

## CASE STUDY

# St. Paul's Cathedral



## Fortifying a national treasure with continuous penetration testing

### About the customer

St Paul's Cathedral is a London icon and national treasure, designed by Sir Christopher Wren in the late 17th century and serving as the cathedral church of the Diocese of London for over 1,400 years. The site welcomes thousands of visitors annually and supports c.200 staff who manage services, events, archives and day-to-day operations.

### The challenge

St Paul's had previously received basic external penetration testing but needed a more comprehensive, continuous approach as cyber threats evolved. The cathedral operates a mixture of public-facing systems and internal platforms (including Azure) that, if compromised, could impact confidentiality, integrity and availability of critical data, visitor services, and reputation. Leadership wanted actionable intelligence about current gaps, a programme they could trust, and assurance of ongoing protection.

### At a glance

**Industry:** Travel & Tourism

**Employees:** 101-200

**Solutions:** CyberGuard



*"We are so happy with our partnership with Wavenet, with them providing our pen testing. They really know their stuff and in this ever-changing landscape of cyber security, it makes us at St Paul's feel more secure and future ready. They are wonderful to deal with, and we have a great relationship."*

**Garry Hunter**

Head of Information Technology, St. Paul's Cathedral.

### The solution

We delivered a continuous, accredited security testing programme tailored to St. Paul's Cathedral's complex estate and operational needs. This includes:

- Quarterly external penetration testing targeting public-facing systems, with findings assessed for exploitability and impact against confidentiality, integrity, and availability.
- Annual internal penetration testing to uncover internal attack paths and privilege-escalation risks.

- Azure configuration reviews of the cathedral's middleware to identify and remediate cloud misconfigurations.
- Prioritised, actionable remediation guidance and clear risk ratings so St. Paul's could focus limited resources on the highest-impact fixes.
- Follow-up validation testing to confirm remediations and demonstrate measurable improvement.
- Delivery by our CHECK-and CREST-approved UK penetration testing team, providing independent, recognised assurance for governance and regulatory needs.

*“Wavenet’s penetration testing has given us clear, practical insight into our security posture. Their expertise, clarity of reporting and ongoing support mean we can make informed decisions and continually strengthen our defences with confidence.”*

**Garry Hunter**

Head of Information Technology, St. Paul's Cathedral.

## The result

- Improved security posture: recurring external and internal tests plus Azure configuration reviews closed critical gaps previously unknown to St. Paul's Cathedral, protecting staff and visitors.
- Continuous risk visibility: quarterly and annual testing provides timely intelligence on emerging threats and configuration weaknesses.
- Compliance and assurance: CHECK and CREST accreditation delivers independent and documented assurance for governance and regulatory purposes.
- Operational resilience: fixes reduced the likelihood of disruption to services, protecting visitor experience and cathedral operations.
- Reputation protection: proactive security reduces exposure to public incidents that could harm an iconic institution.
- Cost avoidance and prioritised remediation: focused findings enabled St Paul's to apply resources where they mattered most, avoiding more costly breaches.
- Peace of mind: cathedral leadership gained confidence that they are better prepared and future-ready against cyber threats.

Ready to make your business tech simpler and smarter?

Talk to us

Let's talk **0344 863 3000**

enquiries@wavenet.co.uk  
wavenet.co.uk

wavenet