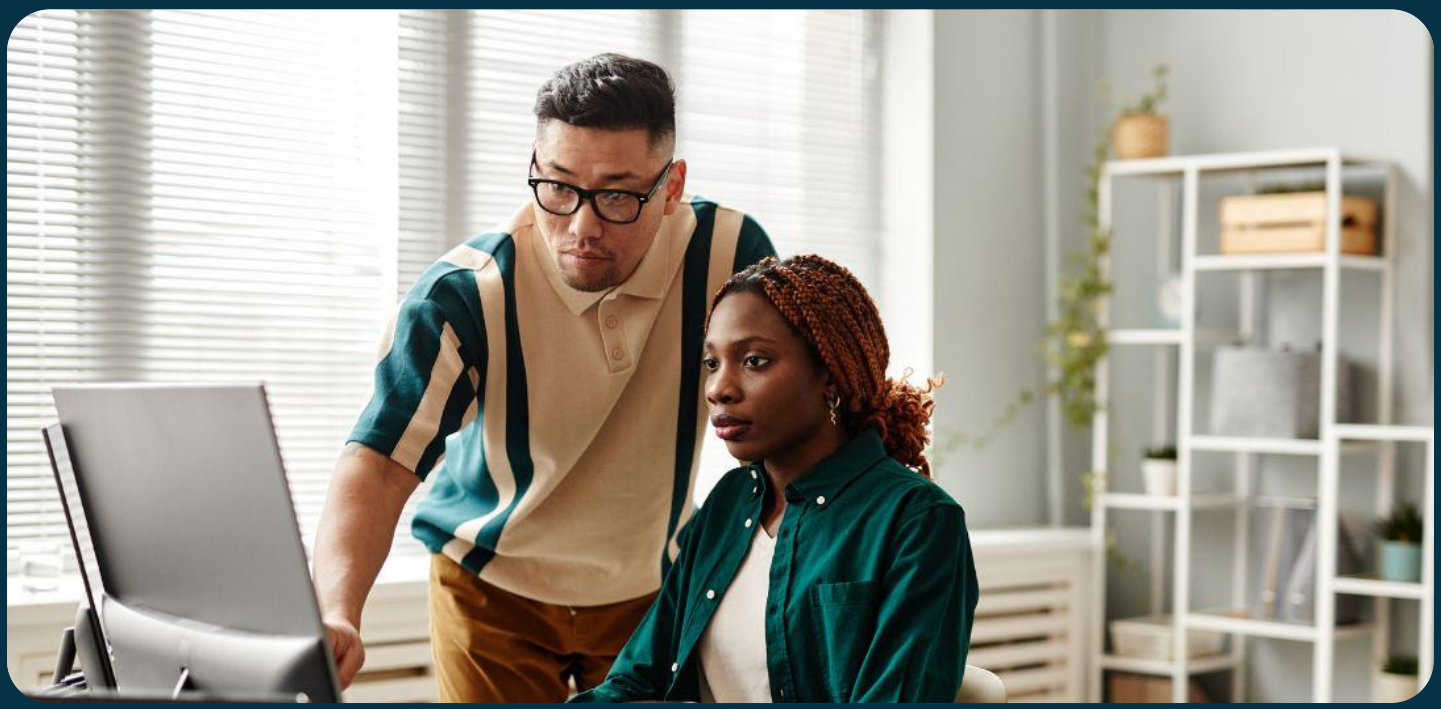
A Guide to Security with Squiz DXP SaaS



Introduction

Squiz provides a Digital Experience Platform (DXP) designed to help organizations reduce complexity while delivering excellent user experiences quickly. Our DXP encompasses multiple verticals, including content management, search and insights, data storage, and integrations, all working together to create a cohesive and powerful digital presence

Squiz DXP is built with a robust security infrastructure designed to protect your digital assets from today's - and tomorrow's - threats. This guide fully details the comprehensive security measures and practices that make Squiz DXP the most secure possible choice for your organization. As you consider adopting Squiz DXP, this guide will help you assess our proactive strategies, rigorous standards, and advanced technologies that ensure the highest level of protection and operational integrity for your digital environment.

Why the Squiz DXP Roadmap Keeps You Covered

As a technology provider of an "as a Service" platform that empowers you to integrate systems, build web presences, search, and customize your user experiences, Squiz applies security across two main focus areas: our Business and our Technology stack.

We implement a risk-based approach according to ISO/IEC 31000, continuously reviewing our risk posture with a focus on confidentiality, integrity, availability, and privacy. Monthly risk-focused meetings and annual formal risk assessments keep our view clear.

The Squiz DXP employs a multi-faceted security approach to safeguard your digital ecosystem. By leveraging global partnerships, advanced threat detection, and automatic threat mitigation, we ensure continuous protection and operational integrity.

Our roadmap includes stringent security measures, such as built-in data sovereignty practices and automatic application of security patches. These measures, combined with our adherence to industry standards and compliance regulations, provide a robust foundation for your digital experiences. We also apply the same level of due diligence to our supply chain, ensuring all components are secure to a high standard, respecting data privacy and sovereignty to the level we do internally.

This extends to any third party vendors who provide AI models, cloud hosting, and supporting services.

Pre-built and pre-checked components available in our Marketplace streamline development while ensuring high security. These components are constantly maintained, reducing the burden on your development team and minimizing potential vulnerabilities.

We utilize a comprehensive suite of tools for both our internal processes and those available to you, including static and dynamic code analysis, dependency management, and penetration testing. This layered approach ensures that both the platform and your applications remain highly secure.

In summary, the Squiz DXP roadmap is meticulously crafted to keep you covered, offering a secure, resilient, and high-performing platform.

Let’s now look at those coverage areas in detail.

Security Governance

Squiz uses ISO/IEC 27001:2022 certified ISMS for security governance, integrating DevSecOps methodologies across all processes. Security controls are implemented and monitored continuously to mitigate risks.

Data Sovereignty and Privacy

Data Sovereignty: Data stored within customer-chosen regions.

Data Privacy: Compliant with GDPR, Australian Privacy Act, New Zealand Privacy Act, and US privacy legislation.

Resilience

Business Continuity: Remote workforce ensures continuous operations.

Technology Continuity: AWS infrastructure with multiple availability zones, regular backups, and disaster recovery plans.

Highly Available

AWS Hosting: Multiple availability zones ensure resilience.

Cloudflare Integration: Content Delivery Network (CDN) and DDoS protection.

Logging and Monitoring

SIEM: Comprehensive event analysis and monitoring using AWS tools like CloudTrail, GuardDuty, and Inspector.

APM: Continuous performance analysis and alerts.

Cryptography

Encryption: TLS 1.2+ for data in transit, AWS KMS for data at rest, FIPS-validated methods, and full disk encryption for devices.

Physical and Environmental Security

AWS Hosting: Secured and audited data centers with ISO 27001, SOC 2, IRAP, and FEDRAMP certifications.

Technology Platform

Vendor Due Diligence: Annual review of vendor security.

In-House Technologies: Security integrated from the idea phase using AWS and Cloudflare capabilities.

Additional Services: Squiz Connect on GCP, encrypted data at rest and in transit using TLS 1.2 or higher.

Compute Security

Instance Isolation: Separate customer instances using EC2 and Containers.

Dynamic Scaling: Automatically scale compute capacity for optimal performance.

Incident Response

ISIRT: Formal incident management process following NIST SP 800-61, with roles like Incident Commander, Incident Point, Communications, Scribe, SMEs, and Security Incident Lead.

Storage and Database Security

Logical Separation: Multi-tenant data stores.

Encryption at Rest: AWS EFS, EBS, and S3 with access controls and encryption.

Networking Security

Environment Separation: Separate AWS accounts for production and other environments.

Network Access Control: Security groups for precise access control.

Edge Security: Application traffic secured with Cloudflare AppSec and AWS GuardDuty for intrusion detection.

Shared Security Responsibility

CDN: Enhance performance and availability with Cloudflare.

DDoS Protection: AWS and Cloudflare protection.

WAF: Squiz-managed or customer-managed Web Application Firewalls.

Your Security Responsibilities

Customer Data: Own and manage data, comply with legal requirements.

Application Security: Secure custom code and integrations using Squiz's pre-built components.

Identity and Access Management: Use integrated roles and permissions, manage access via IdP using SAML.

Vulnerability Scanning and Penetration Testing: Configure scans and tests, collaborate with Squiz.

Squiz's Security Responsibilities

Network Access: Use AWS native networking and Cloudflare edge security.

Identity and Access Management: Centralized IdP with MFA, role-based access, and auditing.

Vulnerability Management: Continuous vulnerability and patch management.

The Squiz Security Health Check Service

On top of that robust roadmap, Squiz offers a comprehensive Security Health Check Service aimed at identifying and addressing potential security vulnerabilities in your digital infrastructure.

It provides a detailed assessment of your platform's security posture, and includes both automated scans and manual checks to ensure a thorough evaluation of your system's security. The service is designed to help organizations identify security risks, understand their impact, and implement necessary measures to mitigate these risks.

Key Components

- Automated scan of your front-end solutions using OWASP Zap to identify security threats.
- The scan includes a 22-point Zap Base Scan which checks for common vulnerabilities and provides a raw report for interpretation and remediation.
- In addition to the Zap Reports, Squiz performs manual checks on commonly seen security practices that may represent security threats. This comprehensive check includes:
  - 14 manual checks for security issues.
  - An interpretation report with recommendations for remediation steps.
  - A walk-through of the report with you.
  - An estimate for the remediation work required.

Conclusion

Between them, the Squiz DXP SaaS security framework and Health Check Service offer comprehensive protection and continuous improvement, keeping your digital experience platform secure, resilient, and compliant. By prioritizing security at every level, Squiz helps CIOs safeguard their organization's digital assets, maintain customer trust, and drive business success.

With a robust roadmap, meticulous governance, proactive vulnerability management, and a Health Check service that gives you detailed insights into how to keep yourself fortified, Squiz DXP is an exceptionally strong choice for organizations looking to streamline their digital experiences without compromising on security.

By choosing Squiz, you are not only investing in a versatile and powerful digital experience platform. You're choosing a trusted business partner committed to the highest standards of security and reliability.

Squiz is a global Digital Experience Platform (DXP) company serving organizations globally in the government, higher education, financial services, insurance services, utilities and other service-driven sectors. Designed for complex organizations, Squiz helps lean teams build digital experiences fast. With our composable, Gartner-ranked DXP there is no vendor lock-in, you unify existing tech and embrace change with confidence.

Get in touch

Book a call with our experts or send us an inquiry.

Gartner
Magic Quadrant for Digital Experience Platforms 2024

GIGAOM RADAR REPORT
DIGITAL EXPERIENCE PLATFORMS (DXPs)
LEADER 2023

High Performer
Americas
FALL 2023

OMDIA UNIVERSE
LEADER
Digital Experience Management
2022