

## How Silverse minimized financial risk and enhanced stakeholder confidence for a major bank in Qatar

A major bank in Qatar introduced multiple smart technologies and business applications to improve operational efficiency and customer experience. This increased the organization's attack surface, leaving it vulnerable to significant financial, regulatory, and reputational risks.

### The Challenge

1. Identifying vulnerabilities within internal and internet-facing business applications.
2. Ensuring compliance with regulatory requirements, internal security policies, and cybersecurity best practices while minimizing operational downtime and risk.
3. Assessing the security posture of CCTV infrastructure and enterprise network components.
4. Securing newly deployed smart devices, which were vulnerable to attacks.
5. Validating the effectiveness of existing security controls and security configurations.

### The Solution

1. Security assessment of smart devices, CCTV infrastructure, supporting management systems, and network infrastructure.
2. Vulnerability Assessment and Penetration Testing (VAPT) for internal and client-facing business applications to identify exploitable vulnerabilities before potential attackers could leverage them.
3. Risk-based prioritization of identified findings with detailed remediation recommendations.
4. Validation of security controls.
5. Executive reporting and technical remediation guidance.

### The Impact

#### Minimized financial risk

Resulting from enhanced cyber resilience.

1

#### Protection of customer data and critical assets

Via strengthened security controls.

2

#### Increased stakeholder and regulator confidence

Through independent security validation.

3

#### Improved brand reputation

By demonstrating a proactive and mature approach to cybersecurity risk management.

4

#### Minimized regulatory risk

Achieved "Green" compliance status against internal governance and regulatory requirements.

5