



CSPM, CWPP, CNAPP, XDR UND ZERO TRUST: WAS IST WAS UND WOFÜR?

Thorsten Willer, Principal Consultant
10. Oktober 2023



CSPM

CLOUD SECURITY POSTURE MANAGEMENT



CSPM

Automatische und kontinuierliche Prüfung auf Fehlkonfigurationen der Cloud (IaaS/PaaS)

- Detektion von und Reaktion auf Datenlecks und Konformitätsverstöße (Sicherheitsrichtlinien des Unternehmens oder sonstige Vorschriften)

Control Plane & PaaS Config

CSPM	IAM Configuration	Control Plane
	Network Configuration	
	Storage Configuration	
	PaaS Configuration	





CSPM

Automatische und kontinuierliche Prüfung auf Fehlkonfigurationen der Cloud (IaaS/PaaS)

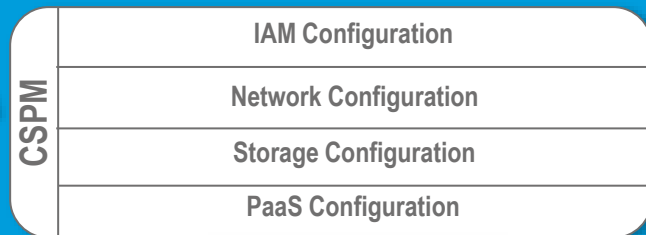
→ Detektion von und Reaktion auf Datenlecks und Konformitätsverstöße (Sicherheitsrichtlinien des Unternehmens oder sonstige Vorschriften)

CWPP

Analyse **aller** Workloads und deren Wechselwirkung untereinander:

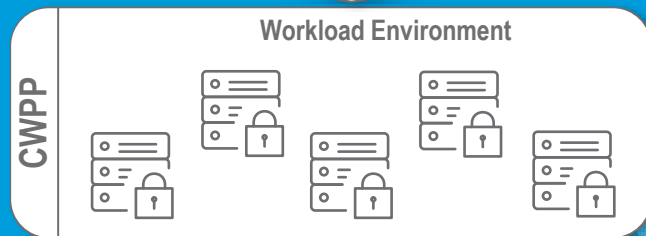
- Identifizierung und Analyse von Schwachstellen inkl. Konfiguration
- Erkennung von „Secrets“ und sensible Daten
- Bewertung der Gefährdung und des Risikos
- Sicherheitsmaßnahmen (gegen die festgestellten Probleme)
- Applikations- und Verhaltenskontrolle

Control Plane & PaaS Config



Cloud-native Security Services

Workload Protection

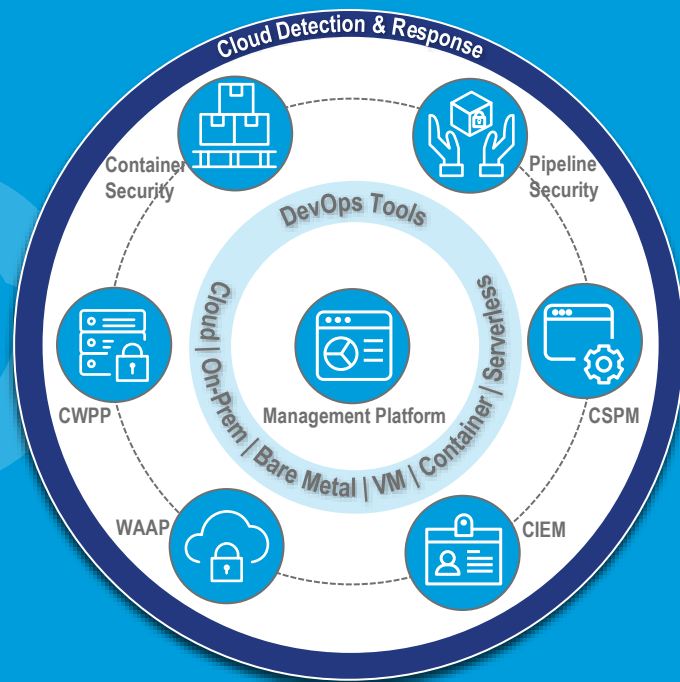




Zusammenführung von **CWPP** sowie **CSPM** und Ergänzung um weitere Komponenten:

- Kubernetes Security Posture Management (KSPM)
- Artifact Scanning
- Cloud Identity and Entitlement Management (CIEM)
- Web Application & API Protection
- Cloud Detection & Response

CNAPP ermöglicht es Entwicklern, Sicherheit in DevOps-Praktiken zu integrieren, ohne unnötigen Overhead zu verursachen.

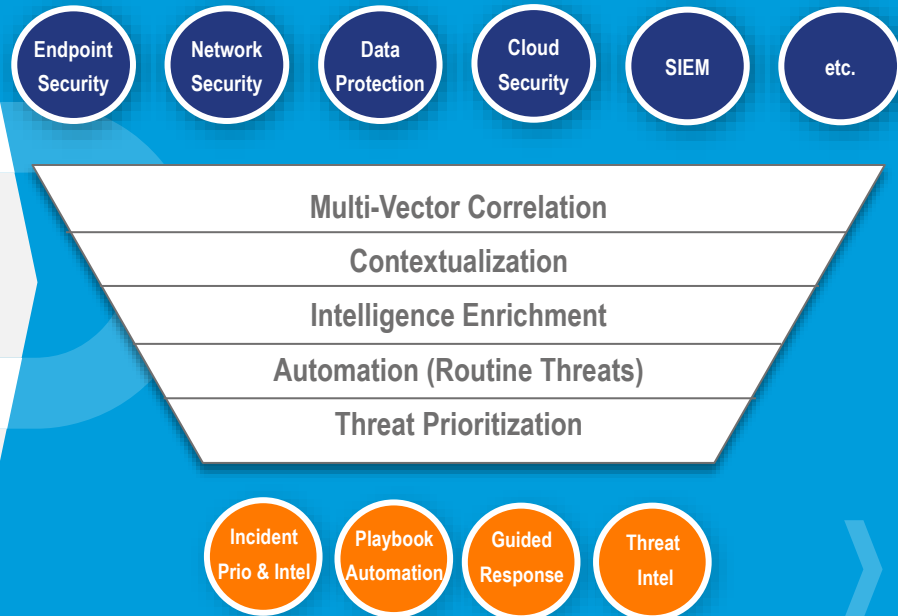




EXTENDED DETECTION AND RESPONSE

Übergreifende **Erkennung** und **Reaktion** gegen (gezielte) Angriffe:

- Multi-Vektor Analytik
- Korrelierte und kontextuale Verhaltensanalyse von Nutzern und IT-Systemen
- Bedrohungsanalyse mit externen und lokalen Bedrohungsdaten
- Automatisierung und Orchestrierung zur Optimierung von SOC-Prozessen
- Ablaufpläne (Playbooks)
- Bereitstellung relevanter Daten (für die Triage) von Vorfällen



ZERO TRUST

DEFINITION

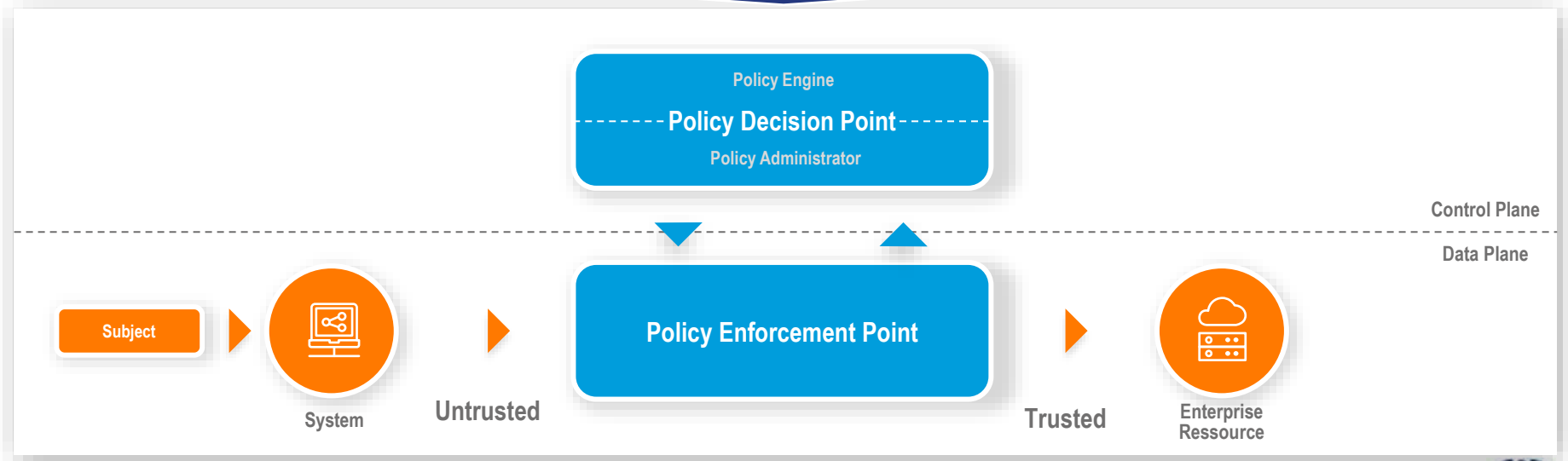
Zero Trust ist ein
CYBERSECURITY-PARADIGMA,
das sich auf den Schutz (**Prävention**) von
Ressourcen und die Prämisse konzentriert,
dass **VERTRAUEN NIEMALS IMPLIZIT**
gewährt wird, sondern
KONTINUIERLICH EVALUIERT
werden muss.

National Institute of Standards
and Technology (NIST – 08/2020)



ZERO TRUST

DAS GESAMTPRINZIP



ZERO TRUST, XDR & CNAPP

FAZIT



Zero Trust, **XDR** und **CNAPP** arbeiten auf **verschiedenen Ebenen** und verfolgen teilweise **unterschiedliche Ansätze** und **Ziele**.

Dennoch gibt es Gemeinsamkeiten:

- Kontext
- Korrelation
- Schnelle, gezielte und automatisierte Reaktion auf Vorfälle
- Hoher Grad an Automatisierung und Orchestrierung

Übergreifende
Prävention & Reaktion

ZERO TRUST

Übergreifende
Detektion & Reaktion

XDR

Prävention, Detektion & Reaktion

CNAPP

Aufwand

Resilienz



**VIELEN DANK!
LINKEDIN PROFIL:**



Let's connect!

