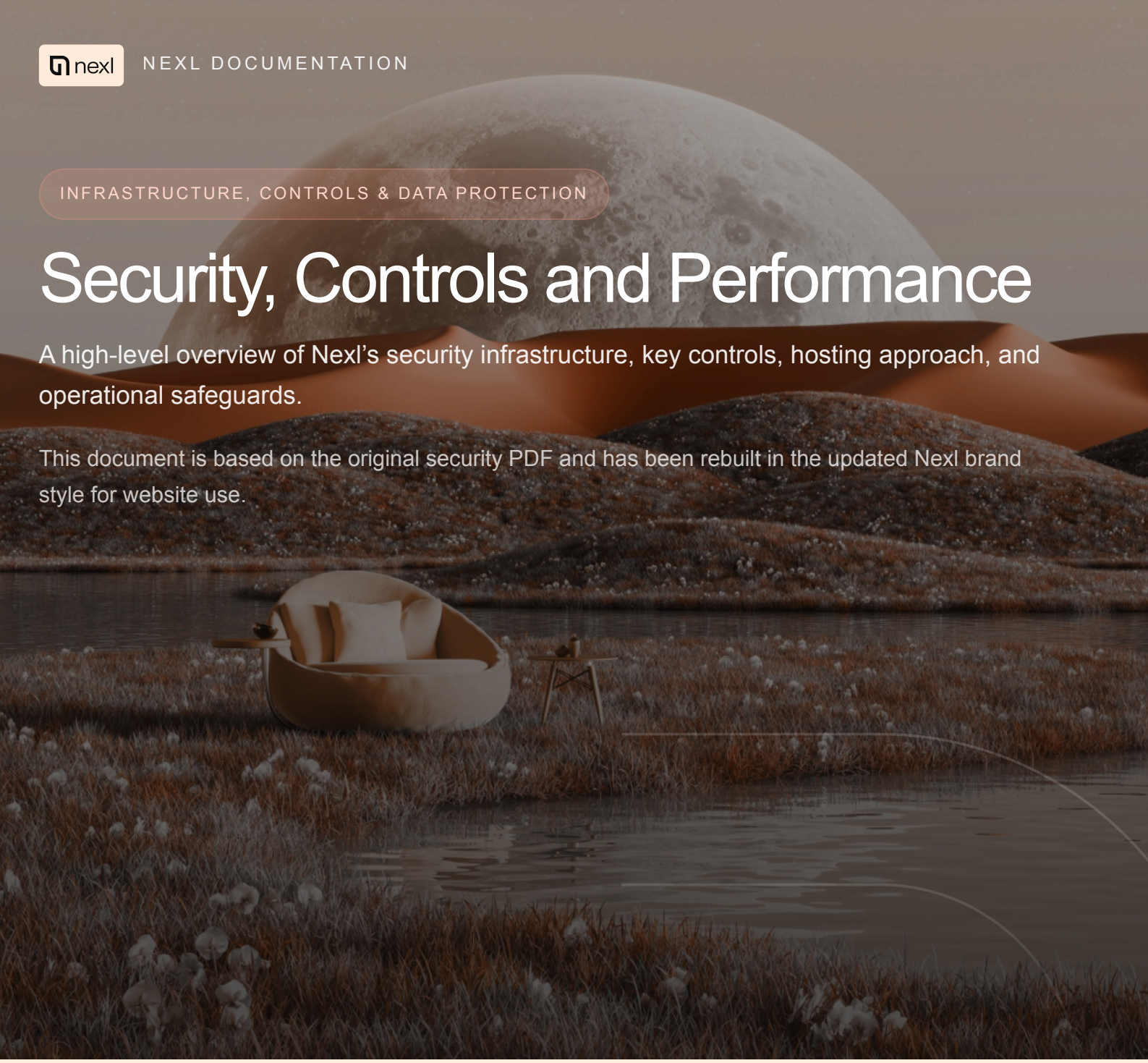
INFRASTRUCTURE, CONTROLS & DATA PROTECTION

Security, Controls and Performance

A high-level overview of Nexl’s security infrastructure, key controls, hosting approach, and operational safeguards.

This document is based on the original security PDF and has been rebuilt in the updated Nexl brand style for website use.



OVERVIEW

A concise view of Nexl’s security posture

The original Security, Controls and Performance document positions Nexl as a cloud platform hosted on audited and accredited infrastructure, with controls designed to protect customer data and support operational reliability.

What this document is for

Use it as a high-level reference when clients, IT teams, or internal stakeholders need a concise summary of how Nexl approaches infrastructure security, data handling, and operational controls.

How the source document frames security

The emphasis is on audited infrastructure, tenant separation, encryption, operational monitoring, and practical safeguards such as backup retention and downtime notices.

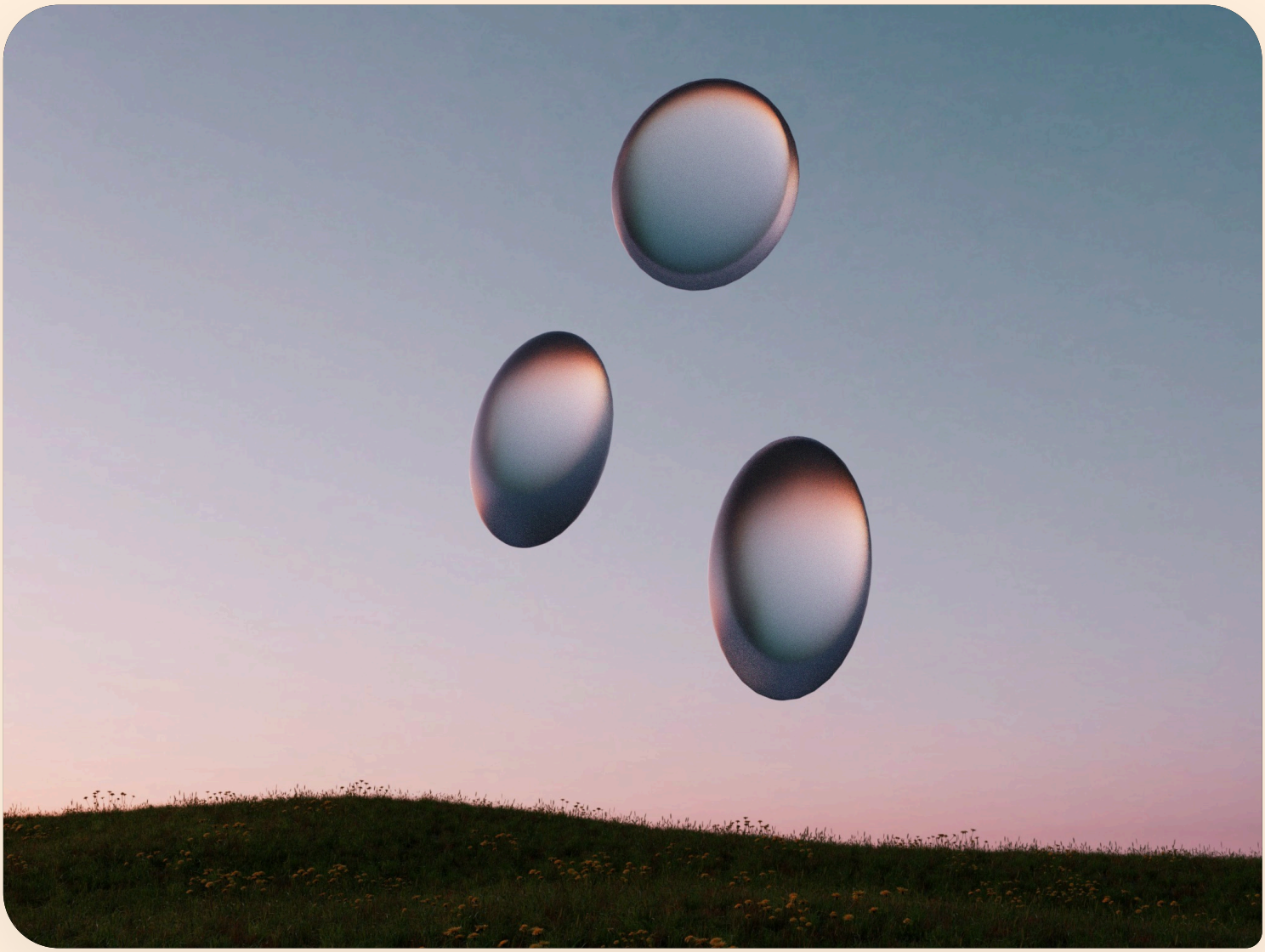
Certifications referenced

The original document references SOC 2, ISO 27001, GDPR compliance, and SSL encryption as part of the broader security posture.

SECURITY INFRASTRUCTURE

How the platform environment is protected

Nexl’s infrastructure security model combines hosted cloud environments, perimeter protection, operational monitoring, and customer data safeguards.



Application protection

- Web Application Firewall (WAF)
- Distributed Denial of Service (DDoS) protections
- Regular penetration testing

- Vulnerability scanning

Infrastructure and operations

- Hosted on leading cloud providers including AWS and Azure
- Network and perimeter protection
- Regional server options
- 24/7 monitoring and incident response
- Security education and awareness training

Customer data protection

The source document highlights logical tenant separation, optional private cloud support, encryption in transit, and encryption at rest.

Regional hosting

Nexl references regional server options including EU, US, and Australia, with Canada also noted in the underlying storage details.

SECURITY CONTROLS

Core controls referenced in the source document

The document lists the controls Nexl uses to support authentication, encryption, monitoring, resilience, and access protection.

Access and authentication

- Two-Factor Authentication (2FA)
- SAML authentication
- Account lockdown in suspected compromise scenarios

Encryption and resilience

- AES-256 encryption at rest
- TLS and HTTPS for data in transit
- Daily encrypted database backups
- Intrusion Detection Systems (IDS)

Auditability

Security-based log retention is maintained for 365 days, supporting auditing, investigation, and compliance-related visibility.

INFORMATION SECURITY DETAILS

Operational and hosting details

The original document includes a compact table of operational details covering storage, locations, backups, accessibility, downtime communications, and linked policy documentation.

Category	Details from the source document
Main data storage	AWS (EU, Australia), Azure (US), and Digital Ocean (Canada)
Available server locations	EU, Australia, USA, Canada
Encryption	Database and file encryption enabled in transit and at rest; all traffic through HTTPS only
Security monitoring	24/7 security monitoring and threat detection through Cloudflare and Rollbar
Email notification delivery	SendGrid
Data backups	Daily backups retained for 7 days and weekly backups retained for 4 weeks
Data accessibility	Data can be accessed 30 days after termination with possible extension up to 90 days; Nexl can provide an extract on request
Planned downtime	Customers are informed at least 2 weeks before planned downtime

Category	Details from the source document
Privacy Policy	Referenced in the source document as part of the security details set
Data Processing Agreement	Referenced in the source document as part of the security details set

Useful summary

For most readers, the key operational takeaways are regional hosting, encrypted transport and storage, regular backups, and clear post-termination access windows.

DATA OWNERSHIP

Ownership and tenant separation

The source document closes with an explicit note on data ownership and separation, reinforcing that customer data remains customer-owned and is not shared across tenants.

Customer ownership

Your contacts and data are fully owned by you. The document explicitly positions Nexl’s enrichment process as a one-way flow where customers receive data, but the enrichment service does not access user data in return.

Tenant isolation

Each Nexl tenant is stored separately with strict data guards in place, helping ensure that data is not shared across customer environments.

Why this matters

This is one of the most important trust points in the source document: the platform is framed not just as secure in transit and storage, but also as clearly separated across customer environments.

Source document: Security, Controls and Performance. Rebuilt as branded HTML for website use from the original uploaded PDF. Keep this HTML file and the assets folder together when publishing.