Produkt-Portfolio

Ermöglichung digitaler betrieblicher Resilienz

OTORIO versetzt Betriebs- und Sicherheitsteams in die Lage, digitale und Cyberrisiken proaktiv zu managen und über ein technologiegestütztes Ökosystem einen widerstandsfähigen Betrieb aufzubauen.

Unsere Technologie ermöglicht ein sicheres und umfassendes OT-Risikomanagement mit proaktiver Überwachung sowie praktikablen und kontextbezogenen Abhilfemaßnahmen. Die OTORIO-Produkte und -Methoden für das OT-Risikomanagement werden von erstklassigen Experten für Cybersicherheit und Industriebereiche bereitgestellt.

OTORIOs proaktiver Schutz von OT-Umgebungen unterstützt die Einhaltung von Vorschriften für Industrieunternehmen, MSSPs, Service-Integratoren, Maschinenbauer, Ingenieurbüros und eine Vielzahl von Interessengruppen.

Die Vereinfachung durch Automatisierung und “Noise Reduction” sorgt für Konzentration auf das Wesentliche, effiziente Ressourcenzuweisung und unmittelbare Ergebnisse.

OTORIO

Produkte für intelligente OT-Sicherheit

RAM²™
Kontinuierliche Bewertung, Überwachung und Verwaltung von OT-IT-IIoT-Sicherheitsrisiken

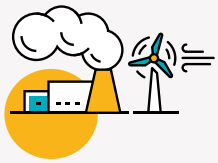
spOT™ Assessment
Bedarfsorientierte OT-Sicherheits- und Konformitätsbewertungen

spOT™ Lifecycle
Sichere und konforme digitale Maschinen

remOT™
Sicherer Fernzugriff auf OT-Anlagen

Warum Sie OTORIO wählen sollten

- Umfassende Einsicht in Anlagen aus bereichsübergreifenden industriellen Datenquellen
- Risikobewertung auf der Grundlage des betrieblichen Kontexts, von einer einzelnen Anlage bis hin zum gesamten Unternehmen
- Befähigung von Betriebs- und Sicherheitsteams, digitale Risiken proaktiv zu mindern
- Ermöglichung der IT-OT-Zusammenarbeit zur effektiven Risikominderung
- Geräuschreduzierung zur Vermeidung von Alert Fatigue
- Out-of-the-Box-Konformität mit Industriestandards und Vorschriften

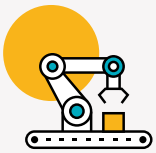


Energie, Versorgungsunternehmen & Bergbau

- Stromerzeugung, -übertragung und -verteilung
- Öl und Gas (Upstream, Midstream und Raffinerie)
- Bergbau

Intelligente Infrastruktur

- Regierung
- Intelligenter Verkehr und Logistik
- Intelligente Gebäude und Städte
- Flughäfen
- Schifffahrt



Fertigung

- Pharmazeutische Industrie
- Automobilindustrie
- Lebensmittel und Getränke
- Chemie
- Zellstoff und Papier

RAM²™

Risiko- und Compliance-Bewertung auf der Grundlage des betrieblichen Kontextes

RAM² von OTORIO ist eine OT-Sicherheitslösung für das proaktive Management digitaler Risiken und den Aufbau widerstandsfähiger Produktions-Abläufe. RAM² bietet eine kontinuierliche, proaktive Risikoidentifizierung, -reduzierung und Konformitätsbewertung für einzelne Anlagen, Produktionslinien und ganze Betriebsstätten. Mit RAM² sind IT- und OT-Teams wirklich miteinander verbunden und für die Zusammenarbeit im Bereich Sicherheit optimiert. OT-Sicherheitsverantwortliche und Anlagenbesitzer erhalten eine bewährte, effiziente und effektive Lösung.

RAM² sammelt, orchestriert und analysiert Daten aus einer Vielzahl von Sicherheits- und Industriequellen, die in der OT-Umgebung vorhanden sind. Dazu gehören IDS, Firewall, EDR, PLC, DCS, SCADA, Historians, technische Systeme und mehr. Die Plattform reichert die Asset-Attribution mit betrieblichem Kontext, Schwachstellen und Gefährdungen an. Sie bietet eine umfassende Bewertung der Sicherheitskontrollen und der Compliance, um nur legitime, priorisierte und relevante Asset-Warnungen anzuzeigen, die Aufmerksamkeit bedürfen.

Die korrelierten Erkenntnisse von RAM² priorisieren die Risiken auf der Grundlage der geschäftlichen Auswirkungen von cyber-physischen Systemen (CPS) und bieten praktische und realisierbare Abhilfemaßnahmen, die auf die OT-Umgebung eines Unternehmens zugeschnitten sind. Die RAM²-Plattform für das OT-Sicherheitsmanagement reduziert die Menge an Rauschen? die von bestehenden Sicherheitslösungen erzeugt wird, erheblich. Darüber hinaus überbrückt sie Kompetenzlücken, um Sicherheits- und Betriebsteams dabei zu helfen, die mittlere Zeit bis zur Entdeckung (MTTD) und Behebung (MTTR) von Risiken zu verbessern.

Wichtigste Vorteile

- RAM² verbessert die operative Widerstandsfähigkeit gegen digitale Risiken
- RAM² reduziert MTTD und MTTR mit einer Sicherheitsanalyselogik (“Analyst-in-a-Box”)
- Die kontextabhängige Risikopriorisierung hilft den Teams, sich auf die wichtigsten Maßnahmen zur Risikominderung zu konzentrieren, um die Sicherheit und Effizienz der betrieblichen Prozesse zu gewährleisten.
- Verringerung des Rauschens und der Ermüdung von Sicherheitsteams durch Priorisierung von Risikowarnungen, angereichert mit betrieblichem Kontext
- Umfangreiches und genaues Anlageninventar
- Priorisierte Alarme zeigen nur legitime, relevante Alarme von stark gefährdeten Anlagen an - für weniger Lärm? und mehr Kontext
- Skalierbare Integration von Drittanbietern in Sicherheits- und Betriebssysteme für vernetzte OT-IT-IIoT-Umgebungen
- Sofort einsatzbereite Konformität (IEC 62443, NERC CIP, NIST)
- Klare, praktikable, auf OT-Umgebungen zugeschnittene Playbooks zur Risikominderung

RAM²™

Kontinuierliche OT-Risikobewertung, Überwachung und Management

Wie funktioniert es?

01

Daten sammeln

Online-/Offline-Netzwerk Überwachungsdaten

Passive, aktive und integrationsbasierte Datenerfassung

02

Anreichern & Analysieren

Marktführende Schwachstellen-Datenbank

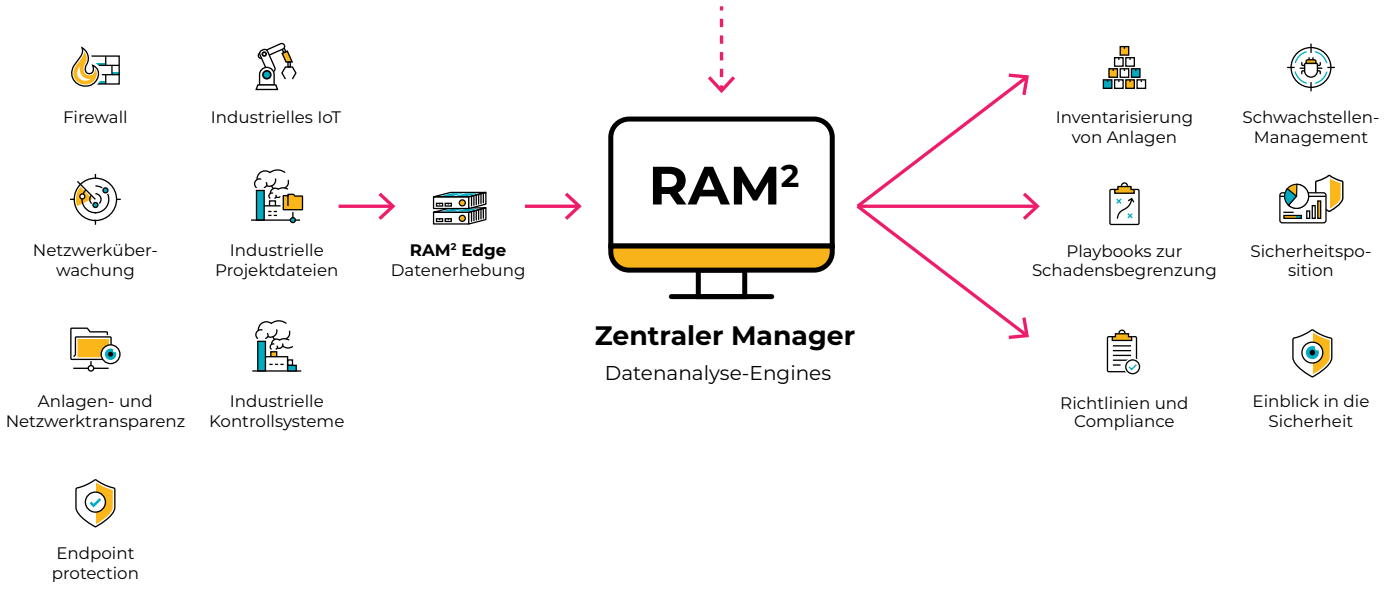
Basierend auf OTORIOs Forschung und professionellen Dienstleistungen

03

Ergebnisse

Dashboards und Berichte

Eine einheitliche organisatorische Ansicht des digitalen Risikos



spOT™ ASSESSMENT

Risiko- und Compliance-Bewertung auf der Grundlage des betrieblichen Kontextes

OTORIO hat spOT Assessment entwickelt, um effiziente, schnelle und effektive regelmäßige technische Risikobewertungen von Betriebsnetzwerken durchzuführen. spOT Assessment beschleunigt den Prozess der technischen OT-Bewertung und -Audits, indem es den Zeitaufwand und die erforderlichen Ressourcen für die Durchführung um bis zu 75% reduziert. Es ermöglicht die Prüfung einer Anlage, eines Standorts oder sogar der Sicherheitslage einer ganzen Organisation über mehrere Standorte hinweg.

spOT Assessment ist einfach einzurichten und auszuführen, entweder vor Ort oder aus der Ferne. Es erstellt automatisch ein angereichertes OT-IT-IIoT-Inventar und analysiert es.

Sobald Sicherheitslücken identifiziert sind, werden die Risiken nach ihrer Auswirkung auf Prozesse und andere Komponenten priorisiert. spOT Assessment liefert klare, praktische Empfehlungen für die schrittweise Behebung jeder identifizierten Schwachstelle, Sicherheitslücke, Gefährdung und Konformitätsabweichung, die alle im spOT Assessment Sicherheitsbericht detailliert aufgeführt sind.

Der ROI für spOT Assessment steigt mit der Zeit. Durch die erneute Bewertung derselben Umgebung bietet spOT historische Vergleiche, Risikotrends und die Möglichkeit, fortlaufende Warnmeldungen als Service zu liefern.

Wichtigste Vorteile

- Ein Bericht zur technischen Bewertung von OT-Sicherheitskontrollen mit Best Practices zur Härtung von Sicherheitskonfigurationen und Netzwerkschnittstellen
- Beschleunigt den Prozess der technischen OT-Bewertung und -Auditierung durch Reduzierung von Zeit und Aufwand
- Durchführung einer sicheren Bewertung der betrieblichen Sicherheitslage ohne Beeinträchtigung des laufenden Betriebs
- Risikobewertungsbericht, der die Schwachstellen nach ihrer Auswirkung auf die OT-Umgebung priorisiert
- Kontextualisierte Abhilfemaßnahmen für jedes Risiko, die auf einfache, umsetzbare und für Betriebsumgebungen geeignete Weise dargestellt werden
- Sofort einsatzbereite Konformität auf Anlagen- und Standortebene (IEC 62443, NERC CIP, NIST) und Umsetzung von Unternehmensrichtlinien
- Realitätsgetreue Bestandsaufnahme der Anlagen mit einem tieferen und umfassenderen Verständnis ihrer Rolle, Auswirkungen, Schwachstellen und Organisationsstruktur
- Verbesserung des ROI für vorhandene Sicherheitstools

spOT™ ASSESSMENT

Risiko- und Compliance-Bewertung auf der Grundlage des betrieblichen Kontextes

Wie funktioniert es?

01

Daten sammeln

Integration in die Sicherheitskontrollen von kritischen Anlagen und betrieblichen Systemen

02

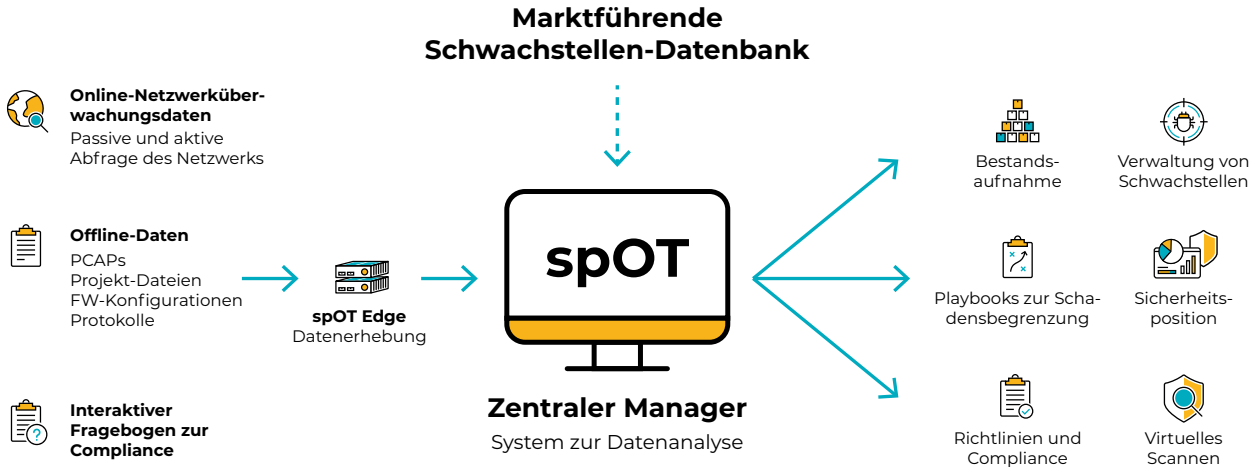
Anreichern und Analysieren

Basierend auf OTORIOs Forschung und professionellen Dienstleistungen

03

Bewertungsberichte

Umfassender Bericht zur Bewertung der digitalen Sicherheit



spOT™ LIFECYCLE

Maschinensicherheit und Konformitätsprüfung

spOT Lifecycle von OTORIO ermöglicht es Maschinenbauern, die Prüfung der Einhaltung von Richtlinien, die Datenerfassung und die Bewertung der Cybersicherheit zu automatisieren. Heutzutage ist der Schutz vor Cybersicherheits- und Compliance-Risiken während der gesamten Lebensdauer einer Maschine notwendig. spOT Lifecycle ermöglicht es Maschinenbauern, Kundenrichtlinien, Best Practices, Garantieanforderungen und gesetzliche Vorschriften einzuhalten.

spOT Lifecycle wurde entwickelt, um die digitale Maschinensicherheit zu vereinfachen und zu automatisieren. Es reduziert den Zeitaufwand und die Kosten für die FAT- (Factory Acceptance Test) und SAT-Prozesse (Site Acceptance Test) für digitale und Cyber-Security mit einer genauen Bestandsaufnahme der Anlagen, sofortiger Konformität, automatischer Identifizierung von OT-Sicherheitslücken und Dokumentation.

spOT Lifecycle lässt sich in den bestehenden Inbetriebnahmeprozess eines Unternehmens integrieren, um eigenständige Maschinen abzufragen, den Cyberschutz und die Konformität zu überprüfen, bevor eine neue Maschine an die Produktionslinie angeschlossen wird oder nach der Wartung.

Es ermöglicht Maschinenherstellern auch, Sicherheit als Service nach der Auslieferung über den gesamten Lebenszyklus der Maschine auf dem Gelände des Kunden anzubieten. spOT Lifecycle prüft regelmäßig Konfigurationen und Schwachstellen während der Serviceeinsätze und der “virtuellen Abfrage” des Fingerabdrucks der Maschine auf neue, öffentlich bekannte Schwachstellen. Die Lösung gibt klare Empfehlungen zur Behebung von Lücken und zur Absicherung gegen Ransomware-Angriffe.

Wichtigste Vorteile

- Standardisiertes, genaues Audit von Maschinen, ohne dass Kenntnisse der Cybersicherheit erforderlich sind
- Vollständig tragbares Plug-and-Query-Gerät zur Überprüfung der Konformität von Maschinen, wo auch immer sie sich befinden mögen
- Umfassende Bestandsaufnahme und Änderungsverwaltung von OT-IT-IIoT-Ressourcen in Maschinen und der Produktionslinie
- Überprüfung der Konformität von Maschinen mit sich ständig ändernden Sicherheitsrichtlinien und Risiken
- Sofortige Identifizierung und Benachrichtigung von Kunden über neue Sicherheitsschwachstellen und Risiken
- Klare Empfehlungen zur Behebung von Sicherheitslücken in Maschinen und zur Vorbereitung auf Ransomware
- Senkung der FAT/SAT-Kosten für Cybersicherheit und Verbesserung des Serviceangebots durch automatisierte Cybersicherheit für Maschinen
- Sicherstellen, dass die Maschinen bei der Inbetriebnahme und Auslieferung die digitalen Sicherheitsrichtlinien, Best Practices und Vorschriften einhalten

spOT™ LIFECYCLE

Maschinensicherheit und Konformitätsprüfung

Wie funktioniert es?

01

Inbetriebnahme einer Maschine

Der Inbetriebnahmetechniker verwendet spOT Lifecycle zur Abfrage einer neuen Maschine während der FAT

02

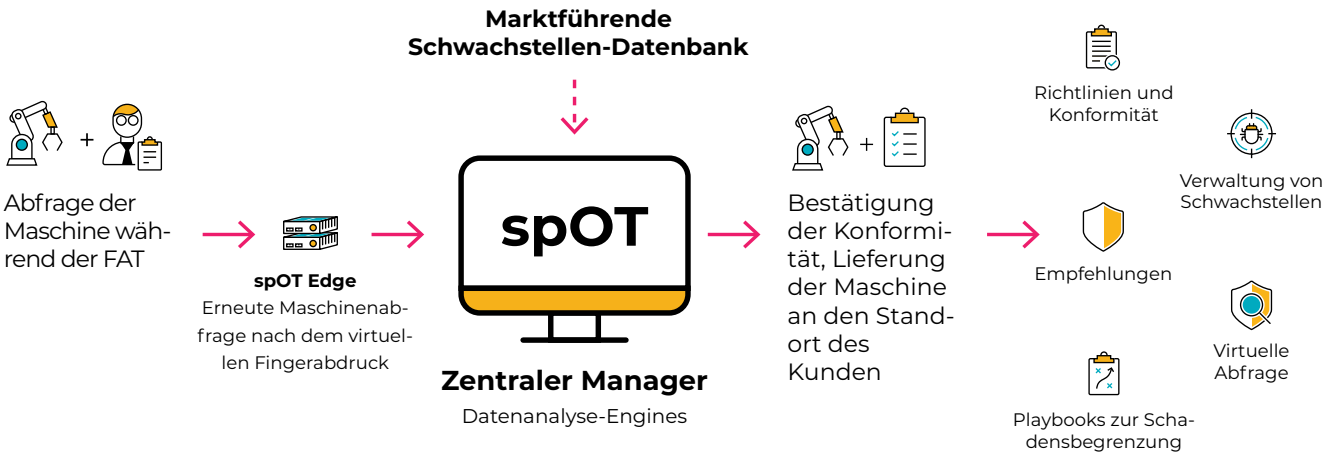
Anreichern und Analysieren

"Virtuelle Abfrage" nach neuen Schwachstellen auf der Grundlage des Fingerabdrucks der Maschine

03

Machine Security as a Service

Der Servicetechniker nutzt spOT Lifecycle für regelmäßige icherheitsüberprüfungen während Serviceeinsätzen, vor Ort oder als Remote-Service.



remOT™

Sicherer Fernzugriff auf betriebliche Anlagen

remOT von OTORIO bietet einen sicheren, einfachen und vollständig kontrollierten Fernzugriff auf die Betriebsumgebung. Als clientlose Lösung ohne Agenten, VPN und Jump Server vereinfacht remOT die Konnektivität zu Anlagen für Drittanbieter, Service Provider und interne Nutzer, ohne Kompromisse bei der Sicherheit einzugehen. Die Lösung lässt sich nahtlos an die Anforderungen Ihres Unternehmens anpassen, während die OT-Netzwerksegmentierung zwischen den Standorten beibehalten wird, und das bei niedrigen Gesamtbetriebskosten (TCO).

Mit remOT wird der Zugriff über ein separates, mandantenfähiges Cloud-Account-Management geregelt und kontrolliert. Der Zugriff wird nur autorisierten Mitarbeitern und autorisierten Dritten auf bestimmte Anlagen gewährt, je nach den Anforderungen industrieller Netzwerke. remOT bietet volle Transparenz für jede sichere Remote-Verbindung.

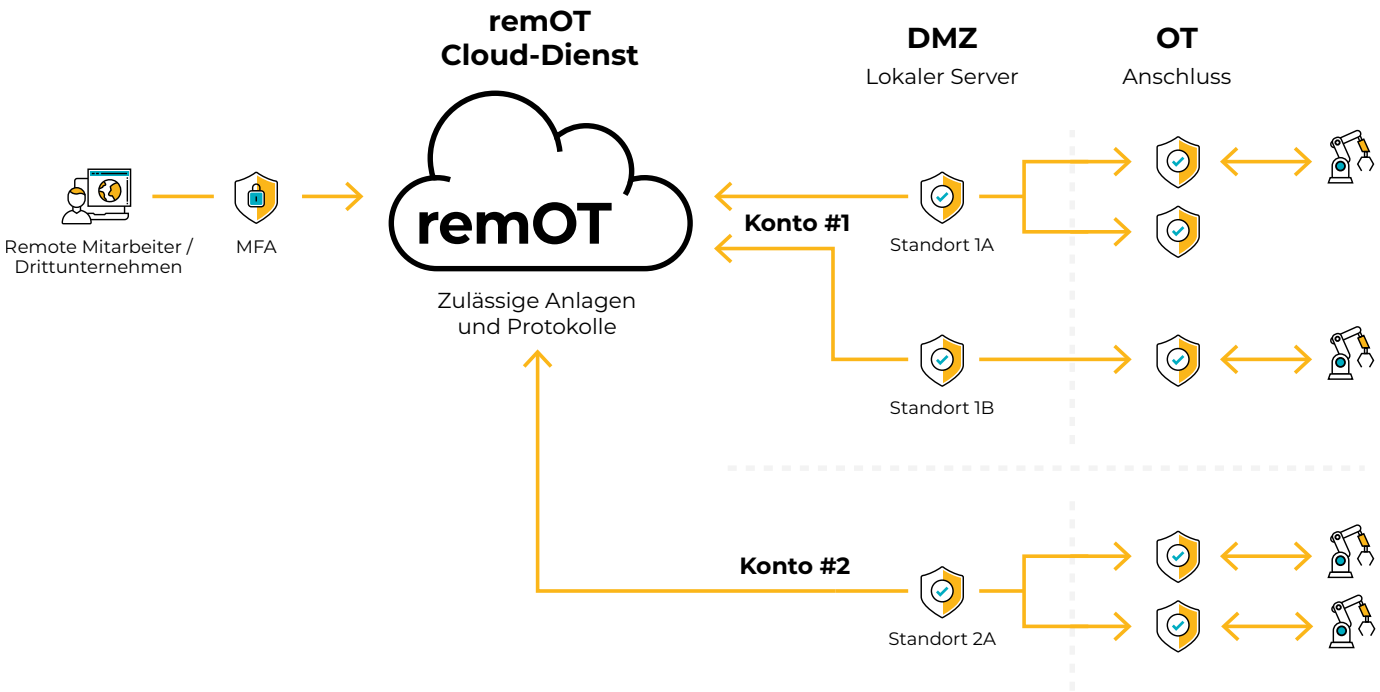
Wichtigste Vorteile

- Zero-Trust-Architektur mit sicherem Zugang für interne und externe Benutzer
- Nahtloser Fernzugriff auf bestimmte Anlagen an den Zielstandorten über den Webbrowser ohne Agenten, ohne VPN und ohne Jump-Server
- Kontrollierter Zugriff mit einmaliger Anmeldung (Single-Sign-On)
- Audit jeder Benutzer- und Admin-Aktion
- Designbedingte Sicherheit mit vollständiger TLS-Kommunikation, Schutz von Anmeldedaten und Assets, Protokoll- und Sitzungsisolierung
- Getrennte, mandantenfähige Cloud-Kontoverwaltung
- Sichere und einfach zu bedienende Dateiübertragung
- Vollständige Kontrolle und Überwachung jeder sicheren Remote-Verbindung
- Einfache Skalierbarkeit bei niedrigen TCO

remOT™

Sicherer Fernzugriff auf betriebliche Anlagen

Wie funktioniert es?



Produkte	Wesentliche Merkmale	Anwendungsfälle
RAM²™ Kontinuierliche Bewertung, Überwachung und Verwaltung von OT-IT-IIoT-Sicherheitsrisiken	• Kontinuierliche, proaktive OT-Sicherheitsbewertung • Zuordnung von Sicherheitsrisiken zu betrieblichen Prozessen • Erkennung von Vorfällen in Echtzeit • Kontextbezogenes OT-Bestandsverzeichnis • Unerreicht flexible Integration mit Sicherheits- und Industriesystemen • Risikopriorisierung nach betrieblichen Auswirkungen • Bewertung von Schwachstellen • Identifizierung von Sicherheitslücken und Schwachstellen • Bewertung der Segmentierung • Klare, umsetzbare OT-Playbooks zur Abschwächung von Schwachstellen • Fallmanagement von Risiken mit Ticketing • Sofort einsatzbereite Konformitäts- und Governance-Bewertung auf Anlagen- und Standortebene für die Standards NIST 82-800, IEC-62443, usw. • Einzigartiger digitaler Cyber-Zwilling und nicht-intrusive Simulationen von Einbrüchen und Angriffen - maßgeschneiderte Sicherheit für jedes einzelne Netzwerk • Dashboards für umfassende Übersichten über die Sicherheitslage, die Einhaltung von Richtlinien und mehr • Umfangreiche, granulare Berichte, die an die Bedürfnisse einer Organisation angepasst werden können	Erweiterte OT-IT-IIoT-Transparenz Schwachstellen-Management Bewertung der Segmentierung Kontinuierliche Identifizierung von Sicherheitslücken und Schwachstellen Erkennung von Vorfällen in Echtzeit OT-kontextualisierte Risikobewertung. Sicherheitskonformität und Governance
spOT™ Assessment Sicherheits- und Konformitätsbewertungen	• Technische Bewertung der OT-Sicherheit für Prüfer und Auditoren • Umfangreiche und genaue Bestandsaufnahme der Anlagen • Automatisierte Risikobewertungsberichte mit nach Prioritäten geordneten Schwachstellen • Praktische Empfehlungen zur Risikominderung • Regelmäßige Überprüfung auf aktuelle Sicherheitsbedrohungen • Sichere Bewertung der betrieblichen Sicherheitslage ohne Beeinträchtigung des laufenden Betriebs • Flexible Integrationen mit bestehenden OT-IT-IIoT-Lösungen • Sofort einsatzbereite Bewertung der Compliance und Governance auf Anlagen- und Standortebene	Risikobewertung einer Produktionslinie, eines Standorts oder einer gesamten OT-Organisation Technische OT-Bewertung OT-Audit-Verfahren Beschleunigen Sie die technische OT-Bewertung
spOT™ Lifecycle Sichere digitale Maschinen	• Eine Lösung für Maschinenbauer • Mobile und portable Abfrage von Einzelmaschinen • Inventarisierung des Maschinenparks • Schwachstellenanalyse für Maschinen • Richtlinien- und Konformitätsprüfung von einem einzelnen Gerät bis hin zur Maschinen- und Linienebene • Sicherheitshärtung von Maschinen, um für Ransomware gerüstet zu sein • Abhilfemaßnahmen für jede identifizierte Sicherheitslücke • Virtuelle Abfrage des Fingerabdrucks eines Rechners auf neue Schwachstellen • Compliance-Bestätigungsbericht für den Endkunden • Regelmäßige Abfrage eines Gerätes während seines gesamten Lebenszyklus	Cybersecurity FAT/SAT von Maschinen Laufendes Schwachstellenmanagement als Dienstleistung Verbesserung der Sicherheit von Maschinen durch Design Regelmäßige Maschinen-Cybersicherheit als Dienstleistung
remOT™ Sicherer Fernzugriff	• Zero-Trust Architektur • Nahtloser Fernzugriff auf bestimmte Anlagen an Zielstandorten über den Webbrowser ohne Agenten, VPN und Jump-Server • Kontrollierter Zugang mit einmaliger Anmeldung (Single-Sign-On) • Audit jeder Benutzer- und Admin-Aktion • Sicherheit durch Design mit vollständiger TLS-Kommunikation, Schutz von Anmeldedaten und Assets, Protokoll- und Sitzungsisolierung • Getrennte, mandantenfähige Cloud-Kontoverwaltung • Sichere und einfach zu bedienende Dateiübertragung	Bereitstellung eines sicheren Ferndienstes durch einen Anbieter oder einen Dienstleister für mehrere Endkunden und Umgebungen Verwaltung des sicheren Fernzugriffs auf eine OT-Umgebung durch mehrere Drittparteien Kontrollierter Zugriff auf Netzwerkressourcen nur durch autorisierte Mitarbeiter

OTORIO

Über uns

OTORIO ist ein End-to-End-OT-Sicherheitsunternehmen, das proaktive, industrietaugliche Lösungen für das digitale Risikomanagement anbietet, um die Geschäftskontinuität und den laufenden Betrieb in Unternehmen und Organisationen weltweit zu schützen. Gemeinsam mit unseren Partnern bieten wir umfassende Lösungen und Dienstleistungen zur Risikobewertung, -überwachung und -verwaltung für kritische Infrastrukturen, intelligente Transport- und Logistiksysteme und industrielle Fertigungsunternehmen an, die es ihnen ermöglichen, ihre digitale Transformation in vernetzten OT-IT-IIoT-Umgebungen effektiv zu sichern. Unser globales Team verfügt über die umfassende Erfahrung führender nationaler Cybersicherheitsexperten in Kombination mit fundiertem Fachwissen in den Bereichen Betrieb und Industrie.

otorio.com

CN 231122