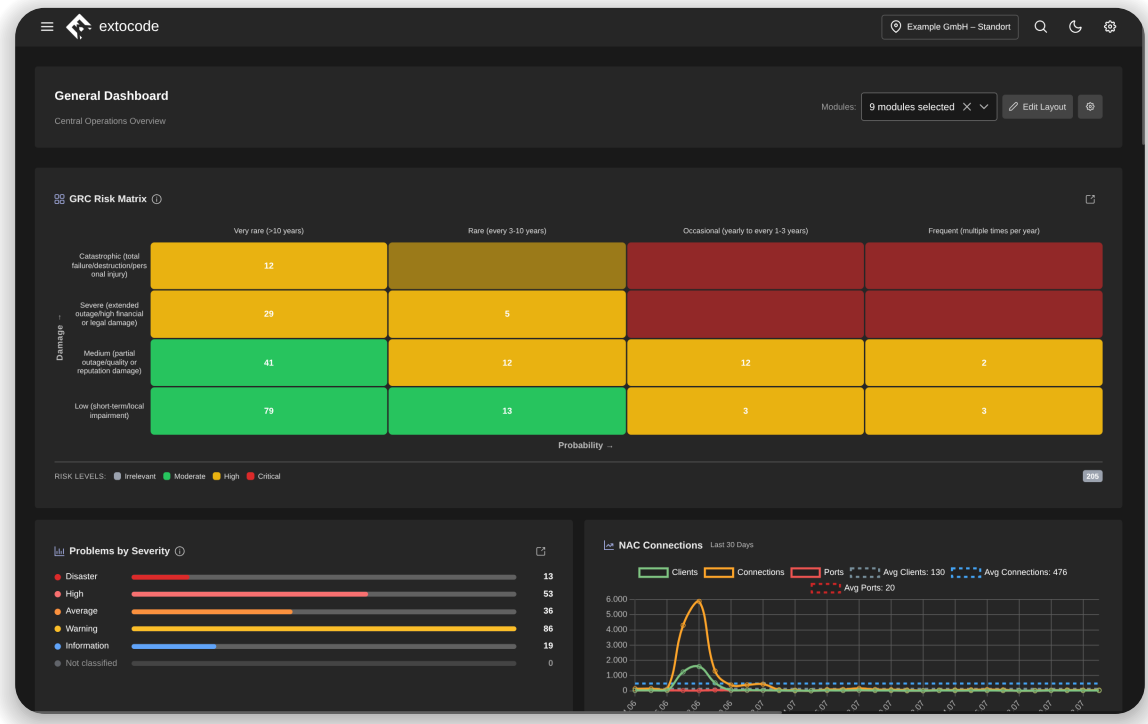
Central Operations Dashboard

Your entire IT infrastructure. One platform.

Documentation, CMDB, password manager, NAC, firewall, monitoring: **five tools, five versions of the truth, one blind spot.** Right there, between what is *running* and what is *documented*, security gaps, duplicated work, and audit stress arise. **COD puts an end to that.** One multi-tenant platform brings your complete infrastructure together in *one* place, across vendors: live, searchable, auditable, and fully operable on-premise.

COD at a glance: multi-tenant • modular • role-based (LDAP/AD) • on-premise or cloud • multi-standard GRC (ISO 27001/27002, 9001, 22301, BSI 200-3, NIS2 readiness) • multi-vendor firewall & VPN • NAC with its own PKI • TACACS+ (AAA) • Zabbix monitoring • zero-knowledge vault • Angular 21 / Prisma, KRITIS-ready.



One dashboard for everything: GRC risk matrix, open problems by severity, and NAC activity at a glance.

All modules. One interface.

No more tool sprawl: COD bundles every discipline of IT operations into *one* consistent platform on a shared, **living** data foundation.

Network & Assets | **NAC & PKI** | **TACACS+** | **Firewall & VPN**

Monitoring | **Vulnerabilities** | **Backup** | **Hypervisor**

GRC | **Captive Portal** | **Automation** | **OTP / 2FA**

Stronghold | **codPass** | **Integrations** | **Platform**

The heart of it: one platform that grows together

Multi-tenancy & roles

Multiple customers, sites, or departments in one platform. Fine-grained role and group management with LDAP/Active Directory integration, or local users.

Central search: first-level support in seconds

When a user reports a problem, support immediately sees: Where is the device located? Which switch and port is it connected to? What is its monitoring status? Who is responsible? The search works by MAC, IP, location, or name.

Central asset management

The automatically maintained foundation for all other modules, instead of hand-kept lists that were already outdated yesterday.

The modules in detail

Network & asset management

Automatically discovers every IP-addressable device, from IT to OT, with live polling status per device (SNMP/SSH/API). Plus an asset workspace per device, rooms/racks with rack elevation, layer-2/layer-3 routing topology, and a global search across your entire infrastructure.

NAC & your own PKI

Control 802.1x and MAC authentication directly in the browser, performant into the millions. Includes your own certificate authority (RSA/ECDSA/EdDSA), client certificates, CRLs, and PKCS#12 export, in sync with FreeRADIUS.

TACACS+: network AAA

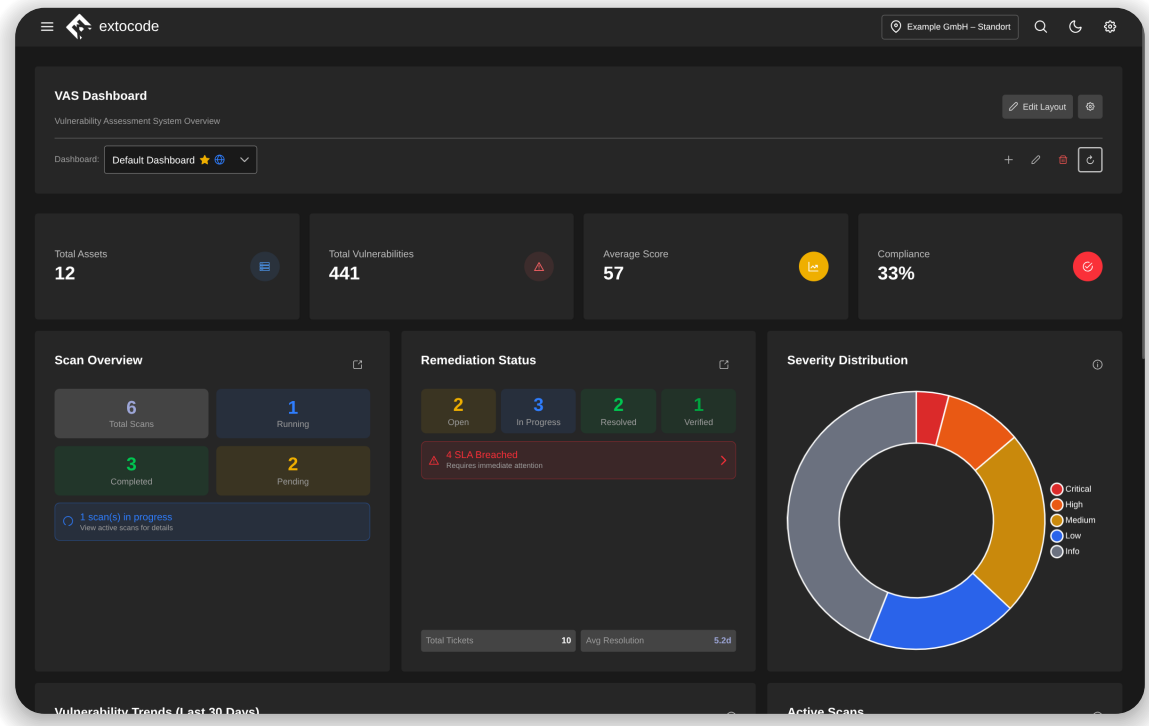
Central management of the in-house TACACS+ server per **RFC 8907**: users, NAS clients, authorization rules with roles and command sets, a role simulator for live policy evaluation, and accounting with a live log.

Firewall & VPN

Cross-vendor management of **AIMdefense, OPNsense, pfSense, and DynFi**: central updates, alias and zone management, certificate monitoring, reachability monitoring per firewall (ICMP/TCP, e-mail on outage), and an SSH terminal in the browser. VPN management for WireGuard, OpenVPN, and IPsec with connection status display.

GRC: Governance, Risk & Compliance

One GRC platform for multiple standards on a single data foundation: versioned multi-standard catalog (**ISO 27001, ISO 27002, ISO 9001, ISO 22301**, and **BSI 200-3**, plus **NIS2 readiness**), Statement of Applicability, asset-based risk assessment per BSI 200-3, cases/incidents with SLAs, document control with an approval workflow, and an append-only audit log (protected against retroactive modification and deletion by database triggers).



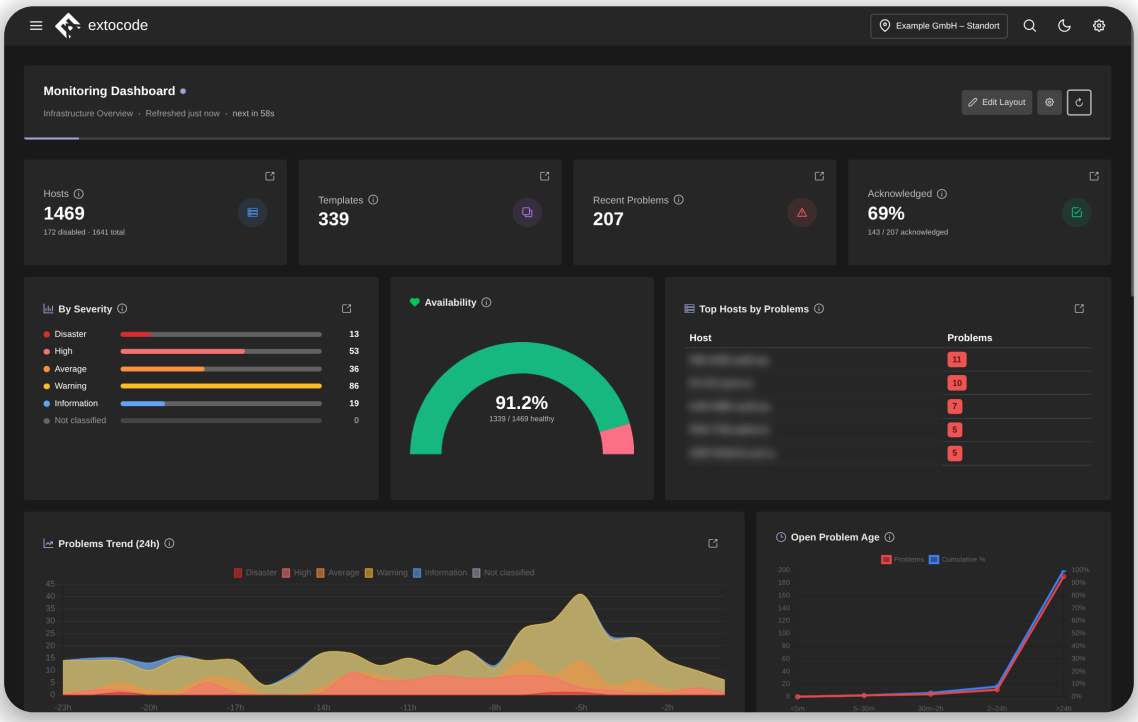
Vulnerability management (in preparation): planned scan overview with remediation status and severity distribution, shown here with sample data.

Vulnerability management (VAS)

Turns vulnerabilities from your network into a prioritized overview, with remediation status, severity distribution, and trend, so what is truly dangerous comes first, instead of lists without context. *In preparation.*

Monitoring: Zabbix integration

Integrates your (customer-owned) Zabbix server into COD: configurable dashboard, availability and problems by severity, monitoring directly on the asset. COD reads the data and acknowledges problems. Alerting itself remains with Zabbix.



Monitoring dashboard: availability, open problems by severity, and the history of the last 24 hours.

Backup

Backs up network, embedded, and Linux/BSD systems, including a configuration diff that makes every change visible.

Hypervisor

Central vSwitch network management with network profiles for your VMware environment.

OTP / two-factor

Central management of time- and event-based one-time passwords (TOTP/HOTP) for the COD login. OTP management is moving to Stronghold: existing tokens are migrated automatically, and the module keeps running as a fallback during the transition.

Captive Portal

Controlled guest and device access through a customizable onboarding portal.

Automation

Recurring mandatory tasks run automatically, for example the daily creation of actions for document reviews that are due. COD executes network actions through an internal Ansible runner engine.

Secrets management: Stronghold & codPass

Stronghold: zero-knowledge vault

New in COD 3.6 and shipped to production: an end-to-end encrypted password and secrets vault directly in COD (Argon2id / X25519 / AES-GCM): personal and shared team vaults, targeted sharing, and a browser extension for Chrome and Firefox. The integrated authenticator also handles TOTP/HOTP codes.

codPass

Standalone, open-source password and secrets manager (`github.com/extocode/codpass`): on-premise, full data sovereignty, independent of COD.

Cross-vendor: Connect integrations

COD talks to your existing systems instead of replacing them:

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

Architecture & operations

- **On-premise or cloud:** full data control, KRITIS-ready. Template updates (ISO controls, BSI catalog) can be applied in a controlled manner.
- **Modern architecture:** Angular 21 (zoneless, signals), Prisma, Nx monorepo. Sensitive fields (passwords, SNMP communities) are excluded from queries by default.
- **Role model:** Manager » SuperAdmin » Admin, multi-tenant throughout.
- **White label:** app name, logo, and colors adjustable without a single line of code.

See COD in action.
We demonstrate the platform hands-on in your environment. No sales pressure, no obligation.

extoco.de • extocode GmbH