TRADITIONAL PENTESTING IS DEAD

THE RISE OF ALWAYS-ON SECURITY

Tom Wedgbury, Managing Principal Security Consultant
David Parsons, Managing Principal Security Consultant

LRQA
Your Risk Management Advantage

LEADERSHIP SERIES

WHO ARE WE?

Tom Wedgbury

Managing Principal Security Consultant, LRQA

Dave Parsons

Managing Principal Security Consultant, LRQA

LRQA

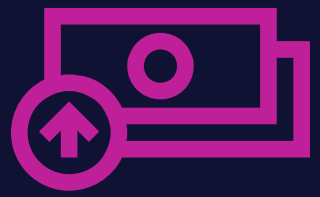
LEADERSHIP SERIES

THE DRIVERS

Why organisations do penetration testing

Compliance requirements

Regulatory audit requirements, e.g. PCI DSS, ISO 27001, CHECK



Cyber insurance

Policy requirements and premium reductions

Business assurance

Board & executive confidence, due diligence for M&A

LRQA

LEADERSHIP SERIES

EVOLUTION OF THREATS

Then vs Now: the security landscape has transformed

20 years ago

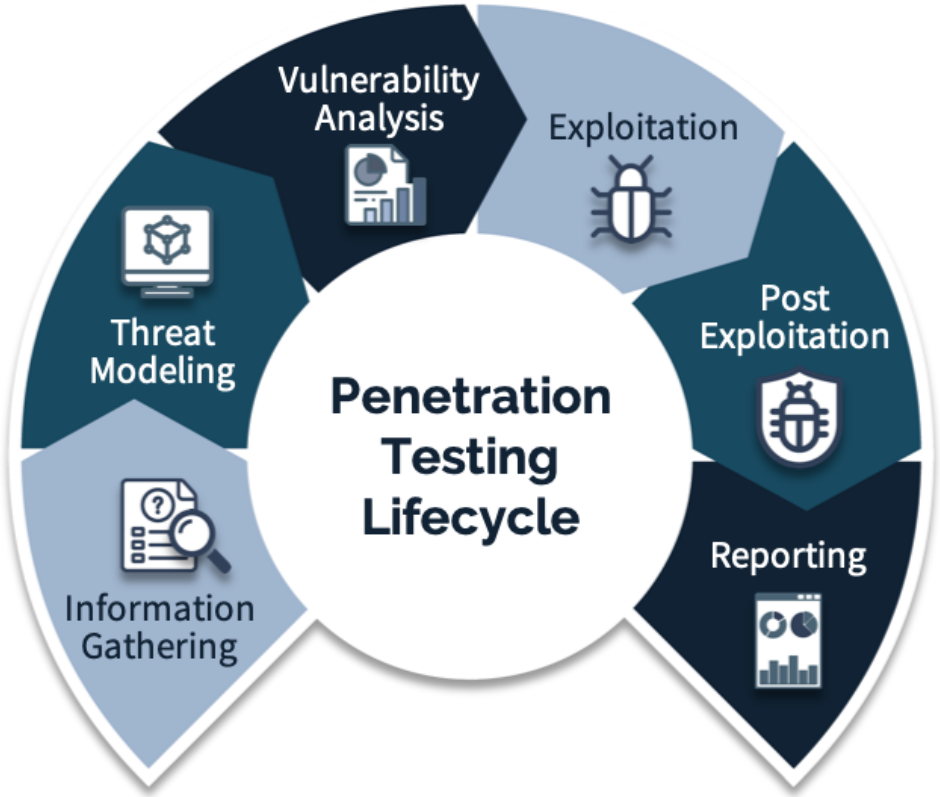
- Predictable, slow-moving threats
- Limited attack surface
- Annual security reviews were sufficient
- Attackers were mostly opportunistic

Today

- Cloud-first, borderless environments
- Nation-state actors and organised crime
- Exponential growth in attack surface
- Threats evolve faster than annual cycles
- AI-powered, automated attack tools

THE TRADITIONAL APPROACH

Point-in-time penetration testing



- **Defined scope** – systems to be tested agreed upfront.
- **Fixed timeframe** – a few days to a few weeks.
- **Repeated periodically** – often an annual cycle.

LRQA

LEADERSHIP SERIES

THE TRADITIONAL APPROACH

Point-in-time penetration testing

- Where traditional penetration testing excels:
  - Deep dive analysis
  - Clear remediation path
  - Meet compliance requirements
  - Expert-led insights

- Limitations of traditional penetration testing:
  - Snapshot in time
  - Blind spots
  - Rigid and costly remediation cycles

LRQA

LEADERSHIP SERIES

THE KEY CHALLENGE

Diminishing returns of annual testing

- Your attack surface changes daily
- Over 40,000 new CVEs discovered in 2024
- Average time to exploit is 5 days
- Many organisations test annually
- Threat actors operate 24/7

LRQA

LEADERSHIP SERIES

A REALITY CHECK

Your last pentest is already obsolete

How many systems changed or have been introduced since your last pen test?

- None
- <10
- 10-50
- 50+
- I don't know

How many new vulnerabilities have been discovered in your systems since?

- None
- <10
- 10-50
- 50+
- I don't know

How confident are you in your security posture right now?

- High Confidence
- Moderate Confidence
- Low Confidence
- No Confidence

LRQA

LEADERSHIP SERIES

A REALITY CHECK

Your last pentest is already obsolete

Interactive Poll

- How many systems changed or have been introduced since your last pen test?
  - **Options**: None, <10, 10-50, 50+, I don't know

- How many new vulnerabilities have been discovered in your systems since?
  - **Options**: None, <10, 10-50, 50+, I don't know

- How confident are you in your security posture right now?
  - **Options:** High Confidence, Moderate Confidence, Low Confidence, No Confidence

LRQA

LEADERSHIP SERIES

THE RISE OF ALWAYS-ON SECURITY

CONTINUOUS ASSURANCE

LEADERSHIP SERIES

TRANSFORMING THE APPROACH

The role of continuous assurance

- **Move from reactive to proactive cybersecurity**
  - Prevent threats instead of chasing them
- **Replace snapshots with continuous monitoring**
  - Step beyond annual testing towards always-on assurance
- **Know about threats as they emerge**
  - Real-time vulnerability notifications

LRQA

LEADERSHIP SERIES

IDENTIFYING YOUR TRUE ATTACK SURFACE

The benefits of continuous assurance

Challenge

You can’t protect what you don’t know exists.

Continuous assurance

- Discover shadow IT and forgotten assets.
- Monitor for new systems automatically.
- Identify exposed ports and misconfigurations.
- Build the foundation for all security testing.

LRQA

LEADERSHIP SERIES

STAYING AHEAD OF THREAT ACTORS

The benefits of continuous assurance

Challenge

Security confidence drops after annual testing.

Continuous assurance

- Maintain high security confidence year-round.
- Respond to new vulnerabilities immediately.
- Proactive defence, not reactive patching.
- Close the gap between discovery and remediation.

LRQA

LEADERSHIP SERIES

MAXIMISING YOUR RETURN ON INVESTMENT

The benefits of continuous assurance

Challenge

Budget constraints make frequent traditional testing cost-prohibitive.

Continuous assurance

- Prevent security incidents before they happen.
- Smart use of AI and automation reduces costs.
- Enhance human expertise without replacing it.
- Faster remediation cycles save time and money.

LRQA

LEADERSHIP SERIES

WHAT THIS LOOKS LIKE IN PRACTICE

LEADERSHIP SERIES

LEADERSHIP SERIES

CONTINUOUS ASSURANCE

Six pillars of always-on assurance

1

Attack Surface Management

We constantly identify and monitor your internet-facing assets. This shows your exposure to vulnerabilities.

2

Penetration Testing

We ensure you get a full and thorough initial penetration test.

3

Targeted Testing

For when your organisation makes system changes ensuring fixes are verified in real time.

4

Unlimited Retesting

When you are ready to retest identified vulnerabilities you can do so an unlimited number of times.

5

Vulnerability Assessment

We scan your systems every month and our experts filter and validate the results for you.

6

Vulnerability Hunting

If a global vulnerability (like MOVEit) hits, we search your systems to check if you are affected.

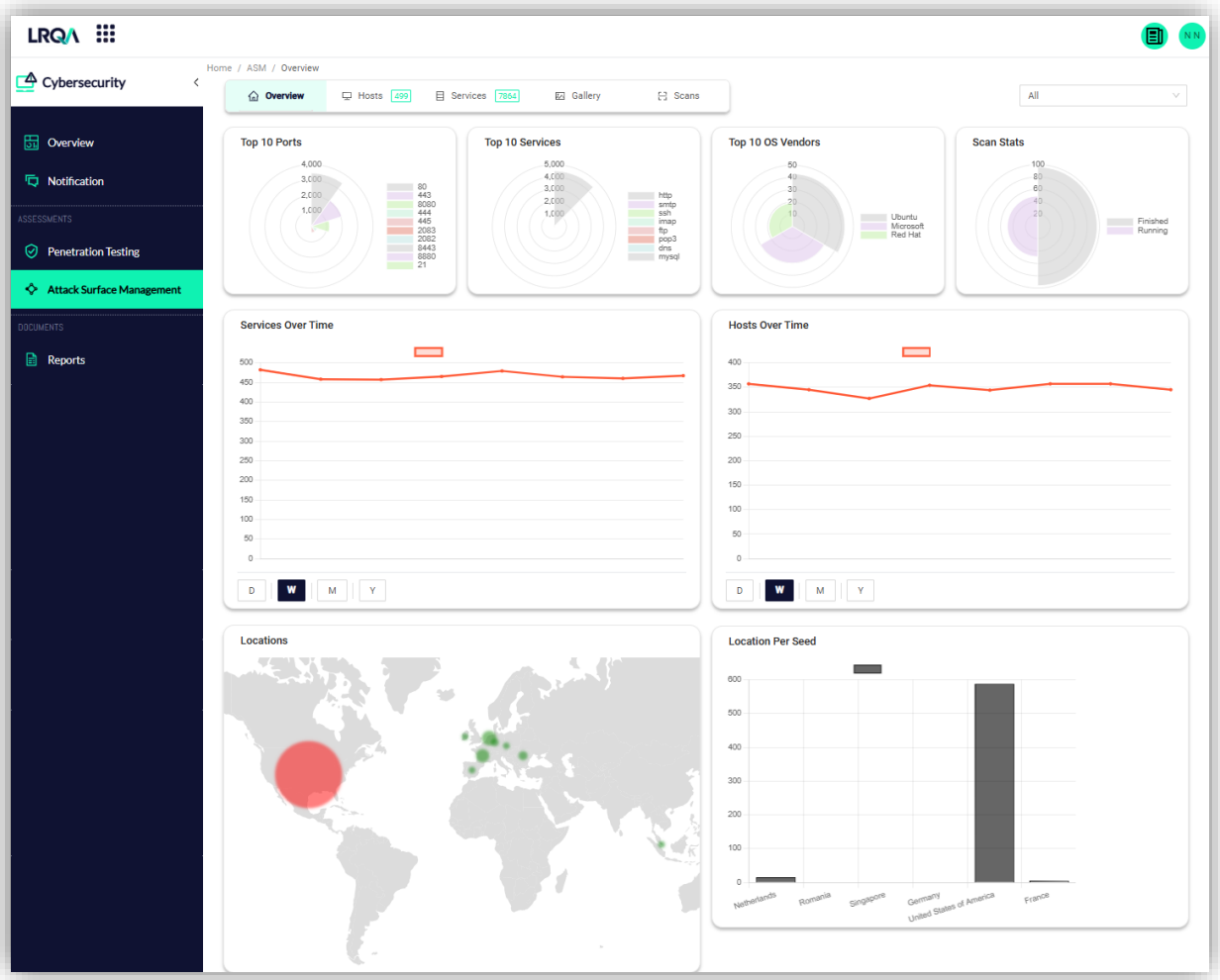
LRQA

LEADERSHIP SERIES

ATTACK SURFACE MANAGEMENT

You can't protect what you don't know exists

- Continuously monitor your internet-facing infrastructure
- Classify assets by business importance and risk level
- Feed discovered assets into penetration testing and vulnerability assessment



LRQA

LEADERSHIP SERIES

ATTACK SURFACE MANAGEMENT

Case study

Challenge

Leading digital media company with limited visibility across multiple brands and acquisitions.

Continuous assurance

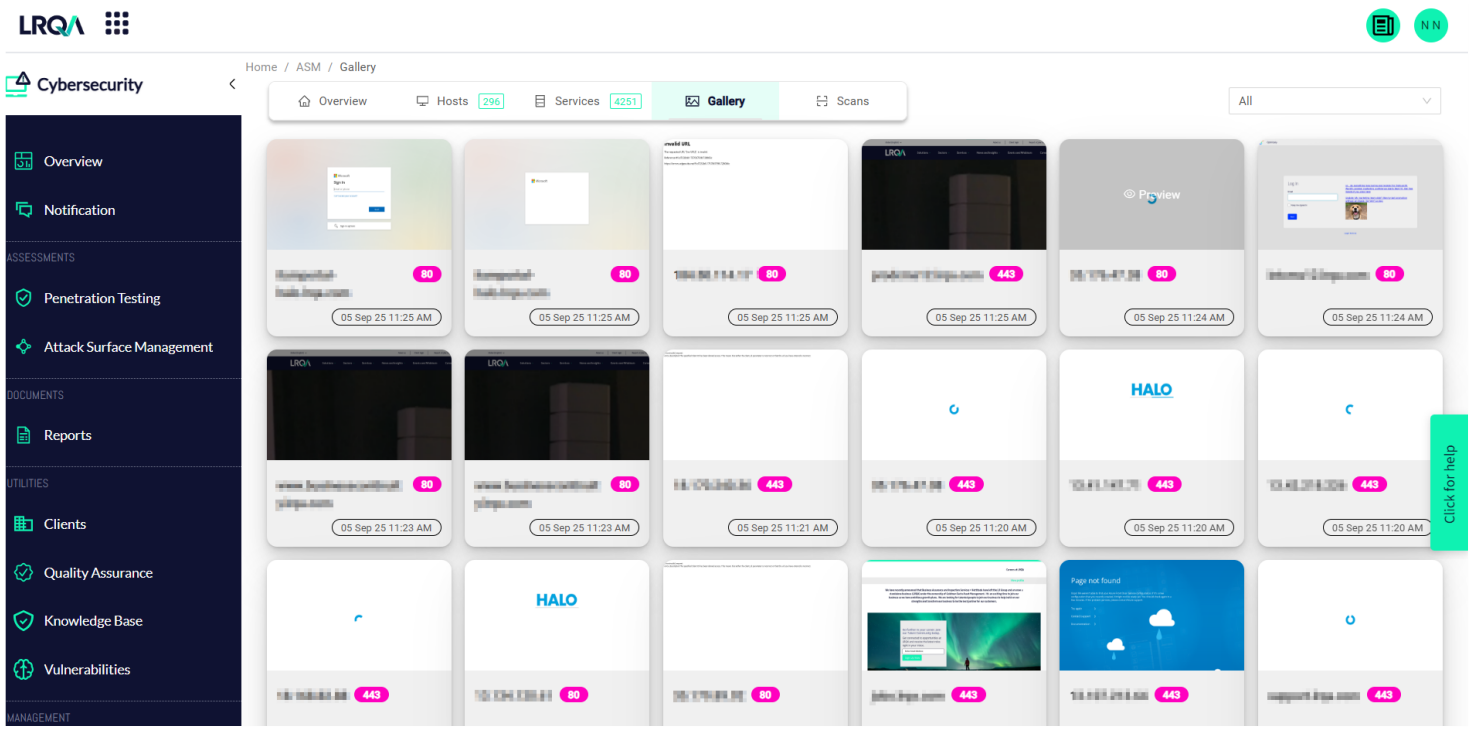
- **Discovery** – ASM identified over 100 unknown subdomains.
- **Critical finding** – Compromised subdomain redirecting customers to illegal gambling site with explicit content.
- **Impact** – Brand reputation, regulatory compliance, and advertiser relationships protected through rapid remediation.

LRQA

LEADERSHIP SERIES

ATTACK SURFACE MANAGEMENT

Case study



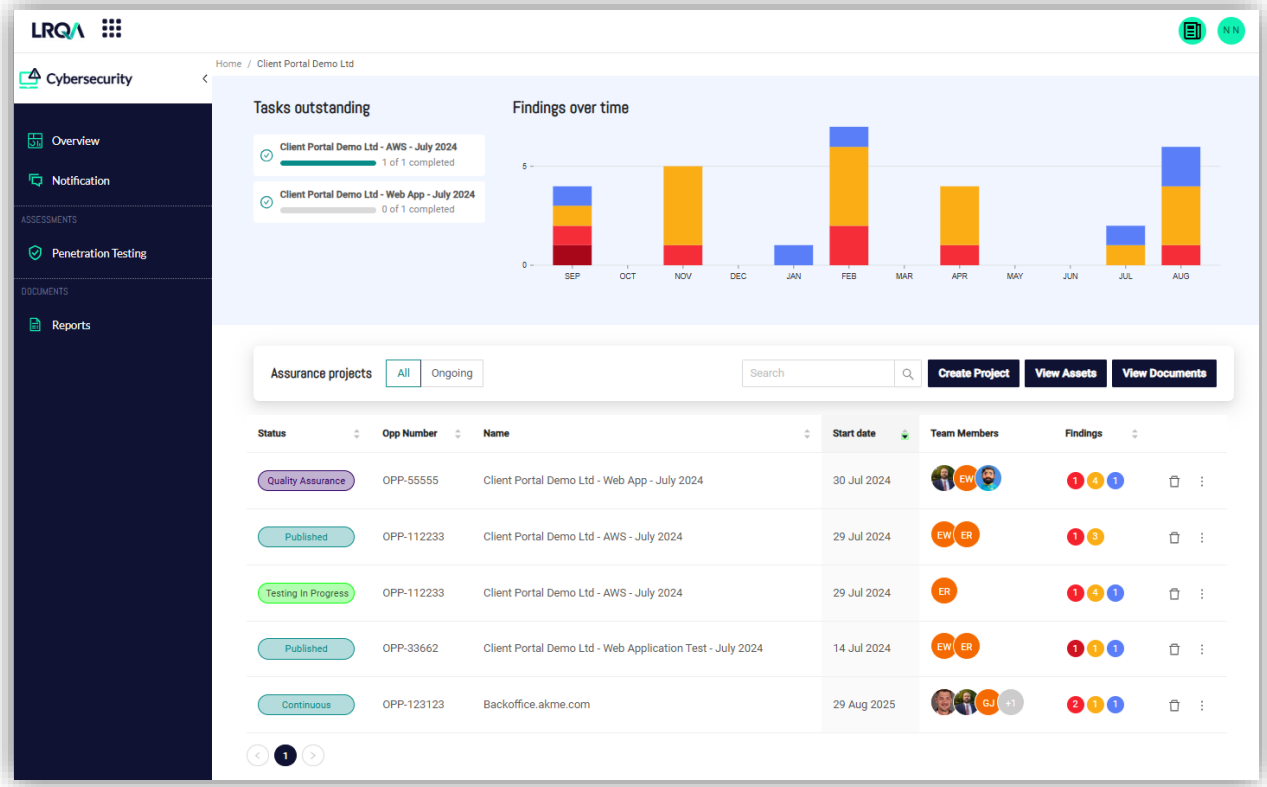
LRQA

LEADERSHIP SERIES

PENETRATION TESTING

Providing depth of coverage

- Human-led penetration testing should always play a part in your assurance program.
- This provides you with a clear, current view of your security posture, focusing on vulnerabilities.
- Meets regulatory and compliance testing requirements.



LRQA

LEADERSHIP SERIES

CLIENT FEEDBACK

Agility	Rapid deployment of testing resources. Remediation testing scheduled immediately rather than waiting for new engagement windows.
Quicker Assurance	Validation of security fixes happens within days, not months. No delays between remediation efforts and security confirmation.
Reduced Cost	Eliminates costly retest procurement and scheduling. Unlimited retesting included prevents budget overruns from multiple engagement cycles.
Better Visibility	Continuous monitoring of your digital footprint including shadow IT assets. Real-time tracking of URLs, IPs, and newly discovered infrastructure.
Surprises	Proactive discovery of unknown assets and exposures. Identifies forgotten systems, abandoned applications, and unmanaged infrastructure before attackers do.

LRQA

THE RISE OF ALWAYS-ON SECURITY

WHY THE URGENCY?

LEADERSHIP SERIES

AI – THE CHALLENGE

Human-led testing is not enough

Attackers: *24/7, automated, evolving*

Defenders: *Periodic, manual, reactive*

LRQA

LEADERSHIP SERIES

AI – THE SOLUTION

How continuous assurance and automated testing can help

Speed and Scale

Match attacker pace with always on vulnerability discovery

Deeper Analysis

Maintain up to date register of public facing assets

Continuous

On-demand testing when you need it, not when the calendar says

The Future

On demand AI Pentesting of all public facing assets.

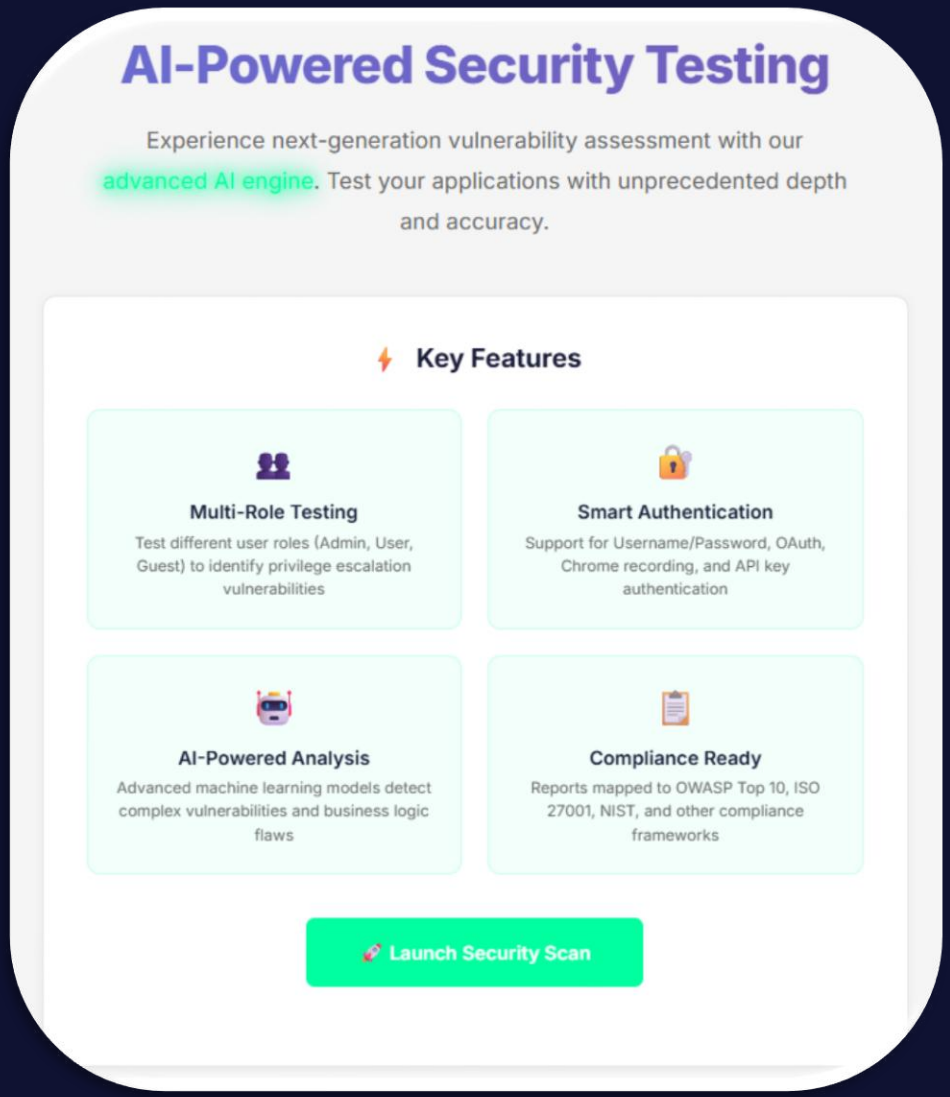
LRQA

LEADERSHIP SERIES

AI – The Future

Automated on Demand Human Augmented Pentesting

- On demand automated pentesting solution for all of your digital assets
- Continuous security validation without waiting for manual tests
- Scalable and cost-effective compared to traditional Pentesting
- Stay compliant and audit-ready with automated reports



Start Security Scan

AI-Powered Security Testing

Experience next-generation vulnerability assessment with our advanced AI engine. Test your applications with unprecedented depth and accuracy.

Key Features

Multi-Role Testing
Test different user roles (Admin, User, Guest) to identify privilege escalation vulnerabilities

Smart Authentication
Support for Username/Password, OAuth, Chrome recording, and API key authentication

AI-Powered Analysis
Advanced machine learning models detect complex vulnerabilities and business logic flaws

Compliance Ready
Reports mapped to OWASP Top 10, ISO 27001, NIST, and other compliance frameworks

Launch Security Scan

THE RISE OF ALWAYS-ON SECURITY

KEY TAKEAWAYS

LEADERSHIP SERIES

WHAT THIS MEANS FOR YOU

The strategic implications

Threats have evolved
Annual testing no longer matches the pace of modern threats.

Gain a competitive advantage
Continuous assurance enables faster, safer innovation.

Level the playing field
Augment human expertise with always-on testing.

The false economy
Hidden costs make annual testing the expensive option.

YOUR NEXT STEPS

Moving from annual to always-on security

1. Assess your current attack surface – understand what you're really protecting.

2. Evaluate your exposure window – map new vulnerabilities against the time since your last test.

3. Determine your level of assurance – are you truly confident in your current security?

4. Calculate your ROI – include all hidden costs and business risks.

5. Pilot continuous assurance – measure the difference in time to detection and remediation.

LRQA

LRQA
Your Risk Management Advantage

THANK YOU

Any questions?

Tom Wedgbury | tom.wedgbury@lrqa.com
Dave Parsons | david.parsons@lrqa.com

LEADERSHIP SERIES