Plurilock
CRITICAL SERVICES

Multi-Cloud Hardening

Secure Foundations. Azure & AWS.

Multi-Cloud Hardening

82% of cloud misconfigurations are caused by human error—not software flaws.

Cloud environments grow faster than security controls. Over time, inconsistent configurations, excess privileges, and unmonitored changes quietly increase risk. What started as a secure deployment gradually drifts into a collection of vulnerabilities waiting to be exploited.

Plurilock's Multi-Cloud Hardening service establishes a secure, CIS-aligned baseline across your Azure and AWS environments. We harden identity, network, and data layers using proven cloud security benchmarks and best practices, then operationalize those controls so security stays enforced as your cloud evolves.

This isn't a point-in-time cleanup. It's the creation of a durable, repeatable security foundation that supports scale, compliance, and future cloud growth.

The Challenge

Most cloud environments inherit their initial security posture from whoever provisioned them first—often without comprehensive security review. As teams add workloads, adjust permissions, and respond to urgent requests, configurations drift away from secure baselines. IAM roles accumulate unnecessary privileges. Network segmentation weakens. Encryption policies become inconsistent. Logging gaps appear.

None of it happens intentionally, but all of it creates risk. By the time security teams notice, the environment is difficult to audit, hard to fix, and full of exposures that attackers can exploit.

What This Service Does

We establish a hardened, CIS-aligned baseline across your Azure and AWS environments. Our approach addresses identity, network, and data security using industry-recognized benchmarks—then operationalizes those controls through automation, continuous monitoring, and clear playbooks your teams can maintain.

The result: reduced attack surface, eliminated configuration drift, and security that scales with your cloud adoption.

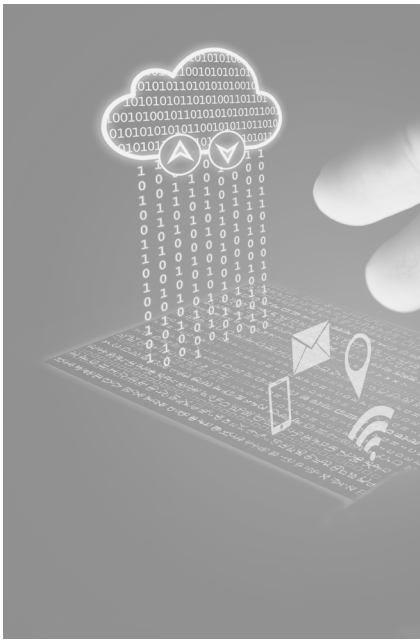
What We Harden

- **Identity** Strong authentication and least-privilege access. Role clarity and privileged access controls. Consistent enforcement across cloud platforms.
- **Network** Secure segmentation and boundary protections. Logging and visibility into network activity. Guardrails that prevent unsafe configurations.
- **Data** Encryption and secure storage policies. Controlled access to sensitive workloads. Protection against accidental exposure.

How We're Different

- **CIS-Aligned Baselines** We use proven, industry-recognized security benchmarks—not custom frameworks that require ongoing interpretation
- **Operational Focus** Hardening includes automation, monitoring, and playbooks so controls stay enforced as environments change
- **Built to Scale** Security baselines apply consistently across existing workloads and future migrations, eliminating rework
- **Durable Foundations** This isn't a point-in-time assessment—it's a repeatable security foundation that supports ongoing cloud growth

Our hardening approach reduces cloud attack surface, eliminates configuration drift, aligns environments with industry-approved security baselines, and makes security repeatable for future workloads and migrations.



Contact Us

+1 (888) 776-9234 (Plurilock)
+1 (310) 530-8260 (USA)
+1 (613) 526-4945 (Canada)

Advanced cybersecurity and Zero Trust
Security assessments and consulting
IT products and solutions
Professional services
Managed services

Business Outcomes

- **Reduced Risk** Hardened configurations eliminate common cloud vulnerabilities and reduce the attack surface across Azure and AWS.
- **Audit Confidence** CIS-aligned security baselines simplify compliance demonstrations and reduce audit friction.
- **Operational Clarity** Clear playbooks and automated enforcement mean teams know what's secure, what requires approval, and what gets flagged.
- **Scalable Security** Baseline configurations apply to new workloads automatically, ensuring security scales with cloud adoption.
- **Fewer Incidents** Proactive hardening prevents the exposures, misconfigurations, and drift that lead to security incidents.

In plain terms: fewer surprises, fewer exposures, fewer late-night incidents.

What You Walk Away With

- **Hardened, CIS-Aligned Cloud Baseline** Secure configurations across Azure and AWS that meet industry-recognized security standards
- **Automated Enforcement & Continuous Monitoring** Tools and policies that prevent drift and alert on deviations from secure baselines
- **Clear Operational Playbooks** Documentation and procedures your teams use to maintain hardened configurations ongoing
- **Executive-Ready Visibility** Dashboards and reporting that show cloud security posture clearly to leadership
- **Repeatable Security Model** Baseline configurations that apply to future workloads and migrations without rework

Built once. Enforced continuously.

How This Helps the Business

Security teams regain control over cloud configurations. Engineering teams keep moving without constant security blockers. Leadership gets clear visibility into cloud security posture.

Plurilock's Multi-Cloud Hardening service establishes a trusted security baseline across Azure and AWS, simplifies compliance and audit readiness, enables safer cloud adoption and modernization, provides clear visibility into cloud security posture, and reduces operational risk without slowing delivery.

Who This Is For

- Cloud security and infrastructure teams managing Azure and AWS environments
- Organizations preparing for compliance audits or security assessments
- Teams struggling with configuration drift and inconsistent security controls
- Enterprises scaling cloud adoption and needing repeatable security baselines
- Security leaders seeking to reduce cloud attack surface systematically

Contact us today to harden your multi-cloud environment.

sales@plurilock.com

Contact Us

+1 (888) 776-9234 (Plurilock)
+1 (310) 530-8260 (USA)
+1 (613) 526-4945 (Canada)

Advanced cybersecurity and Zero Trust
Security assessments and consulting
IT products and solutions
Professional services
Managed services

Plurilock Services

Zero Trust

Design and implementation of zero trust architectures (ZTAs)

Data Protection

Protection of intellectual property and digital assets

Identity and Access Management

Design, implementation, and integration of complete identity and access management (IAM)

Public Key Infrastructure

Design and implementation of modern public key infrastructure (PKI) deployments

Offensive Security

Security assessments and tests with a hacker mindset

Penetration Testing as a Service (PTaaS)

Managed service providing continuous penetration testing to rapidly surface emerging vulnerabilities

Data Protection as a Service (DPaaS)

Managed data protection service to operate DLP and insider threat capabilities as a service

Emergency Support

Immediate, cross functional team for urgent and high impact IT and cyber problems

Selection of current and past customers that can be publicly represented

Plurilock CRITICAL SERVICES