Ein Edge-Architektur-Ansatz zum Schutz industrieller IoT-Netzwerke

Angesichts der zunehmenden Digitalisierung und Vernetzung der Betriebsumgebungen mit der IT-Umgebung erkennen Industrieunternehmen die Notwendigkeit, Betriebstechnologie und das industrielle IoT vor Cyberangriffen zu schützen. Die Bereitstellung von Firewalls zum Aufbau einer demilitarisierten Zone (DMZ) zwischen industriellen Netzwerken und der IT-Domäne ist der obligatorische erste Schritt. Da Unternehmen jedoch immer mehr Geräte miteinander verbinden, mehr Remote-Zugriff ermöglichen und neue Anwendungen erstellen, wird die Air-Gap – also die völlige Isolation vom Internet – zunehmend schwieriger. Dieser Ansatz ist also heutzutage nicht mehr ausreichend.

Sicherheitslösungen für industrielle Netzwerke überwachen in der Regel den Netzwerkverkehr, um Einblicke in Ressourcen, Verhaltensweisen, schädliche Aktivitäten und Bedrohungen zu erhalten. Der Prozess der Bewertung und des Tests dieser Lösungen verläuft anfangs gut – nach einem erfolgreichen Proof-of-Concept beginnen Industrieunternehmen mit der Bereitstellung in großem Umfang. Dabei tauchen die ersten Probleme auf.

Häufig ist es für Unternehmen kostenintensiv, genügend Security-Appliances zu erwerben, um ihre gesamte Betriebsumgebung abzudecken. Oder das Netzwerkteam verfügt nicht über die Ressourcen, um eine Flotte von Security-Appliances bereitzustellen, zu warten und zu verwalten. Der zusätzliche Datenverkehr, der von diesen Appliances erzeugt wird, würde wahrscheinlich ein separates Netzwerk erfordern – was wiederum die Ressourcen für Bereitstellung, Wartung und Verwaltung erfordert.

Glücklicherweise gibt es einen besseren Ansatz zur Sicherung der OT-Umgebung. In diesem Whitepaper werden drei heute verfügbare Architekturansätze sowie eine Alternative vorgestellt, die OT- und IT-Teams die erforderliche Skalierbarkeit und Transparenz bieten, ohne zusätzliche Ressourcen zu benötigen.

Herausforderungen beim Schutz eines IIoT-Netzwerks

Mangelnde Transparenz:

Da industrielle Netzwerke sehr alt und weit verstreut sein können und viele Auftragnehmer umfassen, verfügen Betreiber oft nicht über eine genaue Bestandsaufnahme der Netzwerkkomponenten. Dadurch können sie nur begrenzt eine sichere Kommunikationsarchitektur aufbauen.

Mangelnde Kontrolle:

Mangelnde Transparenz bedeutet auch, dass die Betreiber häufig nicht wissen, welche Geräte miteinander kommunizieren oder welche Kommunikation industrielle Geräte von außen erreicht. Sie können nicht kontrollieren, was Sie nicht kennen.

Verständnis der betrieblichen Technologieumgebung

Um das Skalierbarkeitsproblem in Bezug auf den Schutz der Betriebsumgebung umfassend zu verstehen, müssen wir mit der OT-Umgebung selbst beginnen. Industrielle Steuerungsnetzwerke verbinden viele softwaregesteuerte Automatisierungsgeräte (SPS, RTU, IED, DCS usw.) zur Prozessausführung. Diese OT-Geräte wurden über viele Jahre (manchmal sogar Jahrzehnte) bereitgestellt – zu einer Zeit, als die Cybersicherheit kein Thema war. Daher verfügen sie nicht über strenge Sicherheitsrichtlinien. Erschwerend kommt hinzu, dass einige Geräte von Drittanbietern bereitgestellt, verwaltet und außer Betrieb genommen werden können.

Wenn Unternehmen versuchen, ihr industrielles IoT-Netzwerk zu schützen, stoßen sie auf zwei Hauptprobleme:

1. **Mangelnde Transparenz:** Da industrielle Netzwerke sehr alt und weit verstreut sein können und viele Auftragnehmer involviert sind, verfügen Betreiber oft nicht über eine genaue Bestandsaufnahme der Netzwerkkomponenten. Dadurch können sie nur begrenzt eine sichere Kommunikationsarchitektur aufbauen.
2. **Mangelnde Kontrolle:** Mangelnde Transparenz bedeutet auch, dass die Betreiber häufig nicht wissen, welche Geräte miteinander kommunizieren oder welche Kommunikation industrielle Geräte von außen erreicht. Sie können nicht kontrollieren, was Sie nicht kennen.

Der erste Schritt zum Schutz eines industriellen IoT-Netzwerks ist Transparenz. Sie müssen verstehen, welche Geräte sich im Netzwerk befinden, was sie kommunizieren und wohin diese Kommunikation geht.

Transparenz des Betriebstechnologie-Netzwerks

Die Technologie für Netzwerktransparenz ist heute verfügbar. Deep Packet Inspection (DPI) entschlüsselt alle Kommunikationsströme und extrahiert Nachrichteninhalte und Paket-Header. So erhalten Sie einen Überblick darüber, welche Geräte Sie schützen müssen und welche Richtlinien dafür erforderlich sind.

Mit DPI können Sie Geräteinformationen wie Modell, Marke, Teilenummern, Seriennummern, Firmware- und Hardwareversionen, Rack-Steckplatzkonfigurationen und mehr erfassen. Außerdem können Sie nachvollziehen, was über das Netzwerk kommuniziert wird. Sie können beispielsweise sehen, ob jemand versucht, neue Firmware in ein Gerät hochzuladen oder die Variablen für den industriellen Prozess zu ändern.

Um vollständige Transparenz zu erreichen, muss der gesamte Netzwerkverkehr untersucht werden. Es ist wichtig zu beachten, dass in einem industriellen Netzwerk der meiste Datenverkehr hinter einem Switch auf Zellenebene erfolgt, da dort die Maschinen-Controller bereitgestellt werden. Nur sehr wenig Datenverkehr geht in das zentrale Netzwerk.

Was ist Deep Packet Inspection?

Deep Packet Inspection (DPI) ist eine Art der Datenverarbeitung, die alle Kommunikationsströme entschlüsselt, um Informationen aus den Paket-Headern sowie die Payload der Nachricht zu extrahieren. Sie erfordert perfekte Kenntnisse des Kommunikationsprotokolls, um es decodieren und den Inhalt der Kommunikation verstehen zu können. Dies kann in industriellen Netzwerken, in denen viele Kommunikationsprotokolle der Anbieter von Kontrollsystemen herstellerspezifisch sind, schwierig zu erreichen sein.

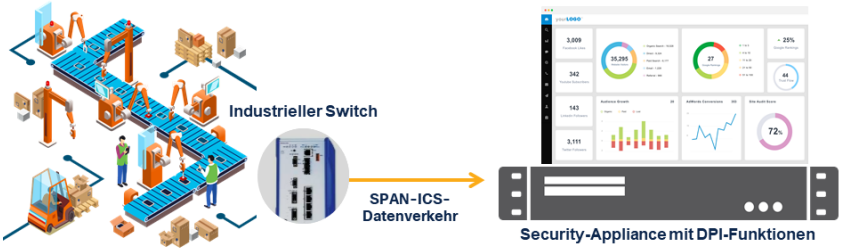
Was ist SPAN?

Switched Port Analyzer (SPAN) ist eine Methode zur Überwachung des Netzwerkverkehrs, die eine Kopie jedes Pakets, das einen Netzwerk-Switch passiert, an einen anderen Port weiterleitet, an den das Netzwerkanalysegerät angeschlossen ist.

Beim Sammeln von Netzwerkpaketen zur Durchführung von DPI konfigurieren Anbieter von Sicherheitslösungen in der Regel SPAN-Ports auf Netzwerk-Switches und verwenden eine von drei Architekturen:

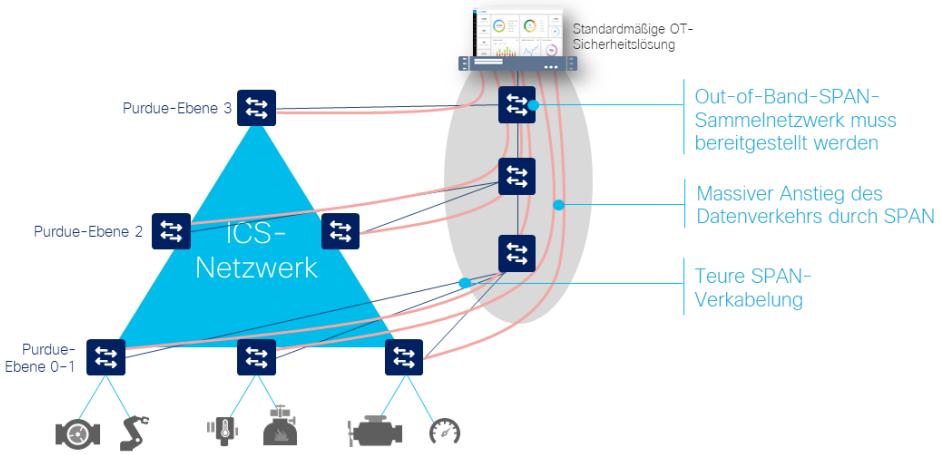
1. Senden des gesamten Datenverkehrs an einen zentralen Server, der DPI-Daten verarbeitet
2. Bereitstellen dedizierter Sensor-Appliances auf jedem Netzwerk-Switch
3. Senden des Datenverkehrs an dedizierte Sensor-Appliances, die an verschiedenen Orten im Netzwerk bereitgestellt werden

Typische ICS-Erkennungslösungen sind abhängig von SPAN



Diese Ansätze bieten zwar Netzwerktransparenz, bringen aber auch neue Herausforderungen mit sich. Die Konfiguration von Netzwerk-Switches zum Senden von Datenverkehr an einen zentralen Server erfordert doppelte Netzwerk-Flows. In der Regel wird ein neues Out-of-Band-Netzwerk benötigt, um diesen zusätzlichen Datenverkehr zu transportieren, was komplex und kostspielig sein kann. Dies kann zwar für einen sehr kleinen Industriestandort akzeptabel sein, in hoch automatisierten Branchen, die viel ICS-Datenverkehr generieren (z. B. in der Fertigung), oder wenn Geräte an Standorten ohne oder mit schlechter Netzwerkverbindung (Öl- und Gas-Pipelines, Wasser- oder Stromverteilung usw.) verteilt sind, ist es jedoch keine ernsthafte Alternative.

SPAN-basierte Lösungen verursachen enorme zusätzliche versteckte Kosten



3 gängige Ansätze zum Schutz des IIoT

1. Senden des gesamten Datenverkehrs an einen zentralen Server, der DPI-Daten verarbeitet
2. Bereitstellen dedizierter Sensor-Appliances auf jedem Netzwerk-Switch
3. Senden des Datenverkehrs an dedizierte Sensor-Appliances, die an verschiedenen Orten im Netzwerk bereitgestellt werden

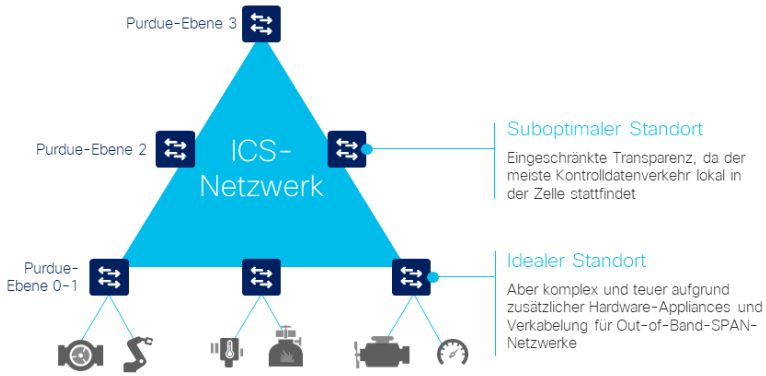
Diese Ansätze bieten zwar Netzwerktransparenz, bringen aber auch neue Herausforderungen mit sich. Die Konfiguration von Netzwerk-Switches zum Senden von Datenverkehr an einen zentralen Server erfordert doppelte Netzwerk-Flows. In der Regel wird ein neues Out-of-Band-Netzwerk benötigt, um diesen zusätzlichen Datenverkehr zu transportieren, was komplex und kostspielig sein kann.

Durch den Anschluss von Sensor-Appliances an Netzwerk-Switches werden Probleme im Zusammenhang mit der Duplizierung des Netzwerkverkehrs behoben. Die Installation, Verwaltung und Wartung dedizierter Hardware kann jedoch schnell zu Kosten- und Skalierbarkeitsproblemen führen.

RSPAN reduziert die Anzahl der Appliances, die für vollständige Transparenz erforderlich sind, erhöht aber gleichzeitig den Datenverkehr, der durch das industrielle Netzwerk fließt, was zu Jitter führt.

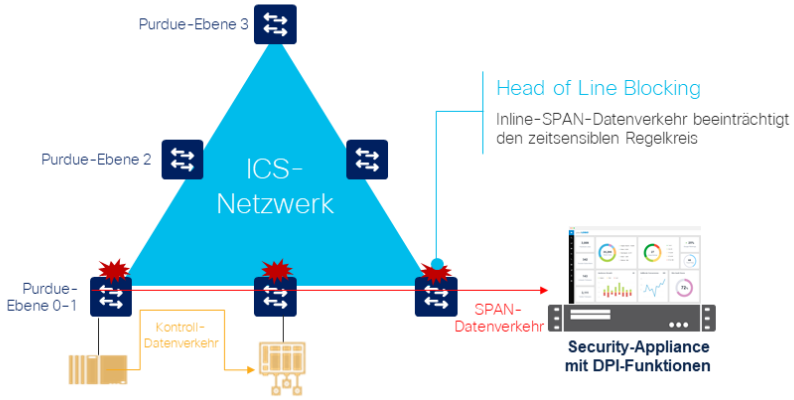
Durch den Anschluss von Sensor-Appliances an Netzwerk-Switches werden Probleme im Zusammenhang mit der Duplizierung des Netzwerkverkehrs behoben. Die Appliance erfasst und analysiert den Netzwerkverkehr lokal und sendet Daten nur zur weiteren Analyse an einen Server. Die Installation, Verwaltung und Wartung dedizierter Hardware kann jedoch schnell zu Kosten- und Skalierbarkeitsproblemen führen. Da der Großteil des industriellen Datenverkehrs lokal ist, erfordert die vollständige Transparenz die Bereitstellung von Appliances auf jedem einzelnen Switch im Netzwerk, was die Kosten und Komplexität auf ein nicht tolerierbares Maß anhebt.

Der DPI-Standort ist entscheidend für eine effektive ICS-Sicherheit



Einige Technologieanbieter versuchen, dieses Problem mit Remote-SPAN (RSPAN) anzugehen. RSPAN ermöglicht es Ihnen, Datenverkehr von einem Switch ohne Sensor-Appliance auf einen Switch mit einer solchen zu duplizieren.

Remote-SPAN führt zu Jitter



Dieser Ansatz reduziert zwar die Anzahl der Appliances, die für umfassende Transparenz erforderlich sind, erhöht aber gleichzeitig den Datenverkehr, der durch das industrielle Netzwerk fließt. Der Datenverkehr wird vervielfacht, weil Sie ihn duplizieren, um ihn auf einen Remote-Switch zu übertragen. Und je mehr Datenverkehr im Netzwerk, desto langsamer wird es, was zu Jitter führt – häufig ein inakzeptabler Kompromiss in industriellen Netzwerken, in denen Prozesse schneller ablaufen und Maschinen rechtzeitig synchronisiert werden müssen.

Vorteile eines DPI-fähigen Switches

Ein industrieller Switch mit nativer DPI-Funktion macht die Duplizierung von Netzwerk-Flows und die Bereitstellung zusätzlicher Appliances überflüssig. Um Transparenz und Sicherheitsfunktionen zu erhalten, müssen Sie lediglich eine Funktion im Netzwerk-Switch, Router oder Gateway aktivieren.

Die Vorteile:

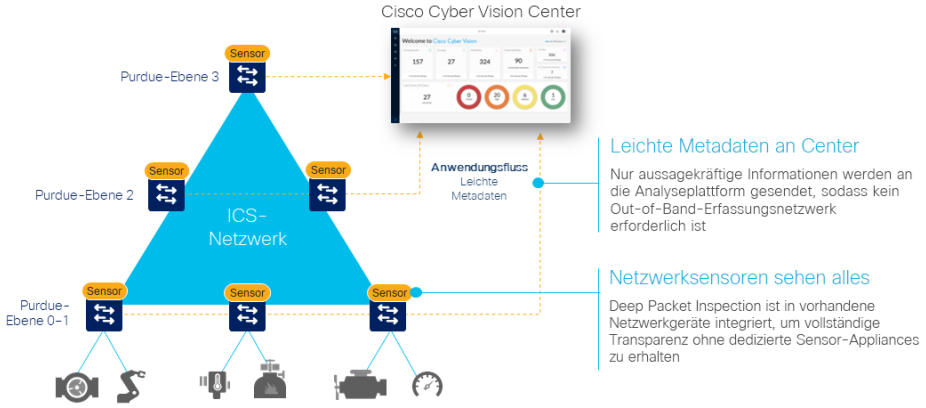
- Kosten, Datenverkehr und Betriebsaufwand werden minimiert.
- Der Datenverkehr wird lokal analysiert, und es werden nur Lightweight-Metadaten an einen zentralen Server gesendet, sodass keine Überlastung entsteht und keine zusätzliche Bandbreite benötigt wird.
- Die IT kann die bestehende Netzwerkinfrastruktur nutzen, um den industriellen Betrieb zu sichern, ohne zusätzliche Hardware beschaffen, bereitstellen und verwalten zu müssen.
- OT erreicht eine nie dagewesene Transparenz der Betriebsabläufe, da eingebettete Sensoren analytische Einblicke in jede Komponente der industriellen Kontrollsysteme liefern.

Alternativen zu SPAN

Anstelle von SPAN können Unternehmen Netzwerk-TAPs, Port-Aggregatoren oder virtuelle Switches verwenden, aber diese Alternativen bringen auch ihre eigenen Nachteile mit sich: 1) Unternehmen müssen weiterhin dedizierte Appliances beschaffen und bereitstellen, 2) Konfiguration und Verwaltung sind nicht unbedingt einfach und 3) das Senden von Datenverkehr an die OT-Sicherheitsplattform erfordert ein Out-of-Band-Netzwerk, um Auswirkungen auf das Produktionsnetzwerk zu vermeiden.

Es gibt einen besseren Weg, um vollständige Netzwerktransparenz zu erreichen: Integrieren Sie DPI-Funktionen in die vorhandene Netzwerkhardware. Ein industrieller Switch mit nativer DPI-Funktion macht die Duplizierung von Netzwerk-Flows und die Bereitstellung zusätzlicher Appliances überflüssig. Um Transparenz und Sicherheitsfunktionen zu erhalten, müssen Sie lediglich eine Funktion im Netzwerk-Switch, Router oder Gateway aktivieren. Kosten, Datenverkehr und Betriebsaufwand werden minimiert.

Transparenz und Erkennung in Ihre Netzwerkinfrastruktur integriert



Ein DPI-fähiger Switch analysiert den Datenverkehr lokal, um aussagekräftige Informationen zu extrahieren. Es sendet nur einfache Metadaten an einen zentralen Server, der die Analytik und Anomalieerkennung durchführt. Diese Metadaten machen etwa 3–5 % des gesamten Datenverkehrs aus. Der Datenverkehr ist so leichtgewichtig, dass er über das industrielle Netzwerk übertragen werden kann, ohne Überlastungen zu verursachen oder zusätzliche Bandbreite zu benötigen.

Die Einbettung von DPI in Netzwerkausrüstung bietet sowohl IT als auch OT einzigartige Vorteile. Die IT kann die vorhandene Netzwerkinfrastruktur nutzen, um den industriellen Betrieb zu sichern, ohne zusätzliche Hardware beschaffen, bereitstellen und verwalten zu müssen. Da diese Netzwerkelemente den gesamten industriellen Datenverkehr erfassen, können eingebettete Sensoren analytische Einblicke in jede Komponente der industriellen Kontrollsysteme liefern. Infolgedessen erhält die OT nie dagewesene Einblicke in Betriebsabläufe.

Überwachung des Datenverkehrs auf älteren Switches

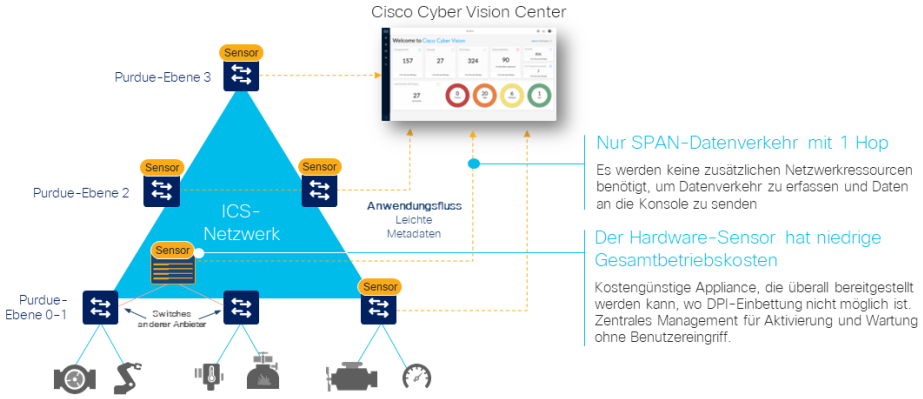
Nicht alle Netzwerkgeräte unterstützen integrierte DPI-Funktionen. Für mehr Transparenz bei dieser lokalen Kommunikation sind Hardware-Sensor-Appliances erforderlich, aber nicht alle Appliances sind gleich.

Um die Vorteile einer Bereitstellung ohne SPAN-Architektur zu erhalten, sollten diese Appliances:

1. zentral verwaltet werden, damit sie einfach bereitgestellt und gewartet werden können
2. über begrenzte Analysefunktionen verfügen, sodass sie auf kostengünstiger Hardware ausgeführt werden können
3. Metadaten nur an die zentrale Konsole senden, sodass sie keine zusätzlichen Netzwerkressourcen benötigen

Allerdings können nicht alle Netzwerkgeräte die integrierte Sensorfunktion unterstützen. Für mehr Transparenz bei dieser lokalen Kommunikation sind Hardware-Sensor-Appliances erforderlich. Beachten Sie, dass nicht alle Appliances gleich sind. Um die Vorteile einer Bereitstellung ohne SPAN-Architektur zu erhalten, sollten diese Appliances 1) zentral verwaltet werden (damit sie einfach bereitzustellen und zu warten sind), 2) über begrenzte Analysefunktionen verfügen (damit sie auf kostengünstiger Hardware ausgeführt werden können) und 3) Metadaten nur an die zentrale Konsole senden (damit Sie keine zusätzlichen Netzwerkressourcen erfordern).

Hardwaresensoren verbinden ältere Switches mit der OT-Sicherheitsinfrastruktur



So kann Cisco helfen

Wenn Unternehmen ihre industriellen Kontrollnetzwerke absichern möchten, müssen sie sich der Auswirkungen der bereitgestellten Lösungen bewusst sein. Der DPI-Standort ist entscheidend. Die Erfassung von Datenverkehr im Aggregation Layer ist mit den meisten heute verfügbaren Lösungen problemlos möglich, führt aber nur zu einer Transparenz des Nord-Süd-Datenverkehrs. Um die Transparenz zu erhalten, die eine wirklich effektive Bedrohungserkennungsstrategie ermöglicht, muss der Netzwerkverkehr auf Zellenebene erfasst werden, was auch die Bereitstellung eines teuren Out-of-Band-SPAN-Netzwerks bedeutet.

Cisco Cyber Vision nutzt eine zweistufige Bereitstellungsarchitektur und einzigartige Edge-Computing-Funktionen, die die Einfachheit und die Kosteneinsparungen bieten, die Industrieunternehmen bei der skalierbaren Bereitstellung von OT-Sicherheit erwarten.

Cyber Vision-Sensoren sind in die industrielle Netzwerkausrüstung von Cisco integriert, sodass Sie überall im Netzwerk problemlos Einblicke in Ost-West- und Nord-Süd-Datenverkehr erhalten. Industrielle Anwendungsflüsse werden am Edge decodiert, sodass keine Spiegelung des Datenverkehrs erforderlich ist, was zu Netzwerküberlastungen und Jitter führen kann. Die Integration von DPI in die vorhandene Netzwerkhardware vereinfacht die Sicherheitsbereitstellung und macht sie skalierbar.

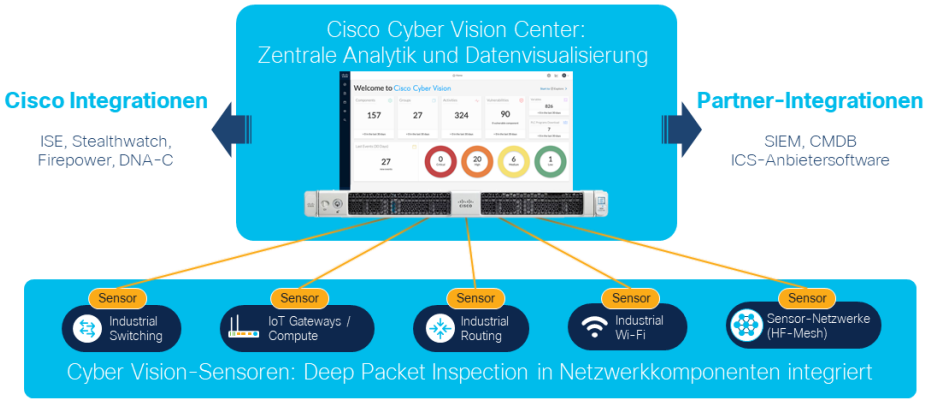
Sind Sie bereit, Ihr industrielles IoT-Netzwerk zu schützen?

Mehr erfahren

Kontakt

Zweistufige Edge-Monitoring-Architektur

Industrielle Cybersicherheit, die skalierbar bereitgestellt werden kann



Die Vorteile von Cisco Cyber Vision sind nicht auf Unternehmen mit Cisco Netzwerken beschränkt. Der Sensor kann auch in einer SPAN-Architektur mit der Cisco IC3000-Hardware-Sensor-Appliance angeboten werden. Dies bietet maximale Bereitstellungsflexibilität, um Ihre Anforderungen mit Ihrem vorhandenen Netzwerk zu erfüllen, während Sie gleichzeitig Zeit haben, ältere Switches durch DPI-fähige Netzwerkgeräte zu ersetzen, die alles sehen können, was damit verbunden ist.

Cisco Cyber Vision bietet umfassende Einblicke in industrielle Kontrollsysteme, damit Sie sichere Infrastrukturen aufbauen und Sicherheitsrichtlinien zur Kontrolle von Risiken durchsetzen können. Durch die Kombination einer einzigartigen Edge-Überwachungsarchitektur und der umfassenden Integration mit dem führenden Security-Portfolio von Cisco lässt sich Cisco Cyber Vision einfach und skalierbar bereitstellen, um die Kontinuität, Widerstandsfähigkeit und Sicherheit des industriellen Betriebs zu gewährleisten.

Sind Sie bereit für den Schutz Ihres industriellen IoT-Netzwerks? Kontakt aufnehmen oder mehr erfahren.

Cisco-IoT-An-Edge-Architecture-Approach-to-Securing-Industrial-IoT-Networks-WP-06232020