Facts zum Produkt

- Einheitliche Plattform für IT-, OT- & IoT-Sicherheit
- Zero-Trust-Ansatz & sicherer Fernzugriff
- Kontinuierliches Risiko- & Bedrohungsmanagement
- Schnelle Integration in bestehende Umgebungen
- Erhöhter Schutz & Resilienz kritischer Systeme

Partnered with:

CLAROTY

Cyber-Resilienz für IT/OT-Umgebungen

Schutz Ihrer industriellen Infrastruktur mit Claroty

Industrial Cyber Resilience ist entscheidend, um industrielle Betriebstechnologien (OT) und deren IT-Schnittstellen vor Cyberangriffen, Produktionsausfällen und Datenverlusten zu schützen. Claroty unterstützt Unternehmen dabei, ihre Sicherheit und Betriebskontinuität zu gewährleisten.

Ihre Herausforderungen:

- **Zunehmende Angriffsfläche:** Wachsende Zahl vernetzter Geräte und IoT-Komponenten.
- **Geringe Sichtbarkeit:** Komplexität und Vielfalt der Systeme erschweren das Monitoring.
- **Fachkräftemangel:** Wenige Experten für OT-Sicherheitslösungen.
- **Heterogene Sicherheitsstandards:** Fehlende Standardisierung erschwert einheitliche Sicherheitsmaßnahmen und beeinträchtigt die Cybersicherheit.
- **Regulatorische Anforderungen:** Standards wie ISO27001:2022 oder KRITIS erhöhen den Druck.

SERVICEWARE

Kontaktieren Sie uns für ein Beratungsgespräch, um einen ganzheitlichen Schutz für Ihre kritische Infrastruktur zu sichern – heute und in der Zukunft.

Mehr erfahren

Konvergenz von IT und OT – Ganzheitliche Sicherheit durch CLAROTY

Die zunehmende Vernetzung von IT- und OT-Systemen schafft nicht nur neue Möglichkeiten, sondern auch neue Risiken. Traditionell werden diese Bereiche separat betrachtet – IT mit Fokus auf Vertraulichkeit und OT auf Verfügbarkeit. Die digitale Transformation erfordert jedoch einen ganzheitlichen Ansatz. Claroty ermöglicht die Integration von OT-Sicherheit in bestehende IT-Sicherheitsstrukturen, wie etwa ein Security Operations Center.

Ihre Vorteile:

- **Erhöhte Transparenz:** Vollständige Sicht auf IT- und OT-Ressourcen durch ein konsolidiertes SOC.
- **Verbesserte Bedrohungserkennung:** Schnellere Identifizierung & Priorisierung von Risiken durch Analysetools, um Schaden zu verhindern.
- **Effiziente Ressourcennutzung:** Optimales Einbinden bestehender Tools und Mitarbeiter:innen zur Senkung der Gesamtbetriebskosten (TCO).
- **Erleichterte digitale Transformation:** Reibungslose Prozesse durch standardisiertes Sicherheitsmanagement, schnelle Anpassungen und die Einhaltung neuer Vorschriften.

Lösungsansätze und Unterscheidungsmerkmale von Claroty

Integration
Nahtlose Einbindung in IT- und OT-Sicherheitsinfrastrukturen für eine bessere Zusammenarbeit der beiden Sicherheitsteams und das Gewährleisten eines ganzheitlichen Ansatzes für Ihre Cybersicherheit.

Identifikation von Ressourcen
Umfassende Bestandsaufnahme von Assets in IT/OT-Systemen, als Grundlage für Cyber-Resilienz.

Bedrohungserkennung und Risikomanagement
Erkennung und Beseitigung nicht erkannter Schwachstellen im Netzwerk mit Zero-Day-Schutz. Schnelle Warnungen, Analysen und automatisierte Workflows für eine unmittelbare Reaktion.

Netzwerkschutz
Zero-Trust-Ansatz stärkt die Sicherheit industrieller Kontrollsysteme (ICS) durch Zugriffskontrollen und Überwachung. Nur autorisierte Geräte erhalten Zugriff.

Compliance & Reporting
Durch automatische Dokumentation wird die Einhaltung der Sicherheitsmaßnahmen von NIS2-Richtlinien durch das Unternehmen belegt und so der Konformitätsprozess vereinfacht.

Über Serviceware

Serviceware bietet seit mehr als 25 Jahren Software, Beratung und Managed Services zur Digitalisierung moderner Unternehmensprozesse. Von Enterprise Service Management über IT Financial Management bis Security, Data und Endpoint Management – hochautomatisiert und sicher.

Serviceware SE
Serviceware-Kreisel 1
65510 Idstein • Germany
+49 6434 9450 0
contact@serviceware-se.com
www.serviceware-se.com

12/2025

SERVICEWARE