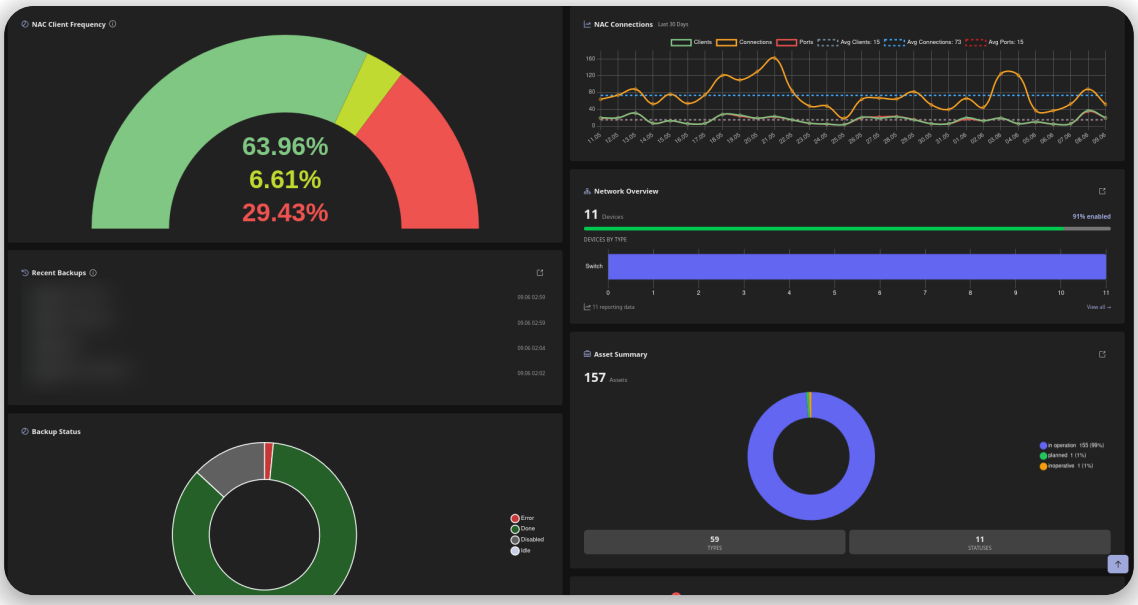
Central Operations Dashboard

Ihre gesamte IT-Infrastruktur. Eine Plattform.

Dokumentation, CMDB, Passwort-Manager, NAC, Firewall, Monitoring — **fünf Werkzeuge, fünf Wahrheiten, ein blinder Fleck.** Genau dort, zwischen dem was *läuft* und dem was *dokumentiert* ist, entstehen Sicherheitslücken, doppelte Arbeit und Audit-Stress. **COD macht damit Schluss.** Eine mandantenfähige Plattform führt Ihre komplette Infrastruktur herstellerübergreifend an *einem* Ort zusammen — live, durchsuchbar, auditierbar und vollständig on-premise betreibbar.

COD auf einen Blick: mandantenfähig • modular • rollenbasiert (LDAP/AD) • on-premise oder Cloud • ISO 27001, 9001, 22301 & BSI 200-3 • Multi-Vendor-Firewall & VPN • NAC mit eigener PKI • aktives Monitoring • Angular 21 / Prisma — KRITIS-tauglich.



Ein Dashboard für alles: NAC-Client-Status, Netzwerk-, Backup- und Asset-Übersicht auf einen Blick.

Alle Module. Eine Oberfläche.

Kein Tool-Wildwuchs mehr: COD bündelt jede Disziplin des IT-Betriebs in *einer* konsistenten Plattform auf einem gemeinsamen, **lebenden** Datenbestand.

Netzwerk & Assets · **NAC & PKI** · **Firewall & VPN** · **GRC**

Monitoring · **Schwachstellen** · **Backup** · **Hypervisor**

OTP / 2FA | **Captive-Portal** | **Automatisierung** | **codPass**

Das Herzstück: eine Plattform, die zusammenwächst

Multi-Mandanten & Rollen

Mehrere Kunden, Standorte oder Abteilungen in einer Plattform. Feingranulare Rollen- und Gruppenverwaltung mit Anbindung an LDAP/Active Directory — oder lokale Benutzer.

Zentrale Suche — First-Level-Support in Sekunden

Meldet ein Anwender ein Problem, sieht der Support sofort: Wo steht das Gerät? An welchem Switch und Port hängt es? Wie ist der Monitoring-Status? Wer ist zuständig? — gesucht über MAC, IP, Standort oder Name.

Zentrales Assetmanagement

Die automatisch gepflegte Grundlage für alle weiteren Module — statt händischer Listen mit Stand von gestern.

Die Module im Detail

Netzwerk & Asset-Management

Findet automatisch jedes IP-adressierbare Gerät — von IT bis OT. Layer-2-/Layer-3-Topologie, Live-Polling-Status je Gerät (SNMP/SSH/API) und eine globale Suche über die gesamte Infrastruktur.

NAC & eigene PKI

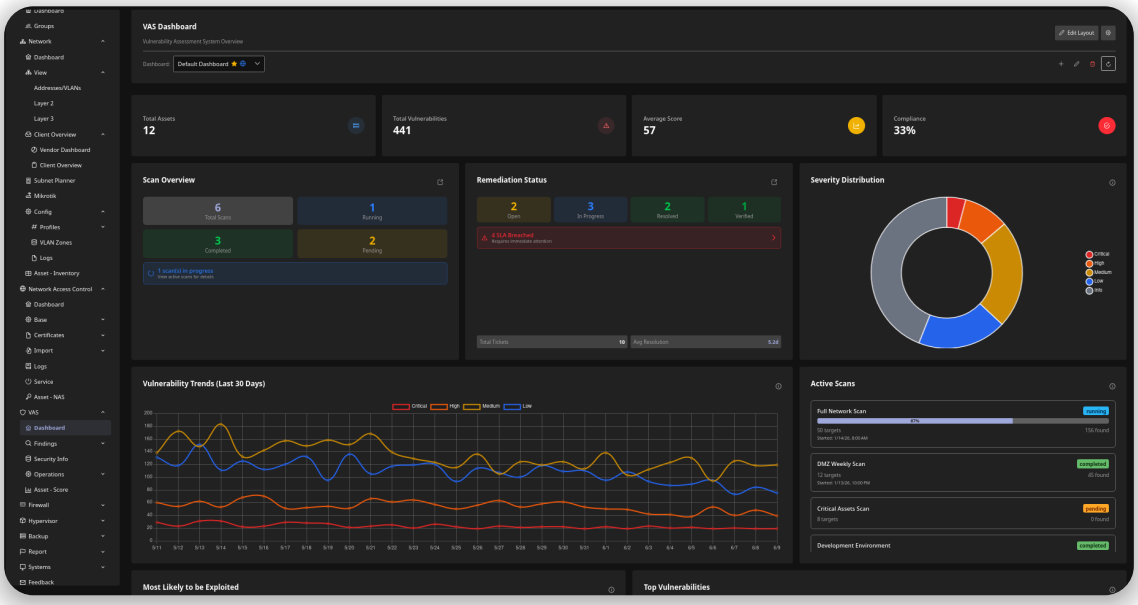
802.1x- und MAC-Authentifizierung steuern Sie direkt im Browser — performant bis in den Millionenbereich. Inklusive eigener Certificate Authority (RSA/ECDSA/EdDSA), Client-Zertifikaten, CRLs und PKCS#12-Export, synchron mit FreeRADIUS.

Firewall & VPN

Herstellerübergreifendes Management von **AIMdefense, OPNsense, pfSense und Dyn-Fi**: zentrale Updates, Alias- und Zonen-Verwaltung, Zertifikatsüberwachung der OpenVPNs, Erreichbarkeitsüberwachung und SSH-Terminal im Browser.

GRC — Governance, Risk & Compliance

Ein Managementsystem für mehrere Normen auf einer Datenbasis: **ISO 27001, ISO 9001, ISO 22301** und **BSI 200-3** — inkl. aller dazugehörigen Controls, asset-basierter Risikobewertung, versionierter Richtlinien (Markdown-Editor) und manipulationssicherem, append-only Audit-Log auf eigener PostgreSQL-Datenbank.



Schwachstellen-Management: Scan-Übersicht, Remediation-Status, Severity-Verteilung und Trends über Wochen.

Schwachstellen-Management (VAS)

Schwachstellen-Scans mit Remediation-Status, Severity-Verteilung und Trendanalyse über Wochen — priorisiert, was wirklich gefährlich ist, statt Listen ohne Kontext.

Monitoring — wissen, bevor der Anwender anruft

Aktives ICMP-/TCP-Probing (fping) mit konfigurierbarem Intervall je Mandant, Polling-Status (OK / Error / Unknown) je Gerät, Problem- und Severity-Übersicht sowie E-Mail-Alarme mit Throttling. Endlich sehen, wenn eine Firewall nicht erreichbar ist — sofort, nicht erst beim nächsten Ticket.

Monitoring-Dashboard: Verfügbarkeit, offene Probleme nach Schweregrad und Verlauf der letzten 24 Stunden.

Backup
Sichert Netzwerk-, Embedded- und Linux/BSD-Systeme — inklusive Konfigurationsvergleich, der jede Änderung sichtbar macht.

Hypervisor
Zentrale vSwitch Netzwerkverwaltung mit Netzwerkprofilen Ihrer VMware Umgebung.

OTP / Zwei-Faktor
Sicheres Management von Zeit- und ereignisbasierte Einmalpasswörter (TOTP/HOTP) des gesamten Teams.

Captive-Portal
Kontrollierter Gast- und Geräte-Zugang über ein anpassbares Onboarding-Portal.

Automatisierung & Wartungskalender
Wiederkehrende Aufgaben per Ansible direkt aus COD ausrollen; geplante Wartungen zentral terminieren — das Monitoring alarmiert dann nicht grundlos.

codPass — quelloffenes Secrets-Management

codPass
Quelloffenes, sicherheitsfokussiert modernisiertes Secrets-Management mit zentraler OTP-Verwaltung — heute eigenständig betreibbar; die native Integration in COD ist in Vorbereitung.

Herstellerübergreifend: Connect-Integrationen

COD spricht mit Ihren bestehenden Systemen, statt sie zu ersetzen:

Zabbix • i-doit • {php}IPAM • baramundi • RADIUS Server

Architektur & Betrieb

- **On-Premise oder Cloud** — volle Datenkontrolle, KRITIS-tauglich; Vorlagen-Updates (ISO-Controls, BSI-Katalog) lassen sich kontrolliert einspielen.
- **Moderne Architektur** — Angular 21 (zoneless, Signals), Prisma, Nx-Monorepo; sensible Felder (Passwörter, SNMP-Communitys) sind standardmäßig aus Queries ausgeschlossen.
- **Rollenmodell** — Manager » SuperAdmin » Admin, durchgängig mandantenfähig.
- **White-Label** — App-Name, Logo und Farben ohne eine Zeile Code anpassbar.

Sehen Sie COD in Aktion.
Wir zeigen die Plattform praxisnah in Ihrer Umgebung — ohne Vertriebsdruck, ohne Verpflichtung.

extoco.de • extocode GmbH