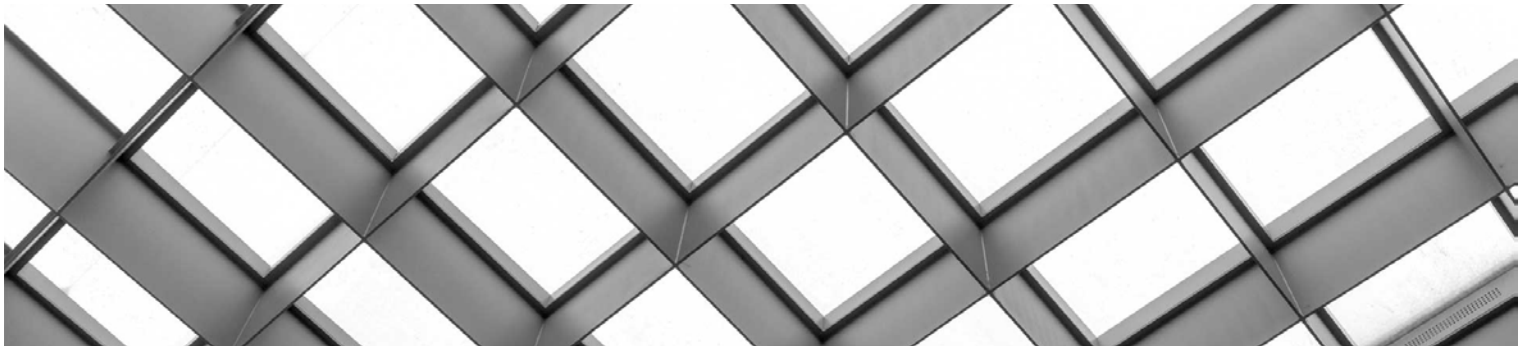
Service

Secure Connectivity

CERUNO

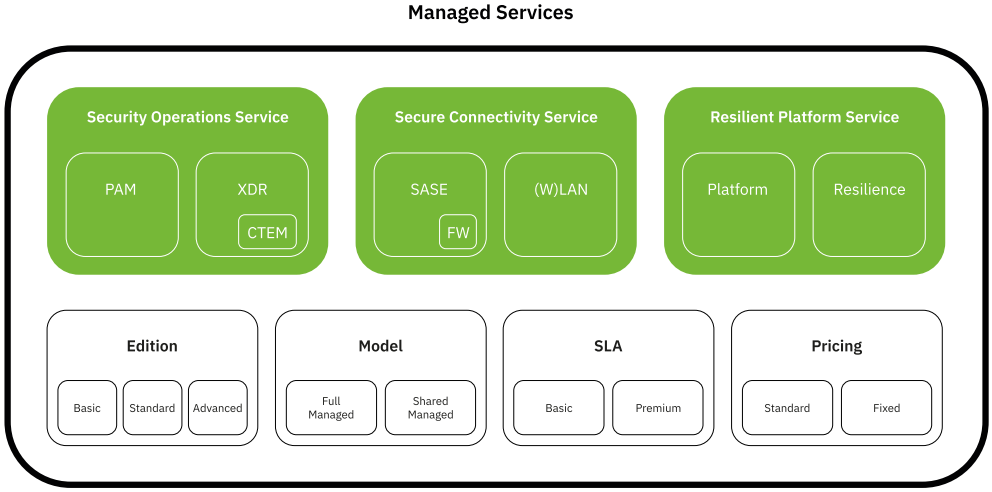


Standorte und User vernetzen. *Performant und identitätsbasiert.*

In einer zunehmend hybriden und cloudbasierten IT-Landschaft sorgen wir dafür, dass Standorte, Nutzer, Geräte und Anwendungen jederzeit **sicher miteinander verbunden** sind – unabhängig ihrer Location. Ziel ist eine **identitätsbasierte, stabile und performante Netzwerkbasis,** die IT-Teams entlastet, Sicherheitsrisiken minimiert und die digitale Arbeitsfähigkeit nachhaltig stärkt.

Unser technologischer Grundgedanke basiert auf einer konsequenten **SASE-Architektur,** die Sicherheit und Vernetzung in einer cloud-nativen Welt untrennbar miteinander verbindet. Zusätzlich bieten wir tiefgreifende **Expertise** sowohl in **Software-Defined Networking (SDN)** als auch in der Orchestrierung klassischer, hochkomplexer **Enterprise-Netzwerke.** Durch die konsequente Anwendung des **Zero Trust** Prinzips stellen wir sicher, dass Identitäten und Anwendungen unabhängig von der physischen Infrastruktur geschützt sind, während wir gleichzeitig die Stabilität und Performance bewährter Netzwerkstrukturen gewährleisten.

Mit dem **Secure Connectivity Service** bieten wir einen ganzheitlichen Service für den sicheren und zuverlässigen Betrieb moderner Unternehmensnetze. Wir übernehmen Planung, Implementierung, Betrieb und kontinuierliche Optimierung der gesamten Connectivity-Infrastruktur – transparent, skalierbar und proaktiv überwacht.



Kunden

- … erhöhen ihr Sicherheitsniveau nachhaltig, da Netzwerk- und Security-Policies einheitlich, identitätsbasiert und nach Zero-Trust-Prinzipien umgesetzt werden.
- … stellen ihre IT zukunftssicher auf, indem sie eine skalierbare Connectivity-Plattform nutzen, die Cloud-, Hybrid- und Mobile-Work-Szenarien optimal unterstützt.
- … profitieren von einer schnellen Bereitstellung neuer User, Standorte und Applikationen, da Rollouts und Änderungen automatisiert und vordefiniert erfolgen.
- … erhalten volle Kostenkontrolle und Planungssicherheit durch transparente, servicebasierte Preismodelle ohne unvorhersehbare Betriebsaufwände.

Module

Managed SASE

Unser Managed SASE Modul ermöglicht Kunden einen sicheren Zugriff auf Applikationen. Unabhängig vom Standort der User. Unabhängig vom Standort der Daten. Hierbei setzen wir auf Zero Trust Network Access (ZTNA) statt klassischem VPN. Zusätzlich werden ein Secure Web Gateway (SWG), Firewall as a Service (FWaaS) und ein Cloud Access Security Broker (CASB) bereitgestellt. Die Policies sind Identity- und kontextbasiert und werden zentral verwaltet, sodass Kunden konsistente Sicherheitsregeln für alle Nutzer und Standorte erhalten.

- ZTNA (Zero Trust Network Access) statt klassischem VPN
- Secure Web Gateway (SWG)
- Firewall as a Service (FWaaS)
- Cloud Access Security Broker (CASB)
- Kontext- & Identity-basierte Policies
- Zentrales Policy- und Log-Management

Module

Managed Firewall

Unser Managed Firewall Modul sorgt für den sicheren Betrieb von Next-Generation Firewalls. Wir übernehmen Design, Konfiguration und regelmässige Überprüfung der Firewall-Policies sowie Firmware- und Security-Updates. Darüber hinaus kümmern wir uns um Monitoring, Incident-Management und Change-Management. Optional kann die Firewall nahtlos in die SASE-Umgebung integriert werden, um konsistente Sicherheitsrichtlinien über alle Zugänge hinweg sicherzustellen.

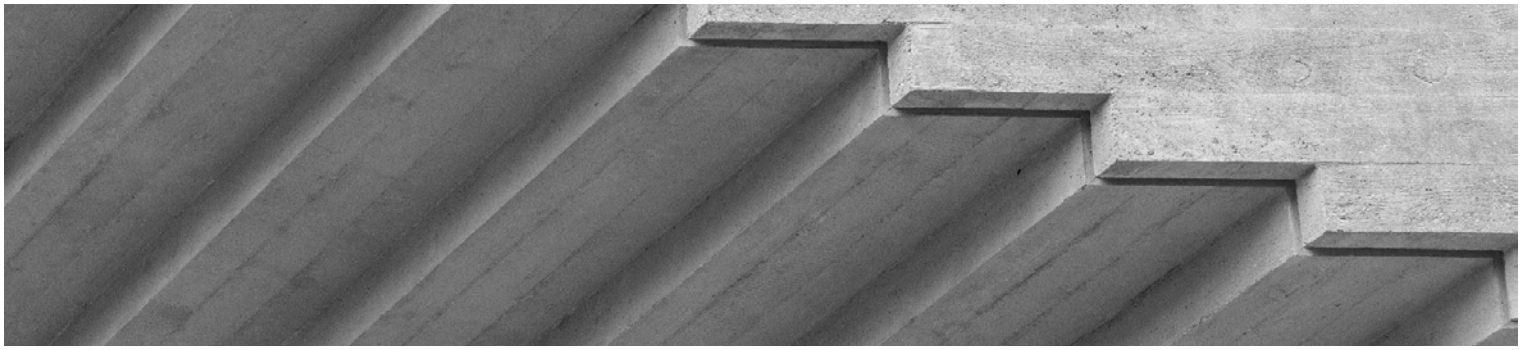
- Design und Standardisierung der Firewall-Policies
- Regelmässige Policy-Reviews
- Firmware- und Security-Updates

Module

Managed LAN & WLAN

Unser Managed LAN & WLAN Modul stellt sicher, dass LAN- und WLAN-Infrastrukturen sicher, leistungsfähig und zentral gemanagt werden. Dabei werden Zugriffe rollen- und identitätsbasiert gesteuert. Die Netzwerke werden segmentiert, z. B. für Clients, Gäste, IoT oder OT. Neue Standorte können dank Zero-Touch-Provisioning schnell in Betrieb genommen werden, während proaktives Monitoring und Performance-Optimierung die Verfügbarkeit und Stabilität sicherstellen.

- Cloud-managed LAN- und WLAN-Infrastruktur
- Identity- und rollenbasierte Netzwerkzugriffe (Network Access Control - NAC)
- Netzwerksegmentierung (User, Gast, IoT, OT)
- Zero-Touch-Provisioning für neue Standorte und neue Geräte
- Proaktives Monitoring und Performance Optimierung

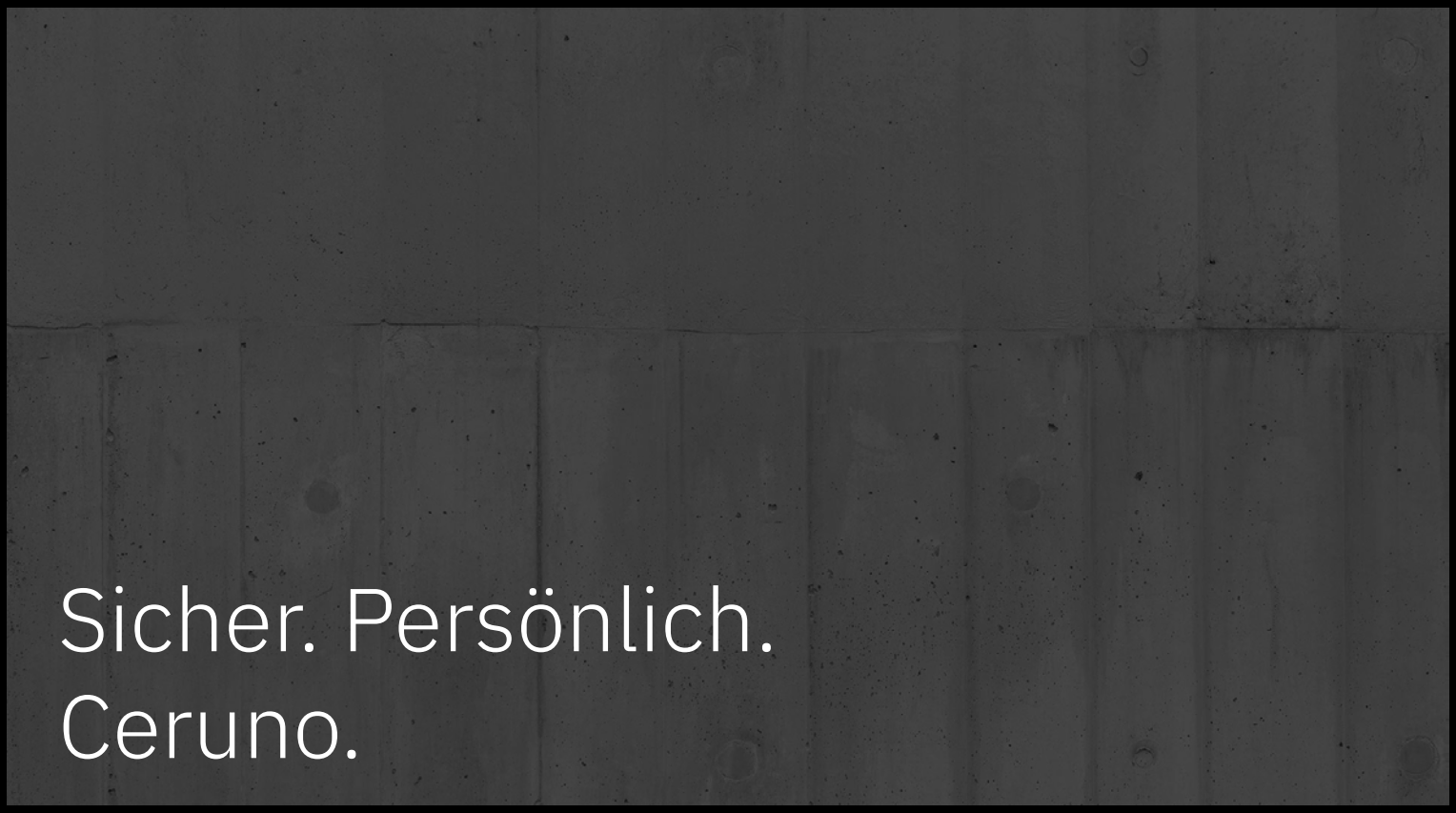


Betriebsmodelle

Wir bieten ein zentrales Monitoring rund um die Uhr (optional), standardisierte Incident-, Change- und Problem-Management-Prozesse, klar definierte SLAs und Eskalationswege sowie regelmässige Service- und Security-Reports.

Shared Managed Model
Beim Shared Managed Model übernimmt der Kunde bestimmte Aufgaben selbst, während wir zentrale Management- und Security-Funktionen bereitstellen. Typische Aufgaben des Kunden können die lokale Konfiguration von Switchports oder einzelnen Firewall Rules sein. Unser Team stellt sicher, dass Richtlinien, Monitoring, Updates und zentrale Security-Policies konsequent umgesetzt werden.

Full Managed Model
Im Full Managed Model übernehmen wir den vollständigen Betrieb der Secure Connectivity Umgebung. Das beinhaltet die Verwaltung von SASE, Firewall, LAN und WLAN, Policy-Management, Monitoring, Incident- und Change-Management sowie die kontinuierliche Optimierung der Performance und Security. Der Kunde muss sich um keine operativen Aufgaben kümmern und erhält regelmässig Reports sowie Transparenz über die gesamte Infrastruktur.



Sicher. Persönlich.
Ceruno.

Hauptsitz
Ceruno AG
Rosenbergstrasse 93
9000 St. Gallen

Chur
Hartbertstrasse 10
7000 Chur

Triesen
Landstrasse 123
9495 Triesen

+41 58 733 01 01
info@ceruno.ch
ceruno.ch

CERUNO