

AIRLOCK®

Cutting Edge Applikations- und API-Sicherheit

In Kubernetes

Besuchen Sie
uns auf der it-sa:
Halle 7A, Stand 116
10. – 12. 10. 23
Nürnberg



secunet

terreActive



CSO

COMPUTERWOCHE

10:00 Einleitung durch Thomas Kohl, Senior Business Development International

10:05 Studienvorstellung «IAM as a Service» durch Simon Hülsbömer, Senior Project Manager Research Studien-projekte in der Marktforschung von CIO, CSO und
COMPUTERWOCHE

10:20 Kein Zugriffsmanagement ohne starke Authentifizierung durch Esther Schulz,
Produkt Manager Innovation & Produkt Management Division Public Authorities

10:40 Pause

11:00 Docker exposed: Wie Hacker Kubernetes heute und morgen angreifen durch Florian Hansemann, Geschäftsführer HanseSecure und Marc Bütikofer, Head of Innovation, Airlock



11:30 Wie Sie sich in der aktuellen Bedrohungslage mit einem **SOC und Threat Detection** schützen durch Silvan Leuenberger, Head of Service Management Center

11:50 Offene Diskussionsrunde mit Brötchen

API Security ist interdisziplinär

Figure 1: API Security Consists of API Protection and API Access Control

API Security Consists of API Protection and API Access Control

	 API Protection	 API Access Control
Key Functionality	Content validation, threat detection, traffic throttling	Authentication, authorization, identity propagation
Key Technologies Used	Attack signature, reputation-based control, anomaly detection, OAS message validation	OAuth 2.0, OpenID Connect, JSON Web Tokens
Product Categories	Web application firewalls, API management, application delivery controllers	API management, access management software, IDaaS

Source: Gartner (October 2020)

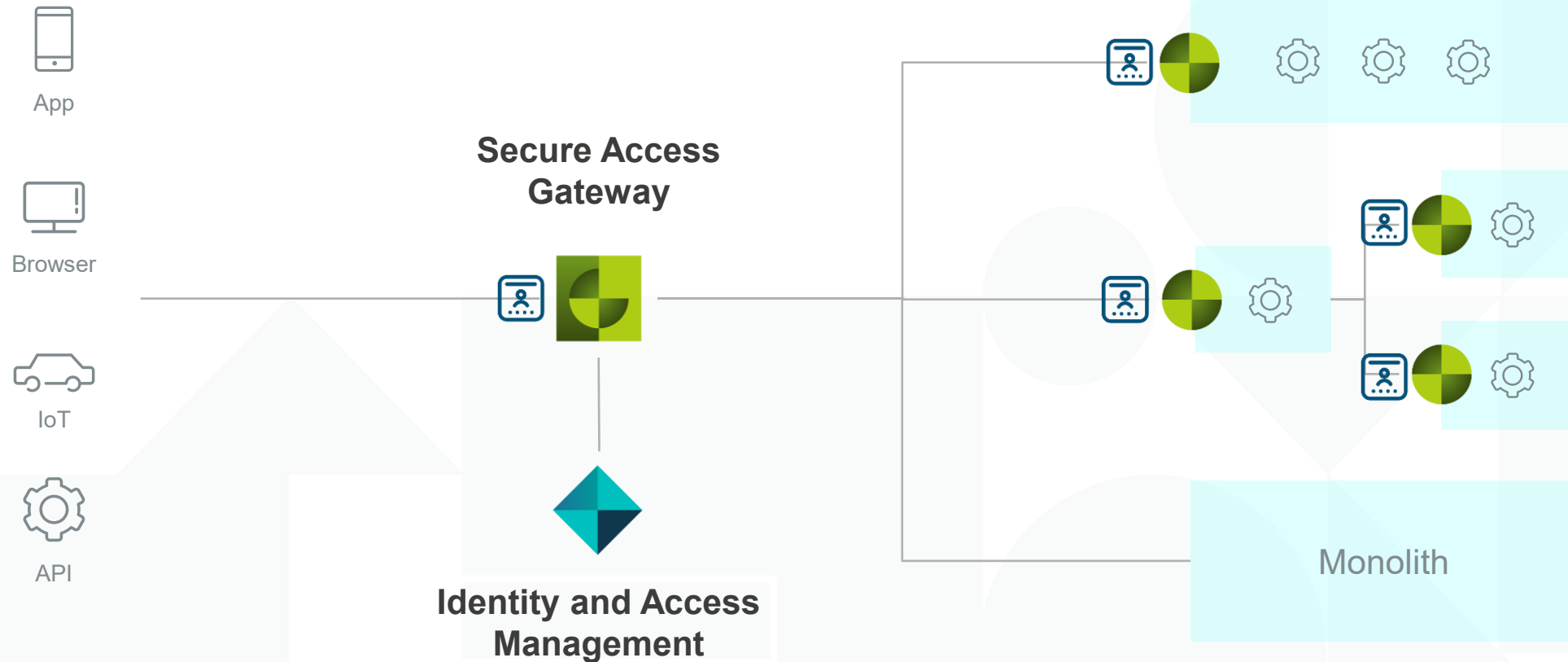
IDaaS = identity as a service; OAS = on-access scan

728915_C

Neuer Begriff: WAAP

Zero-trust architecture

Identity is the new perimeter





Thomas Kohl



ChatGPT

How would you explain
"Continuous Adaptive Trust"?

Continuous Adaptive Trust ist ein Sicherheitsansatz, der durch kontinuierliche Überwachung und **adaptive Sicherheitsmaßnahmen** das Vertrauen in die Anwendungen und Systeme eines Unternehmens aufbaut und aufrechterhält.

Der Ansatz basiert auf der Idee, dass **Vertrauen** kein statischer Zustand ist, sondern vielmehr ein **dynamischer und fortlaufender Prozess**, der **kontinuierlich überwacht** und an sich ändernde Bedingungen angepasst werden muss.