Connecting your world. paloalto NETWORKS

Sovereign Cortex with T Security

Cyberabwehr für das KI-Zeitalter

Der Modernisierungsdruck ist real

Die sich stetig weiterentwickelnde Bedrohungslage erfordert KI-gestützte Sicherheit, schnellere Reaktionsfähigkeit und höhere Resilienz. Gleichzeitig steigen die regulatorischen Anforderungen. Sicherheitsverantwortliche tragen die Verantwortung für beides.

KI- und Cloud-Beschleunigung

Die KI- und Cloud-Einführung schreitet rasant voran – getrieben durch Wettbewerbs- und Kostendruck.

Steigende Governance-Anforderungen

Aufsichtsbehörden und Vorstände stellen zunehmend anspruchsvollere Fragen zu Zugriff, Kontrolle und Datensouveränität.

Fragmentierter Betrieb

Sicherheit ist über mehrere Clouds, Tools und Teams verteilt. Das erschwert die eindeutige Zuordnung von Verantwortlichkeiten.

Modernisierung oder Kontrolle. Ein vermeintlicher Zielkonflikt.

In vielen Unternehmen gilt: Modernisierung geht auf Kosten der Kontrolle. Datensouveränität oder leistungsfähige Cyberabwehr?

Diese Wahrnehmung bremst den Fortschritt auf beiden Seiten.

Modernisierung erfordert KI, Cloud und leistungsfähige Technologien.

Souveränität erfordert Kontrolle, Governance und Verantwortlichkeit.

Cyberabwehr modernisieren – ohne Kontrollverlust.

Datensouveränität ist operativ, nicht geografisch

Es geht längst nicht mehr nur darum, wo Daten gespeichert werden.

Entscheidend sind operative Kontrolle, Governance und Verantwortlichkeit in der Praxis.

- Wer hat Zugriff – und unter welcher Jurisdiktion?
- Wie werden Betriebsprozesse gesteuert und durchgesetzt?
- Hält dies vor Audits und regulatorischer Prüfung stand?

Zielkonflikte sind real, aber beherrschbar.

Datensouveränität
Durchgesetzt durch operative Kontrolle über:

- Verschlüsselung
- Zugriff
- Datenresidenz

Sovereign Cortex with T Security: Das operative Fundament

01. Gemeinsame Ebene

Souveränität in der Praxis

Steuerbare und verantwortliche KI-Sicherheitsoperationen

- KI-gestützte Sicherheit – nachvollziehbar und kontrollierbar
- Einheitlicher Betrieb über alle Umgebungen hinweg
- Definierte Governance- und Eskalationsmodelle

02. KI-gestützte Cyberabwehr

paloalto NETWORKS

Leistungsstarke Cyberabwehr

KI-gestützte Erkennung, Analyse und Reaktion über Cloud, Netzwerk und Endpunkte hinweg.

- **1,4 Mrd** analysierte Bedrohungen pro Tag
- **70.000+** Kunden weltweit
- **Anerkannt** von Gartner und Forrester

03. Souveräne Governance

Connecting your world.

Operativ durchsetzbare Datensouveränität

- Operativer Zugriff, ausschließlich innerhalb der EU
- Verschlüsselungsmanagement unter Kontrolle der Deutschen Telekom
- Audit-Logging und Transparenz
- Datenverarbeitung am Standort Frankfurt
- 24x7 gemanagter, souveräner Betrieb

Kontrolle ohne vollen Betriebsaufwand

Datensouveränität ohne Kompromisse

Ein Betriebsmodell für datensouveräne Cyberabwehr: kontrollierte Modernisierung, klare Verantwortlichkeit und operatives Vertrauen.

- **Leistungsstarke Cyberabwehr** mit durchsetzbarer Souveränität
- **KI-Sicherheitsoperationen,** die Audit-Anforderungen standhalten
- **Nachvollziehbare** Datensouveränität
- **Ein Betriebsmodell** – einheitlich und klar verantwortet

Sovereign Cortex with T Security
Cyberabwehr für das KI-Zeitalter

> Sovereign Cortex with T Security entdecken

Connecting your world. paloalto NETWORKS