MilesGuard

SCHWEIZER CYBERSECURITY

SOUVERÄNE PLATTFORM · LINUX + KUBERNETES

Holen Sie die Kontrolle zurück. Ihre Plattform. Quelloffen. In der Schweiz.

Ein gehärtetes Fundament ersetzt Dutzende Cloud-Abos: Dateien, E-Mail, Chat, Video, ERP und KI auf Infrastruktur, die Ihnen gehört, fully managed durch MilesGuard. **Digitales Büro, Security Operations Center (SOC), Air-Gap-Betrieb und geprobte Restores in einem Produkt.**

ERSETZT SAAS-ABOS WIE

Microsoft 365 · Google Workspace · Slack · Teams · Zoom · Dropbox · Jira · Zendesk · Calendly · TeamViewer · 1Password · ChatGPT

HEUTE		DIESE PLATTFORM
US-Hyperscaler · CLOUD Act · fremdes Recht	→	Schweizer Recht oder Ihr Haus · air-gap-fähig
SaaS-Abos · jedes Jahr teurer	→	keine Lizenzen, keine Telemetrie · typisch 30 bis 50 Prozent günstiger · SOC inklusive
Lock-in · Exit teuer und riskant	→	alles als Code in Ihrem Git · übernehmbar auch ohne MilesGuard

BASIS TALOS LINUX + KUBERNETES · GITOPS FLUX CD · ZERO TRUST MTLS
HOSTING FREI WÄHLBAR: CLOUD, VPS ODER ON-PREM · BETRIEB FULLY MANAGED · CO-MANAGED · KAUF · CLOUD-EXIT

40+	**100%**	**<15min**	**2×**
ANWENDUNGEN, MODULAR AKTIVIERBAR	OPEN SOURCE, KEINE BLACKBOX	AUTOMATISCHE SELBSTHEILUNG	UNABHÄNGIGE BACKUP-WEGE, GEPROBT

APPS

Ein Login. Ihr komplettes digitales Büro.

Über 40 Anwendungen hinter einem zentralen Single Sign-on. Sie schalten frei, was Sie brauchen; eigene Anwendungen laufen als Standard-Container mit. Dazu die Werkzeuge des SOC (Seite 4).

Dateien & Office

6 APPS

- **Nextcloud**: Dateien, Kalender, Kontakte
- **Collabora**: Office-Suite im Browser
- **Excalidraw**: Whiteboard
- **Stirling-PDF**: PDF-Werkzeugkasten
- **Syncthing + Obsidian LiveSync**: Datei- und Notizen-Sync

ersetzt OneDrive · Dropbox · MS Office · Miro

Kommunikation

7 APPS

- **Element / Matrix**: Chat, föderierbar, mit Video (Element Call)
- **Jitsi**: Videokonferenzen
- **Stalwart**: eigener Mailserver (SMTP/IMAP/JMAP)
- **Mastodon**: eigener Server im Fediverse

ersetzt Slack · Teams · Zoom · Exchange

Business

8 APPS

- **ERPNext**: ERP: Auftrag, Lager, Buchhaltung
- **Plane**: Projektmanagement
- **Cal.com**: Terminbuchung
- **Zammad**: Helpdesk & Ticketing
- **Snipe-IT**: IT-Inventar
- **CISO Assistant**: Governance, Risk & Compliance
- **Windmill + Temporal**: Workflows & Automatisierung

ersetzt Jira · Calendly · Zendesk · Zapier

Lokale KI, ohne Datenabfluss

4 APPS

- **Ollama + Open WebUI**: LLM-Chat auf eigener Hardware; Prompts und Dokumente verlassen das Haus nicht
- **LibreTranslate**: Übersetzung
- **Whisper**: Transkription (Speech-to-Text)

ersetzt ChatGPT-Abos · DeepL

Zugriff & Netzwerk

5 APPS

- **NetBird**: WireGuard-VPN-Mesh
- **Guacamole**: RDP/SSH/VNC im Browser
- **RustDesk**: Fernwartung
- **Vaultwarden**: Passwortmanager für Teams
- **ALTCHA**: datenschutzfreundliches Captcha

ersetzt Tailscale · TeamViewer · 1Password

Betrieb, Medien & Gebäude

9 APPS

- **Homer / Glance**: Portal & Dashboard
- **Gatus**: Statusseite
- **Coder**: Cloud-Entwicklungsumgebungen
- **Headlamp**: Kubernetes-UI
- **changedetection**: Web-Monitoring
- **Jellyfin**: Medien
- **Home Assistant**: Gebäudeautomation
- **Frigate**: Kameras/NVR mit Objekterkennung

ersetzt Codespaces · Statuspage

EIN LOGIN

Keycloak Single Sign-on (OIDC) mit Hardware-MFA (FIDO2/WebAuthn) vor jeder Anwendung. Keine einzige Route ist ohne Anmeldung erreichbar. Gruppenbasierte Berechtigungen gelten zentral, vom Dateiordner bis zur Admin-Konsole.

INFRASTRUKTUR

Die Infrastruktur im Detail.

EBENE	KOMPONENTE	AUFGABE
OS	Talos Linux	unveränderlich, API-only, LUKS2
GitOps	Flux CD	deklarativer Soll-Zustand aus Git
Netzwerk	Cilium	eBPF, kube-proxyless, WireGuard
Ingress	Traefik + Gateway API	TLS 1.3, HSTS, ForwardAuth
Identität	Keycloak + SPIRE	SSO (OIDC/FIDO2) + Workload-mTLS
Secrets	OpenBao + SOPS/age	Secrets-Engine + Git-Verschlüsselung
Storage	Longhorn	replizierter Blockspeicher (2 Replikate)
Datenbank	CloudNativePG	PostgreSQL-Operator, Streaming-Backup
Backup	Velero + restic/Kopia	Ziele: SeaweedFS + Garage (S3, Object-Lock)
Monitoring	VictoriaMetrics/Logs	Metriken, Logs, Alarme (+ Vector)
Autoscaling	KEDA + KRR	lastabhängig, Scale-to-zero, Sizing
Registry / Git	Zot + Forgejo	Air-Gap-Quelle für Images + Code + CI
Policy	Kyverno	30+ Admission-Policies, PSS restricted
Runtime-Security	Tetragon · Suricata	eBPF-Enforcement · IDS (+ CrowdSec IPS)
SIEM / XDR	Wazuh	XDR, Log-Korrelation
DFIR	Velociraptor + DFIR-IRIS	Forensik, IR-Fälle
SOAR / TI	Shuffle + MISP	Playbooks, Threat Intel
Schwachstellen	Greenbone · Trivy	Netz-, Image-, SBOM-Scans

ARCHITEKTUR: SCHICHTEN		EVICTION-SCHUTZ
T0	**Fundament**	GitOps-Engine, Storage, Datenbank, Workload-Identität; weicht zuletzt.
T1	**Plattform**	Netzwerk, Ingress, Zertifikate, Monitoring, SSO, Secrets, Backup, Security-Stack.
T2	**Apps**	40+ Anwendungen, einzeln aktivier- und pausierbar; weichen unter Last zuerst.

Referenz-Sizing

- ✓ **Ab 4 Nodes produktiv:** 3× Control-Plane à 8 GiB (etcd-Quorum) + 1 Worker à 16 GiB, wächst durch weitere Worker.
- ✓ **Provider-unabhängig:** läuft auf jedem VPS-Anbieter oder Bare-Metal; Provider-Wechsel ist dokumentierter Standardfall.
- ✓ **Bootstrap:** von leeren Nodes zum laufenden Cluster mit einem Befehl (just install).
- ✓ **Storage-Kontrakt:** jeder Datensatz hat Klasse, Backup-Weg und dokumentierte Verlust-Auswirkung; Quelldaten immer repliziert.

HÄRTUNG · TLS ≥1.3 · HSTS · PKCE S256 · LUKS2 · WireGuard · mTLS required · PSS restricted · seccomp · readOnly-FS · non-root · SBOM CycloneDX · Cosign · CIS-Scans (kube-bench) · CVE-Scans (Trivy)

SICHERHEIT & BETRIEB

Verteidigung in sechs Schichten. Betrieb, gemessen.

Wir greifen unsere eigenen Cluster regelmässig an und dokumentieren die Grenzen.

S1	**Unveränderliches Betriebssystem**	Talos Linux · kein SSH, keine Shell · Verwaltung nur über signierte API · LUKS2-verschlüsselt
S2	**Netzwerk: default-deny**	jede Verbindung explizit erlaubt, pro Dienst (Cilium) · intern WireGuard · am Edge TLS 1.3 + HSTS
S3	**Identität statt IP-Adressen**	kryptografische Identität pro Dienst (SPIFFE/SPIRE) · mTLS erzwungen
S4	**Zulassungskontrolle**	30+ Regeln (Kyverno) · nur signierte Images · kein Root · strengster Pod-Standard
S5	**Laufzeit-Überwachung**	Kernel-Sensoren (Tetragon) · IDS (Suricata) · IPS (CrowdSec) · Honeypots mit Canary-Secrets
S6	**Erkennung & Reaktion**	vollständiges SOC eingebaut · Erkennung, Fälle, Forensik, Threat Intel

Das eingebaute SOC

Anderswo ein eigenes, oft sechsstelliges Projekt. Hier Teil der Plattform:

- ✓ **Wazuh** — SIEM / XDR
- ✓ **DFIR-IRIS** — Incident-Response-Fälle
- ✓ **MISP** — Threat Intelligence
- ✓ **Shuffle** — SOAR-Automatisierung
- ✓ **Velociraptor** — Endpoint-Forensik
- ✓ **Greenbone + Trivy** — Schwachstellen-Scans
- ✓ **Gophish** — Phishing-Simulation
- ✓ **MITRE Caldera** — Angriffs-Emulation

BETRIEB

GitOps	Jede Änderung ist ein Commit · Vier-Augen per PR · CI-Gate vor Rollout · Rollback per Git-Revert.
Selbstheilung	Hängende Kernkomponenten reparieren sich in unter 15 Minuten, ohne Eingriff · Dead-Man-Heartbeats überwachen die Überwachung.
Backups	2 unabhängige Wege · S3 Object-Lock · Restore-Drill monatlich (Checksummen) · etcd stündlich.
Stresstest	Kein Ausfall der Kernschichten · Erholung unter 30 Sekunden · Limits dokumentiert.
Monitoring	Metriken, Logs, Alarme (VictoriaMetrics) · Statusseite (Gatus) · Health-Check in 3 Kommandos.
Updates	Wöchentlich kuratiert (Renovate) · CI-validiert · Versions-Pinning statt «latest» · CVE-Scans im Cluster.
Lieferkette	SBOM (CycloneDX, Dependency-Track) · nur signierte Images (Cosign) · Air-Gap-Spiegel Forgejo + Zot.

COMPLIANCE · CIS Benchmark (kube-bench) · NIST SP 800-190 · nDSG · NIS2 · ISG · GRC-Tool inklusive

Reden wir über Ihre Plattform.

Kostenloses Erstgespräch. Fully managed (auf Wunsch Managed Security und externer CISO), co-managed: Sie betreiben die Apps, wir Infrastruktur und Updates. Oder Kauf und schrittweise Migration.

MilesGuard GmbH
Bruggwiesenweg 18 · 9000 St. Gallen
info@milesguard.ch
+41 71 552 21 01 · milesguard.ch