iTmethods · Forge

FORGE HARDENING SHEET

Managed GitHub Enterprise on Forge. The hardening sheet.

Twelve named controls. Inside your trust boundary. Hardened, governed, Reign-ready.

SECTION 2

Why this matters.

Source code is the largest single attack surface in a regulated enterprise. It contains every secret, every architecture decision, every business logic rule, and every coding-assistant prompt the bank has ever issued. The 2024-2026 wave of source-code-platform incidents made one principle plain. The trust boundary matters more than the feature set. Source code that lives outside the customer's authorization boundary is exposed by the vendor's posture, not the customer's. Forge runs GitHub Enterprise Server or GitHub Enterprise Cloud inside the customer's authorization boundary. Reign governs every AI coding tool that touches the code. Continuous assurance of every read and every write.

SECTION 3

What Forge applies on day one. Twelve named controls.

01 **SAML or OIDC identity boundary, bound to customer IdP.**

No vendor-side IdP path. Enforcement of MFA at the identity provider. Group-based access propagated from the IdP into GitHub Enterprise via SCIM.

02 **IP allow-list at the platform edge and the runner edge.**

Two-layer IP restriction. GitHub-side allow-list at the org level. Forge-edge IP allow-list at the network boundary. Both layers enforced independently.

03 **GitHub Actions runners isolated per environment.**

Short-lived OIDC tokens scoped to the workload. No long-lived secrets in the runner. Self-hosted runner topology configured for environment isolation. Runner labels enforced per repo and per branch.

04 **Advanced Security (GHAS) enabled by default.**

Code scanning, secret scanning, dependency review. Custom CodeQL queries supported. Secret scanning push protection on for every protected branch.

05 **Branch protection rules enforced via policy-as-code, not manual configuration.**

Required reviewers, required status checks, signed commits, linear history, no force push. Policy-as-code stored in a separate governance repository. Drift detection against policy.

06 **Audit log streamed to the customer's SIEM and to Reign's Audit Ledger (CAVR).**

Every push, pull request, merge, secret access, settings change, integration install. Tamper-evident replication into CAVR. Twelve-month retention default, configurable.

01 **Copilot, Cursor, Claude Code, Cortex governed through the Reign AI Gateway.**

Every coding-agent call routed through the call-layer policy decision point before the LLM sees the code. Identity-bound. Content-classified.

02 **Approved-model registry for any LLM the coding agents call.**

Versioned. PCCP-aligned change records. Drift detection. Out-of-policy model invocations blocked at the gateway.

03 **Repository data-classification labels propagated to Reign for policy enforcement.**

Customer-defined classification taxonomy (e.g., MNPI, regulated-data, internal, public) propagated from repository metadata to the AI Gateway policy decisions.

04 **Egress controls. Private Link / Private Endpoint to AWS, Azure, GCP services.**

No public-internet egress from the GitHub Enterprise deployment by default. Service-by-service allow-list enforced.

05 **Backup and DR posture documented and audit-grade.**

Snapshot cadence, cross-region replication, RPO and RTO defined and tested. DR test artifacts retained as evidence.

06 **Quarterly hardening review by the FDE pod.**

Continuous-remediation SLA on findings. P0 within seven days, P1 within twenty-one days, P2 within sixty days.

SECTION 4

Where each control maps.

CONTROL	SR 26-2	OSFI E-23	EU AI Act	DORA	FINOS AIGF	ISO 42001	SOC 2	FedRAMP
01 Identity boundary	✓	✓	✓	✓	✓	✓	✓	✓
02 IP allow-list	✓	✓		✓		✓	✓	✓
03 Runner isolation	✓	✓		✓	✓	✓	✓	✓
04 GHAS	✓	✓	✓	✓	✓	✓	✓	
05 Branch protection	✓	✓	✓	✓	✓	✓	✓	✓
06 Audit log to SIEM+CAVR	✓	✓	✓	✓	✓	✓	✓	✓
07 Reign AI Gateway	✓	✓	✓	✓	✓	✓	✓	
08 Approved-model registry	✓		✓		✓	✓		
09 Data classification	✓	✓	✓	✓	✓	✓	✓	✓
10 Egress controls	✓	✓		✓	✓	✓	✓	✓
11 Backup / DR	✓	✓		✓		✓	✓	✓
12 Quarterly FDE review	✓	✓	✓	✓			✓	✓

SECTION 5

Deployment options.

Three deployment topologies. Pick based on regulatory posture.

GitHub Enterprise Server in Customer Cloud.

Your AWS, Azure, or GCP account. Your VPC. Forge operates the cluster. Twelve to sixteen weeks to GA depending on existing tooling. Most common for US D-SIB and EU systemic banks.

GitHub Enterprise Cloud, hardened.

Forge-managed identity, network, audit-trail wiring. Reign on the AI-tool layer. For organizations that prefer the GHEC product surface but require operator-grade hardening.

GitHub Enterprise Server in air-gapped sovereign deployment.

Defense, classified, sovereign-national programs. FIPS 140-2 Level 3. ITAR, NIST 800-171, CMMC alignment.

SECTION 6

The AI coding tool layer.

Copilot, Cursor, Claude Code, Cortex, and any future coding-agent that the customer's engineering org sanctions. Every coding-agent call routed through the Reign AI Gateway. Identity-bound. Content-classified. Policy-enforced before the LLM sees the code. Tamper-evident audit trail of every coding-agent decision in the Reign Audit Ledger (CAVR). Approved-model registry mapped to the customer's AI governance posture.

SECTION 7

What we run, what you run.

Path B shared-responsibility model.

FORGE AUTOMATED	CUSTOMER AUTHORED	FDE INTERVENTION
Identity boundary, network policy, audit log streaming, AI Gateway policy decision point, CAVR ledger.	Repository structure, branch protection policy-as-code, classification taxonomy, approved-model registry contents.	Initial hardening, examination snapshots, P0/P1/P2 remediation, quarterly hardening reviews, regulator-facing posture support.

SECTION 8

Reign tier alignment.

Most regulated GitHub on Forge customers are planning to utilize **Reign Assurance** or **Reign Continuous** for AI Governance requirements. The coding-agent governance is delivered by Reign at the call layer. The hardening and operations are delivered by Forge. Same FDE pod runs both.

SECTION 9

Operator credentials and next step.

SOC 2 Type II. AWS Advanced Tier Services Partner. Validated AWS MSP. Twenty-one years operating critical infrastructure for regulated enterprises.

NEXT STEP

Talk to Forge engineering.

itmethods.com/contact?topic=forge →