Case study

INFOVISION
#AccelerateDigital

Strategic cloud security transformation for a UK-based accounting software provider

Strengthening security for a UK-based SaaS accounting platform

InfoVision enabled a connected cloud accounting platform provider in the UK to enhance its security infrastructure and achieve PCI DSS compliance. Through extensive VAPT and DAST on its critical cloud assets and SaaS application, the customer was able to mitigate risks and deliver secure, reliable services.

About the customer

Our customer stands as an innovative technology partner for small and medium-sized accountancy practices in UK. Their platform combines automated accounts production with robust practice management tools, empowering accountants to operate smarter, more efficiently, and with higher profitability.

* Vulnerability Assessment and Penetration Testing (VAPT)
* Dynamic Application Security Testing (DAST)
* Health Insurance Portability and Accountability Act (HIPAA)

© InfoVision, Inc. All Rights Reserved.

Business need

The BFI digital landscape's evolving threat matrix demands a proactive security approach. Our customer recognized that maintaining technological leadership necessitated an uncompromising commitment to cybersecurity. Their strategic objectives transcended traditional security parameters:

- **Comprehensive vulnerability detection:**
  Conducting a forensic examination of potential risks across web applications and cloud infrastructure
- **Regulatory compliance assurance:**
  Achieving and maintaining rigorous PCI DSS standards
- **Operational resilience:**
  Guaranteeing uninterrupted, secure data availability and service delivery for accounting professionals

Importance of VAPT and DAST

Beyond traditional security measures, VAPT and DAST represent a proactive, intelligent defense strategy:

- **Predictive risk management:**
  Identifying and neutralizing vulnerabilities before they can be exploited
- **Regulatory intelligence:**
  Dynamically aligning with evolving compliance frameworks
- **Adaptive security architecture:**
  Building robust, responsive defense mechanisms
- **Operational continuity:**
  Minimizing potential service disruptions

Solution delivered

Strategic scoping

Meticulously mapping stakeholder ecosystems and critical asset landscapes.

Hybrid testing methodology

Integrating advanced automated scanning with expert manual penetration testing.

Intelligent risk prioritization

Delivering granular, actionable vulnerability insights.

Collaborative remediation

Engaging customer teams through structured, solution-oriented brainstorming sessions to close critical vulnerabilities effectively.

Re-validation for assurance

Conducted follow-up assessments to ensure critical issues were resolved.

© InfoVision, Inc. All Rights Reserved.

Tech stack

Tools leveraged:
Qualys, Nessus, Burp Suite Pro, Metasploit, Kali Linux

Compliance framework:
PCI DSS

Key outcomes

Strengthened cloud security

Reduced exposure to critical vulnerabilities, ensuring robust protection for infrastructure and applications.

Seamless regulatory compliance

Full alignment with PCI DSS requirements

Enhanced operational reliability

Significant improvements in system stability and uptime

Elevated stakeholder confidence

Reinforced trust among customers and partners through demonstrable security commitment.

© InfoVision, Inc. All Rights Reserved.