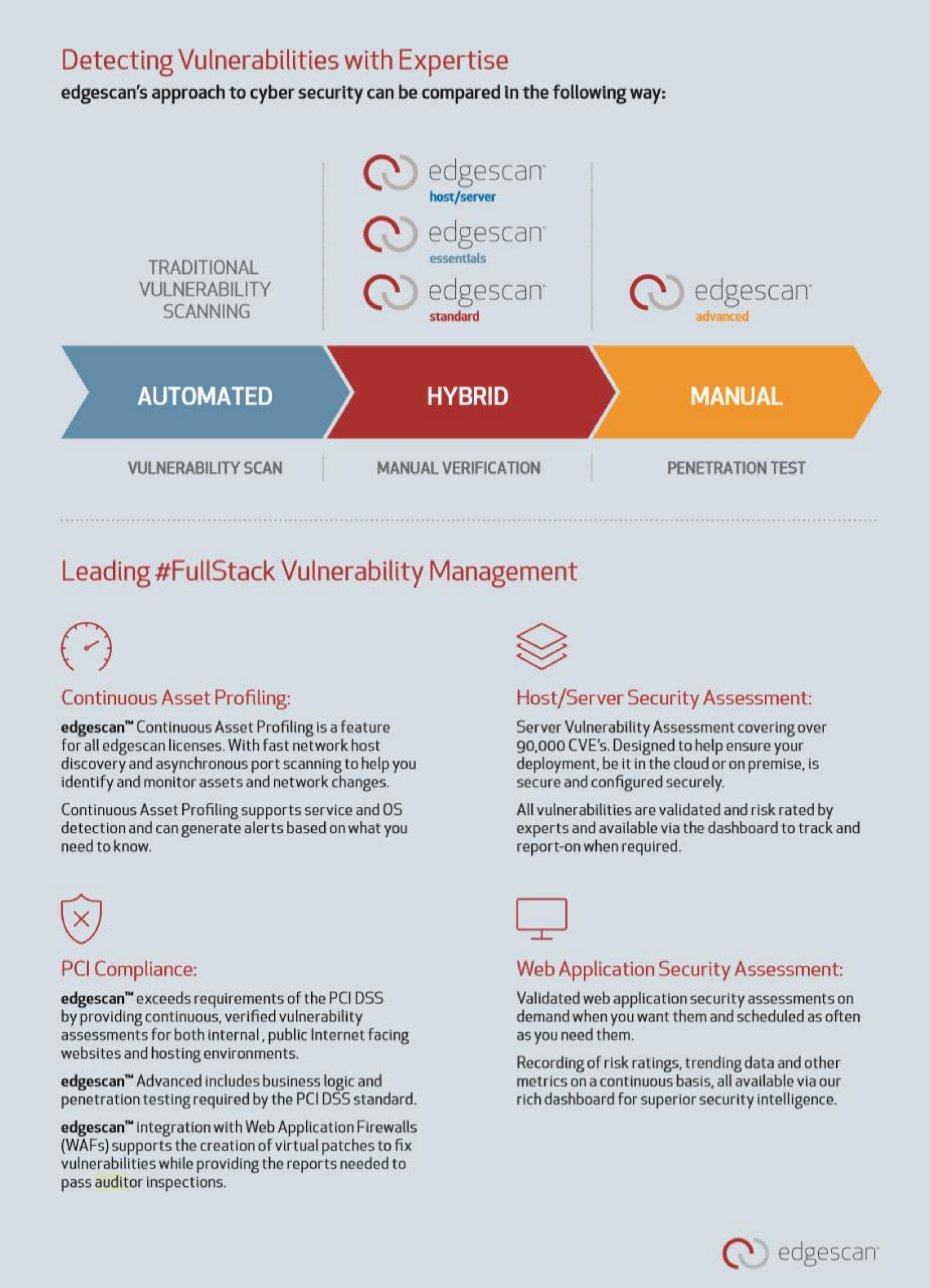
edgescan™ Fullstack Vulnerability Management helps companies to get the most from their vulnerability scanning and management requirements.

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:
Freeing staff to focus on more core aspects of your business
Vulnerability management handled by experts with direct contact to your system owners
Reducing overall cost while increasing security posture

1.7 edgescan™ Approach





Detecting Vulnerabilities with Expertise

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

TRADITIONAL VULNERABILITY SCANNING
edgescan host/server
edgescan essentials
edgescan standard
edgescan advanced
AUTOMATED
HYBRID
MANUAL
VULNERABILITY SCAN
MANUAL VERIFICATION
PENETRATION TEST

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.

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.

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.

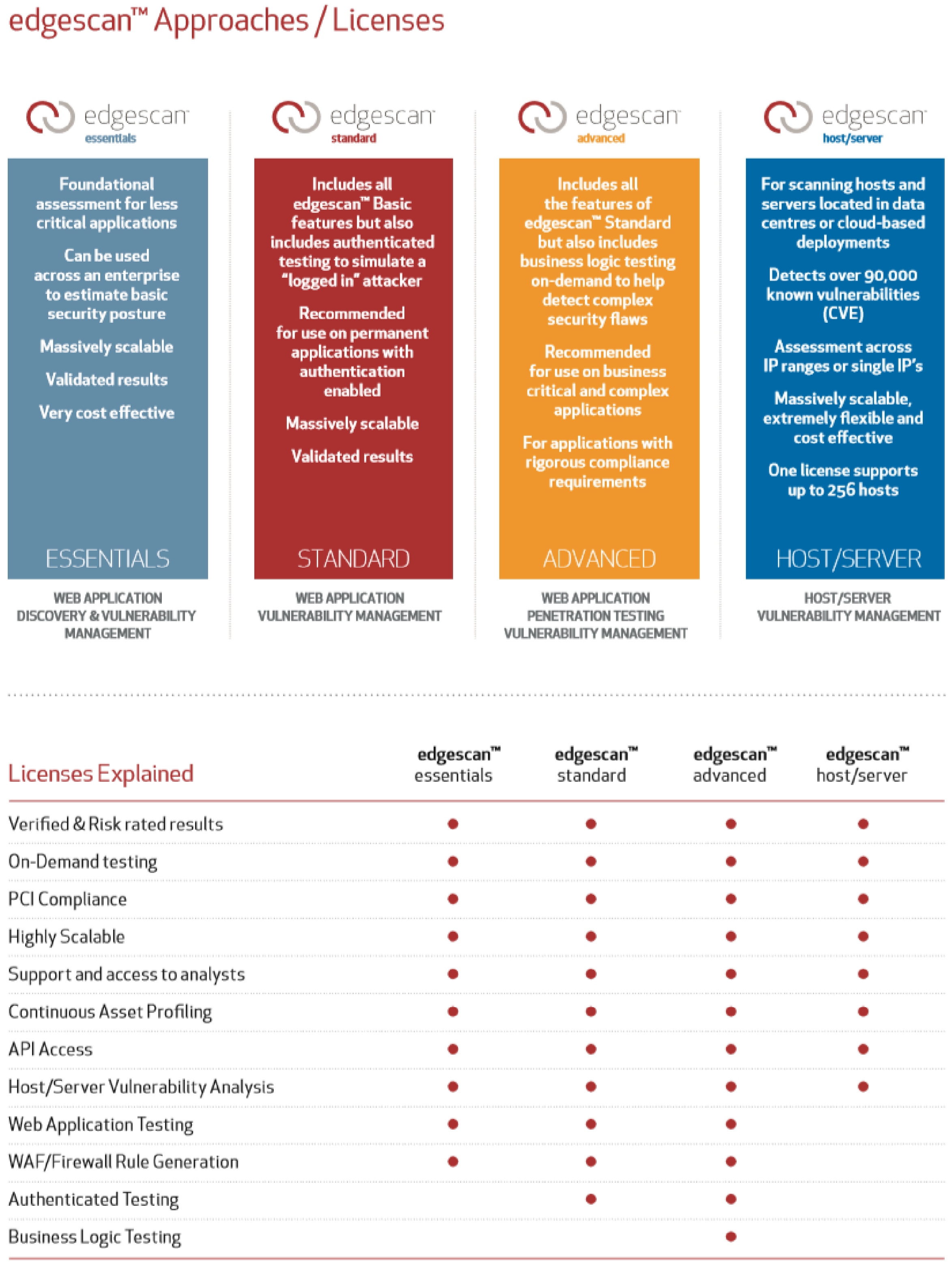
All vulnerabilities are validated and risk rated by experts and available via the dashboard to track and report-on when required.

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



edgescan™ Approaches / Licenses

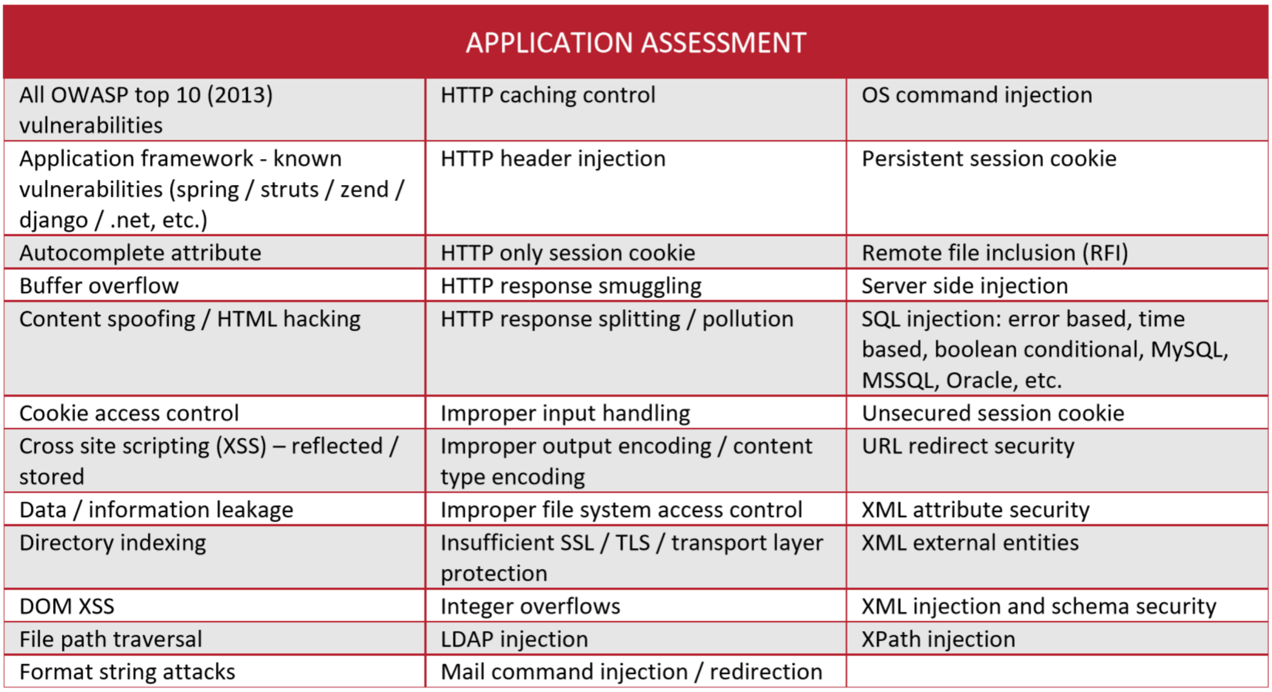
edgescan essentials	edgescan standard	edgescan advanced	edgescan host/server
Foundational assessment for less critical applications Can be used across an enterprise to estimate basic security posture Massively scalable Validated results Very cost effective	Includes all edgescan™ Basic features but also includes authenticated testing to simulate a "logged in" attacker Recommended for use on permanent applications with authentication enabled Massively scalable Validated results	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	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
ESSENTIALS	STANDARD	ADVANCED	HOST/SERVER
WEB APPLICATION DISCOVERY & VULNERABILITY MANAGEMENT	WEB APPLICATION VULNERABILITY MANAGEMENT	WEB APPLICATION PENETRATION TESTING VULNERABILITY MANAGEMENT	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			●	

1.8 Application Security

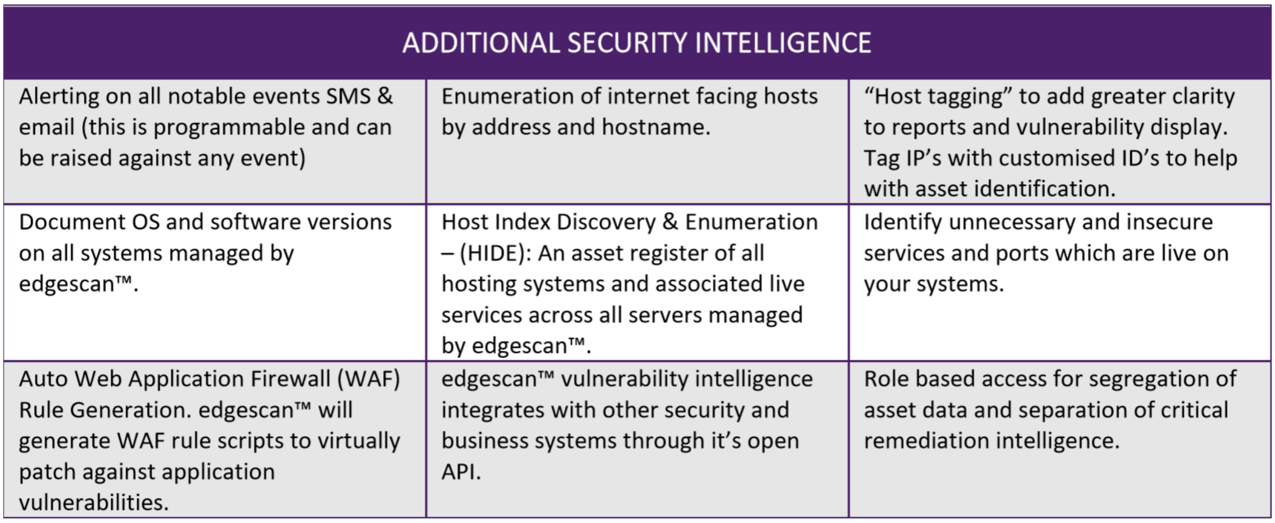
The global application security testing industry is changing. Applications and application programming interfaces are critical to every facet of our private and corporate daily lives. To meet this changing paradigm, edgescan™ offers continuous Dynamic Application Security Testing (DAST) integrated with deep dive, business logic penetration testing through our edgescan™ advanced licence. This combination of automation and manual testing on one platform allow enterprises meet the ever-increasing demand for accurate and useful Application Security Testing (AST) intelligence. See details of our DAST and Business Logic Penetration Testing services below

1.8.1 edgescan™ standard / (DAST)



APPLICATION ASSESSMENT		
All OWASP top 10 (2013) vulnerabilities	HTTP caching control	OS command injection
Application framework - known vulnerabilities (spring / struts / zend / django / .net, etc.)	HTTP header injection	Persistent session cookie
Autocomplete attribute	HTTP only session cookie	Remote file inclusion (RFI)
Buffer overflow	HTTP response smuggling	Server side injection
Content spoofing / HTML hacking	HTTP response splitting / pollution	SQL injection: error based, time based, boolean conditional, MySQL, MSSQL, Oracle, etc.
Cookie access control	Improper input handling	Unsecured session cookie
Cross site scripting (XSS) – reflected / stored	Improper output encoding / content type encoding	URL redirect security
Data / information leakage	Improper file system access control	XML attribute security
Directory indexing	Insufficient SSL / TLS / transport layer protection	XML external entities
DOM XSS	Integer overflows	XML injection and schema security
File path traversal	LDAP injection	XPath injection
Format string attacks	Mail command injection / redirection	

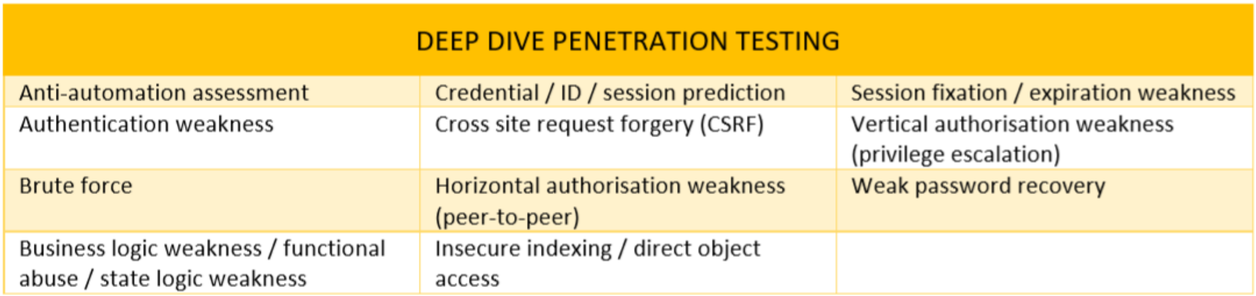
1.8.2 edgescan™ vulnerability intelligence



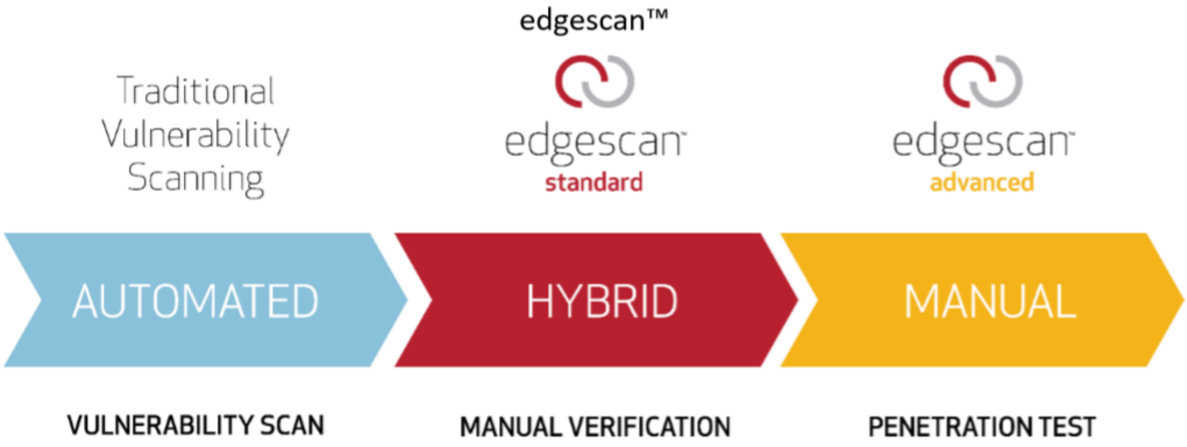
ADDITIONAL SECURITY INTELLIGENCE		
Alerting on all notable events SMS & email (this is programmable and can be raised against any event)	Enumeration of internet facing hosts by address and hostname.	“Host tagging” to add greater clarity to reports and vulnerability display. Tag IP’s with customised ID’s to help with asset identification.
Document OS and software versions on all systems managed by edgescan™.	Host Index Discovery & Enumeration – (HIDE): An asset register of all hosting systems and associated live services across all servers managed by edgescan™.	Identify unnecessary and insecure services and ports which are live on your systems.
Auto Web Application Firewall (WAF) Rule Generation. edgescan™ will generate WAF rule scripts to virtually patch against application vulnerabilities.	edgescan™ vulnerability intelligence integrates with other security and business systems through it’s open API.	Role based access for segregation of asset data and separation of critical remediation intelligence.

1.9 edgescan™ advanced (Penetration Testing)

In addition to the edgescan Standard (DAST) testing (above) penetration testing attempts to discover issues which scanners generally don’t detect. The discovery of such issues are unique to Penetration Testing or using an edgescan Advanced license as the issues are contextual and require human intelligence to discover and exploit.



DEEP DIVE PENETRATION TESTING		
Anti-automation assessment	Credential / ID / session prediction	Session fixation / expiration weakness
Authentication weakness	Cross site request forgery (CSRF)	Vertical authorisation weakness (privilege escalation)
Brute force	Horizontal authorisation weakness (peer-to-peer)	Weak password recovery
Business logic weakness / functional abuse / state logic weakness	Insecure indexing / direct object access	



1.10 edgescan™ Example Deployment

1.10.1 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.

1.10.2 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.

CYBER ESSENTIALS

TRUSTED PARTNER

Scottish Business Resilience Centre
Creating a secure Scotland for business to flourish in

POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

BARRIER NETWORKS

272 Bath Street, Glasgow G2 4JR | 0141 356 0101
info@barriernetworks.com | www.barriernetworks.com