

XPERIOS SECURITY ASSURANCE STATEMENT

Security, Architecture & Compliance Overview

Product: Xperios Desktop Client & Azure-Hosted Services

Date: 11/02/2026

Document Version: 1.0

Prepared by:
Paritor Ltd
Winslade Park,
Manor Drive,
Clyst St Mary,
Exeter,
EX5 1FY

Table of Contents

1. Executive Summary
2. Security Approach in the Upgrade from Ensemble to Xperios
 - 2.1 Secure Development Lifecycle
 - 2.2 Threat Modelling
 - 2.3 Secure Deployment
3. Security Controls Protecting Customer Data
 - 3.1 Data Protection
 - 3.2 Identity & Access Management
 - 3.3 Network Security
 - 3.4 Monitoring & Logging
 - 3.5 Operational Security
4. Security Testing & Assurance
 - 4.1 Penetration Testing
 - 4.2 Vulnerability Scanning
5. ISO27001 Alignment
6. Integrations & Dependencies
 - 6.1 Azure-Native Services
 - 6.2 Third-Party Dependencies
 - 6.3 Integration Security Assurance
7. Architecture Overview (Diagram)
8. Data Flow Overview (Diagram)
9. Conclusion

1. Executive Summary

Xperios is the modern successor to the Ensemble platform, designed with a security-first mindset and built entirely on Microsoft Azure's enterprise-grade cloud infrastructure. This document provides assurance regarding the security controls, testing processes, and architectural safeguards that protect customer data and ensure the resilience of the Xperios platform.

2. Security Approach in the Upgrade from Ensemble to Xperios

2.1 Secure Development Lifecycle (SDL)

All development is performed within Azure DevOps, following a structured SDL:

- Protected branches and gated pull requests
- Mandatory peer reviews
- Automated static code analysis (SAST)
- Dependency scanning (SCA)
- Secret-detection tooling
- MFA and RBAC enforced for all DevOps operations
- Full audit trails for code and deployment activities

2.2 Threat Modelling

- Formal threat-modelling exercises conducted during redesign
- Risks such as data exposure, privilege escalation, and API misuse identified early
- Mitigations embedded into design and user stories

2.3 Secure Deployment

- Azure DevOps release pipelines with signed artefacts
- Infrastructure-as-Code ensures consistent, repeatable deployments
- Segregated environments with controlled promotion paths

3. Security Controls Protecting Customer Data

3.1 Data Protection

- TLS 1.2+ encryption for all data in transit
- AES-256 encryption for all data at rest
- Azure Key Vault for secrets, certificates, and encryption keys

3.2 Identity & Access Management

- Azure AD authentication
- MFA and conditional access
- RBAC across all services
- Least-privilege service identities

3.3 Network Security

- Azure Firewall and NSGs
- Private endpoints to minimise public exposure
- Azure DDoS Protection Standard

3.4 Monitoring & Logging

- Azure Monitor and Application Insights
- Microsoft Defender for Cloud for threat detection
- Audit logs retained and reviewed regularly

3.5 Operational Security

- Quarterly independent penetration testing
- Continuous vulnerability scanning
- Patch management aligned with Microsoft's update cadence

4. Security Testing & Assurance

4.1 Penetration Testing

Xperios undergoes quarterly penetration testing by an independent third-party provider. Testing covers:

- Authentication & session management
- API security
- Desktop client attack surface
- Azure infrastructure boundaries

All critical and high-severity findings are remediated before release.

4.2 Vulnerability Scanning

- Automated dependency scanning (SCA)
- Static Application Security Testing (SAST)
- Continuous infrastructure scanning via Microsoft Defender

5. ISO27001 Alignment

While Paritor Ltd does not currently hold ISO27001 certification, Xperios is built entirely on Microsoft Azure, which is certified under:

- ISO/IEC 27001
- ISO/IEC 27017
- ISO/IEC 27018
- SOC 1, SOC 2, SOC 3
- CSA STAR

Internal processes align with ISO27001 principles, including:

- Access control
- Change management
- Incident response
- Logging and monitoring
- Secure development practices

6. Integrations & Dependencies

6.1 Azure-Native Services

Xperios relies on secure, managed Azure services:

- Azure App Services
- Azure SQL / Cosmos DB
- Azure Storage
- Azure Key Vault
- Azure Active Directory
- Azure Monitor & Defender for Cloud

6.2 Third-Party Dependencies

- Standard .NET libraries
- Vetted NuGet packages
- Automated dependency scanning ensures no known CVEs

6.3 Integration Security Assurance

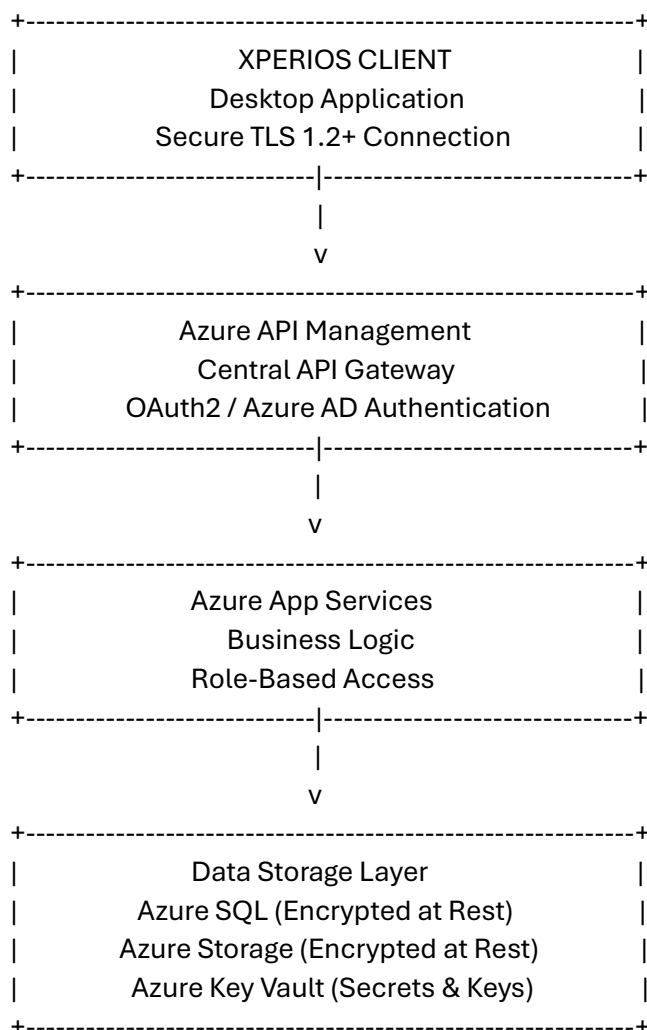
- All integrations included in quarterly penetration testing

- OAuth2 or signed tokens for API authentication
- Resilience testing ensures graceful degradation

7. Architecture Overview (Diagram Description)

You can paste this into Visio, PowerPoint, or draw.io to create a clean diagram.

Diagram Structure:



8. Data Flow Overview (Diagram Description)

1. User launches Xperios desktop client
2. Client authenticates via Azure AD (MFA enforced)
3. Client communicates with Azure API Management over TLS 1.2+
4. API Management validates tokens and routes requests
5. Azure App Services process business logic

6. Data retrieved from Azure SQL / Cosmos DB (AES-256 encrypted)
7. Logs and telemetry sent to Azure Monitor & Application Insights
8. Security events monitored by Microsoft Defender for Cloud

9. Conclusion

Xperios delivers a secure, modern, Azure-native platform that significantly enhances the security posture compared to Ensemble. With continuous penetration testing, Azure-backed compliance, and a robust secure development lifecycle, Xperios provides strong assurance that customer data remains protected, resilient, and aligned with industry best practices.