# SCHUTZ VOR DEM PERFEKTEN STURM

## WIE NETZWERKVISIBILITÄT IHR UNTERNEHMEN IN EINER ZUNEHMEND DÜSTEREN BEDROHUNGSLAGE SCHÜTZEN KANN

Gigamon® | NOZOMI NETWORKS

# INHALTSVERZEICHNIS

# WILLKOMMEN IN DER VERNETZTEN WELT

Die Vernetzung definiert unser Leben so stark wie nie zuvor. Die Zahl internetfähiger IoT-Geräte wächst exponentiell, 5G verspricht eine Revolution der Konnektivität – und Unternehmen und Organisationen sehen sich gezwungen, die Konvergenz zwischen ITund OT-Technologien ebenso wie die aufkommenden Herausforderungen zu bewältigen.

## BEDINGUNGEN FÜR DEN PERFEKTEN STURM

Doch je stärker die Vernetzung wird, desto stärker öffnen sich die Unternehmen einer digitalen Ausbeutung durch Cyberkriminelle in beispiellosem Ausmaß. Bedrohliche Zunahmen von DDoSAngriffen, Ost-West-Infiltration und staatlich geförderte Cyberkriminalität lassen die Bedrohungslage zunehmend düsterer und gefährlicher werden.

Könnten die erweiterte Konnektivität und das erhöhte Cyberrisiko **gemeinsam den perfekten Sturm auslösen?** In diesem Whitepaper werden die Bedrohungen durch die neuesten Trends beleuchtet, und es wird untersucht, wie Tools für Netzwerkvisibilität und Netzwerkschutz dazu beitragen können, die Sicherheit Ihres Unternehmens und Ihrer Mitarbeiter zu wahren.

# CYBERANGRIFFE: GRÖSSER UND ZERSTÖRERISCHER ALS JE ZUVOR

### VERSTOSS GEGEN WASSERWERTE IN FLORIDA BEDROHT DIE GESUNDHEIT VON 15.000 EINWOHNERN

Hacker haben in einer Wasseraufbereitungsanlage in Oldsmar (Florida, USA) die Kontrolle über die Konzentration von Natriumhydroxid übernommen, einer stark ätzenden Substanz zur Neutralisierung des Säuregehalts im Wasser. Bei diesem Angriff im Februar 2021 wurde die Konzentration kurzzeitig von 100 Teilen pro Million (ppm) auf 11.100 ppm erhöht, bis ein Bediener die richtige Konzentration der Chemikalie wieder einstellte und damit die drohende Katastrophe abwendete. **Wäre dieser Angriff nicht aufgehalten worden, wäre die Gesundheit von 15.000 Einwohnern in ernsthafter Gefahr gewesen.**

2021

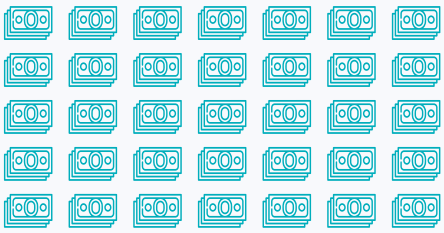
**15.000**

### 100 MILLIARDEN US-DOLLAR KOSTEN ZUR BESEITIGUNG EINES STAATLICH GEFÖRDERTEN HACKERANGRIFFS AUF SOLARWINDS

2020 verursachten Cyberangreifer aufgrund einiger Sicherheitsmängel in Microsoft-, SolarWinds- und VMware-Software Tausende von Datenschutzverletzungen in der gesamten NATO, bei Microsoft, im Europäischen Parlament, in US-amerikanischen und britischen Behörden sowie in zahllosen weiteren Organisationen. Der Angriff ging auf das Konto staatlich geförderter russischer Hacker, blieb monatelang unentdeckt und verursachte weltweit Schäden in Milliardenhöhe, u. a. Kosten von voraussichtlich mehr als **100 Milliarden Dollar für USamerikanische Unternehmen und Behörden.**

2020

**100 Mrd. US-$**



### WANNACRY-ANGRIFF KOSTET UNTERNEHMEN WELTWEIT MEHR ALS 6 MILLIARDEN US-DOLLAR

2017 waren in 150 Ländern mehr als **200.000 Computer** vom WannaCry-Cyberangriff betroffen, dem weltweit schwerwiegendsten Ransomware-Zwischenfall. Ziele waren u. a. der NHS in Großbritannien/Nordirland, Telefonica in Spanien, FedEx in den USA und die Deutsche Bahn. Beim NHS England waren mindestens 80 von 236 Trusts und 603 Primärversorgungszentren infiltriert. Unentbehrliche IT- und Telefonsysteme waren nicht nutzbar; Tausende von Operationen und Patiententermine mussten abgesagt werden, und es entstanden **Kosten von mehr als 92 Millionen Dollar.**

2017

**200.000**

# DIE BEDROHUNGSLAGE

### 1. KONVERGENZ VON IT UND OT VERVIELFACHT DIE BEDROHUNGEN

In sämtlichen Branchen nimmt die Konvergenz der **OT-** *(operative Technologie)* und der **IT-Umgebungen** *(Informationstechnologie)* an Tempo zu.

Die IT-Cybersicherheit hat sich längst als Branche mit ausgereiften Lösungen zur Abwehr von Cyberkriminellen etabliert, doch die OT-Cybersicherheit steckt noch in den Kinderschuhen – damit ist die **OT ein relativ weiches Ziel für Hacker.**

OT war anfangs relativ weit vom Internet abgeschirmt und unempfänglich gegen Cyberbedrohungen. Mittlerweile werden jedoch mehr und mehr Fertigungsverfahren durch IoT-Geräte und Cloud-Computing gesteuert. Die so entstandene Konfluenz der Technologien hat die Angriffsfläche erheblich ausgeweitet, sodass **Malware nahtlos zwischen IT und OT wandern kann.**

OT-Verletzungen bleiben oft einige Zeit unentdeckt und verursachen Produktionsstörungen, Mängel bei den Erzeugnissen oder Unterbrechungen bei den Dienstleistungen mit entsprechenden Schäden hinsichtlich des **Markenrufs,** des **Finanzergebnisses** und des **Kundenvertrauens.**

Der OT-Schutz verlangt nach einer zweigleisigen Strategie:

+ **Erkennung** und **Beseitigung** von Schwachstellen in bestehenden Technologien mit langem Lebenszyklus
+ **Einbindung** der Cybersicherheit beim Design neuer OT-Systeme

### 2. 5G-EINFÜHRUNG BRINGT ERHEBLICHE NEUE RISIKEN MIT SICH

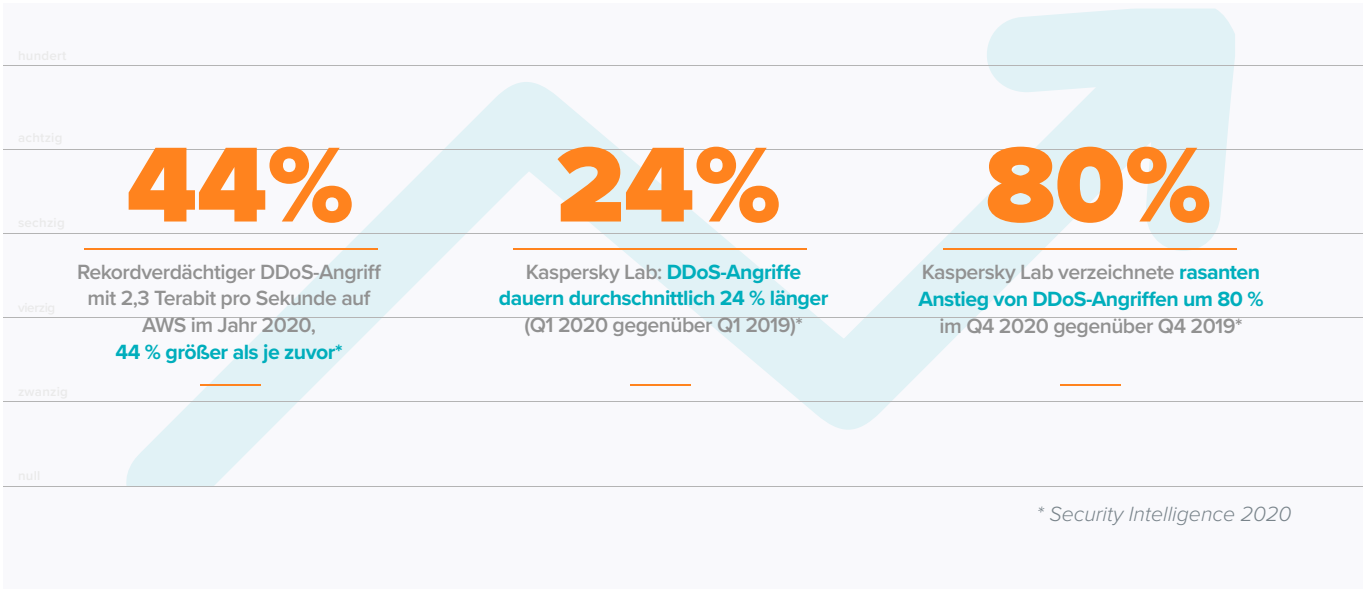
Laut allgemeiner Meinung öffnet 5G böswilligen Hackern potenziell Tür und Tor, episches Chaos **für Privatpersonen, Unternehmen und staatliche Organisationen in der ganzen Welt** auszulösen.

Unzählige 5G-Anwendungen werden neue Möglichkeiten für die Verwaltung von Infrastrukturen, Ressourcen und Organisationen mit sich bringen – Stichwort: Smart Citys, Gesundheitswesen, Verkehrswesen, Städteplanung oder öffentliche Sicherheit.

Doch die höhere Effizienz und die bessere Skalierbarkeit gehen Hand in Hand mit der lang erwarteten „totalen Konnektivität“ von 5G als das Bindeglied zwischen Milliarden von internetfähigen IoT-Geräten, die Angreifern reichlich Gelegenheit bieten, unverzichtbare Infrastrukturen für die Energieversorgung, das Gesundheitswesen und die Sicherheit in die Knie zu zwingen. Mit Blick auf Einzelpersonen erhalten Hacker mit 5G größere Möglichkeiten, alles von persönlichen Wearables oder Medizinprodukten bis hin zu Fahrzeugsteuerungen und Haussicherheitssystemen zu infiltrieren.

5G wird die Zahl von Kleinzellen-Antennen in städtischen Gebieten exponentiell in die Höhe schnellen lassen, sodass unzählige „harte“ Ziele entstehen. Gleichzeitig bilden das von Software bestimmte Routing und die Netzwerkverwaltung eine kapitale Schwachstelle für Cyberangreifer.

## 3. DDOS-ANGRIFFE: SCHWERWIEGENDER UND ÖFTER




DDoS-Angriffe (Distributed Denial of Service) werden weitreichender, länger und häufiger. Die Verbreitung von IoT-Geräten hat dabei entscheidenden Einfluss, und die ultraschnelle Superkonnektivität von 5G mit seiner Megabandbreite öffnet einen attraktiven Weg für größere, schnellere, schwerwiegendere DDoS-Angriffe.

Durch die DNS-Erweiterung kann ein Täter im Alleingang einen **hocheffektiven, kostengünstigen, umfangreichen DDoS-Angriff starten und dabei auf eine riesige Gruppe kompromittierter IoT-Geräte zurückgreifen, auf denen jeweils mindestens ein Bot ausgeführt wird.** Dieses Netzwerk aus Bots (Botnet) bildet die Grundlage für einen umfangreichen Angriff, der die Bandbreite des Opfers überlastet und die Betriebsabläufe lahmlegt. Botnets erstrecken sich oft über Tausende von Quell-IP-Adressen, weshalb es nahezu unmöglich ist, bestimmte Angriffe mit traditionellen Verfahren abzuwehren.

## 4. STAATLICH GEFÖRDERTE CYBERKRIMINALITÄT

Von versuchter Einflussnahme auf die Wahlen über industrielle Cyberspionage bis hin zu persönlichen Angriffen auf die Reichen und Einflussreichen … staatlich geförderte Cyberverbrechen gibt es in den verschiedensten Formen. Unternehmen gelten als unkomplizierte Alternative zu gut geschützten militärischen oder staatlichen Zielen. Daher geraten sie oft ins Visier, insbesondere wenn sie vertrauliche Daten speichern, ausgesprochen lohnend erscheinen, mit Behörden in Verbindung stehen, unverzichtbare öffentliche Dienste leisten oder IT-Ausfallzeiten nur schwer verkraften können.

**Staatlich unterstützte Cyberverbrechen nehmen Jahr für Jahr zu. Cyberkrieg eröffnet Nationen eine relativ kostengünstige, risikoarme, äußerst einträgliche Möglichkeit zur Spionage.** Heutzutage sind Russland, China und Nordkorea normalerweise die „üblichen Verdächtigen“, doch die niedrigen Einstiegshürden verleiten ärmere Länder dazu, Technologien als Waffe einzusetzen und damit zu versuchen, ihren Einfluss in der Welt zu vergrößern.

## 5. LATERALE OST-WEST-AUSBREITUNG

Maßnahmen für die Cybersicherheit konzentrieren sich in der Regel auf die Absicherung des Perimeters (den sogenannten Nord-Süd-Schutz). Doch mittlerweile **können viele Angreifer unentdeckt die Perimeterverteidigung durchbrechen und monatelang inaktiv und unentdeckt im Inneren verborgen bleiben.** Wenn der richtige Zeitpunkt kommt, wird die Malware aktiviert und lateral im gesamten Netzwerk verbreitet, von einem internen Host oder Segment zum nächsten.

Diese Taktik der Ost-West-Ausbreitung nutzt den jüngsten Trend der Vernetzung von IT-, OT- und IoT-Geräten in einer einzigen Infrastruktur. Verletzungen werden durchschnittlich erst nach 207 Tagen entdeckt. Die Angreifer innerhalb des Perimeters haben also reichlich Gelegenheit, die Netzwerke unbehelligt zu durchforsten, Schwachstellen auszuspähen und die Assets zu ermitteln, deren Diebstahl, Ausbeutung oder Schädigung am lohnenswertesten ist.

## DER PERFEKTE STURM BRAUT SICH ZUSAMMEN

IT-/OT-Konvergenz, 5G-Einführung, DDoS-Angriffe, Ost-West-Ausbreitung, staatlich gefördertes Hacken: Alle diese Sicherheitsbedrohungen nehmen ständig zu. Schon einzeln gesehen kann jede Bedrohung erheblichen Schaden anrichten. Doch **zusammengenommen könnten diese Risikofaktoren einen Angriff auslösen, dessen Ausmaß die gesamte Geschichte der Cyberkriminalität in den Schatten stellt.** Dieser perfekte Sturm könnte sich in weltumspannenden Dimensionen auf Menschen, Unternehmen und Volkswirtschaften auswirken.

**207* TAGE:**

Durchschnittliche Zeit bis zur Entdeckung eines Verstoßes*

**073* TAGE:**

Durchschnittliche Zeit bis zur Eindämmung eines Verstoßes*

**„Cost of a Data Breach Report", IBM, 2020*

# OT-/IOT-VISIBILITÄT FÜR GRÖSSERE PRODUKTIVITÄT, HÖHERE SICHERHEIT UND GERINGERE AUSFALLZEITEN

## VERSTÄNDNIS UND SICHERUNG IHRES OT-/IOT-NETZWERKS

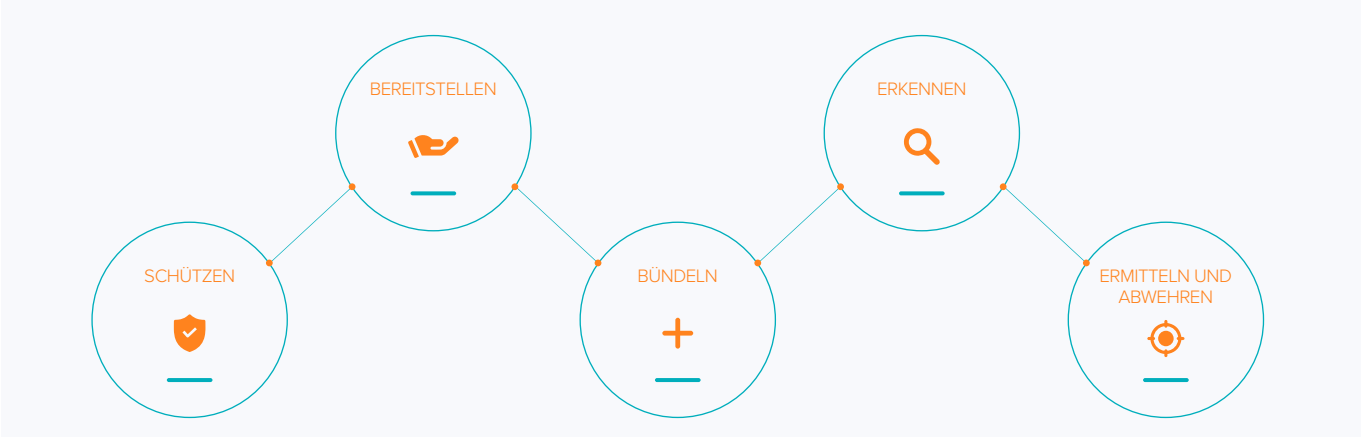
Zum besseren Risikomanagement bei der IT-/OT Integration **sind Organisationen auf die vollständige Visibilität ihres Netzwerks angewiesen: Assets, Schwachstellen und operative Bedienelemente sind nachzuverfolgen und zu überwachen,** und anormale Veränderungen müssen rasch aufgedeckt werden.

In OT-Netzwerke tummeln sich oft unzählige „Geistergeräte“ ohne Wissen der Manager, die eine immense Sicherheitsbedrohung bilden. Angesichts dieser Unwägbarkeiten **müssen IT-, OT- und IoT-Tools Ihr Netzwerk in Gemeinschaftsarbeit abriegeln.** Intelligente Funktionen für die Netzwerkfilterung und -gestaltung sorgen dafür, dass die Netzwerkpakete stets zur richtigen Zeit an die richtige Stelle transportiert werden, und schützen so Ihre wertvollen OT-Assets.

## OT-SCHUTZ FÜR UNTERNEHMEN MIT GIGAMON UND NOZOMI NETWORKS

In Gemeinschaftsarbeit bieten Gigamon und Nozomi Networks großen Unternehmen und Organisationen weltweit die Netzwerkvisualisierung in Echtzeit und die minutenaktuelle Bedrohungserkennung für ihre OT-Assets:

+ **Schützen der Industriesteuerungsnetzwerke vor** Cyberangriffen und Betriebsstörungen durch passive Analyse des Netzwerkverkehrs
+ **Bereitstellen eines umfassenden Inventars der OT-Assets** und Schwachstellenbeurteilung
+ **Bündeln von Daten für Hunderte dezentraler Betriebsanlagen** für den konsolidierten Fernzugriff auf Ihre ICS-Daten durch Guardian Appliances vor Ort
+ **Erkennen bekannter und unbekannter Bedrohungen,** optimiert durch die AI- und Machine-Learning-Technologie von Nozomi Network zur Erkennung von Anomalien
+ **Ermitteln und Abwehren** der **wichtigsten Sicherheitswarnungen** in kürzerer Zeit



## UMFASSENDE VISIBILITÄT IN IT UND OT

Sie können nicht sichern, was nicht sichtbar ist. **Cyberresilienz, Erkennung, Schutz und Mitigation steht und fällt mit der Visibilität.**

Gigamon ist zwischen OT-Geschäftsnetzwerk, Produktion, Prozessnetzwerk und Tools (z. B. Nozomi Networks) angesiedelt und sorgt für die Visibilität unabhängig vom Medium (physisch, virtuell, Cloud), einschließlich des Ost-West-Traffics.

Unterm Strich **bewirkt die Gemeinschaftslösung die umfassende, integrierte Visibilität für sämtliche IT- und OT-Assets.** Mit der Gigamon Deep Observability Pipeline ist gewährleistet, dass der relevante Datenverkehr effizient und im richtigen Format an Nozomi Networks Guardian und andere Tools transportiert wird.

Links mit geringem Volumen werden vor der Weiterleitung gebündelt, Pakete werden dedupliziert, damit kein unnötiger Mehraufwand entsteht. Und das asymmetrische Routing, mit dem Sitzungsinformationen zur Analyse durch die Nozomi Networks Sicherheitstools zusammengestellt werden, lässt sich einfacher steuern.

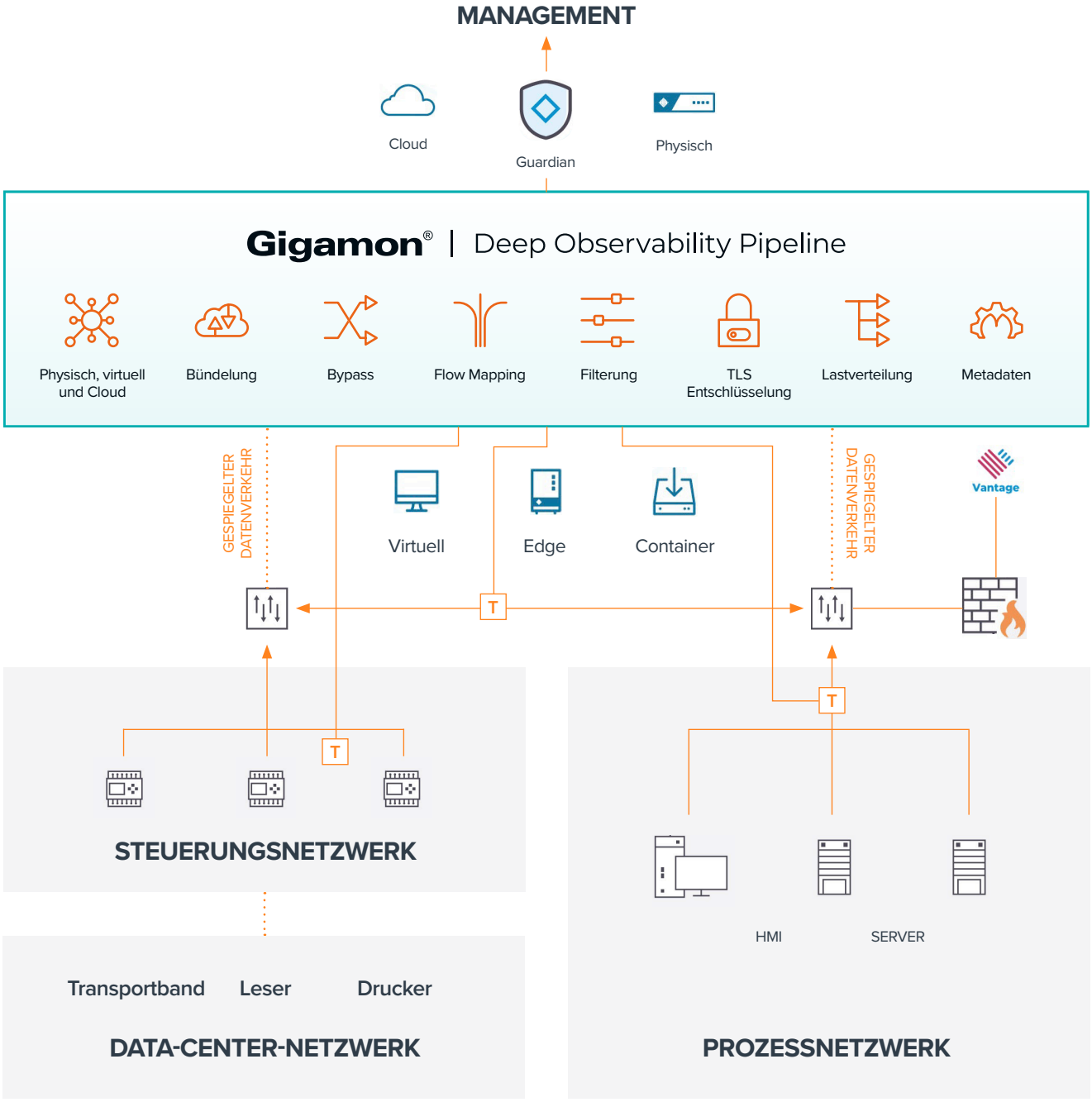
## OT-SCHUTZ MIT GIGAMON UND NOZOMI NETWORKS

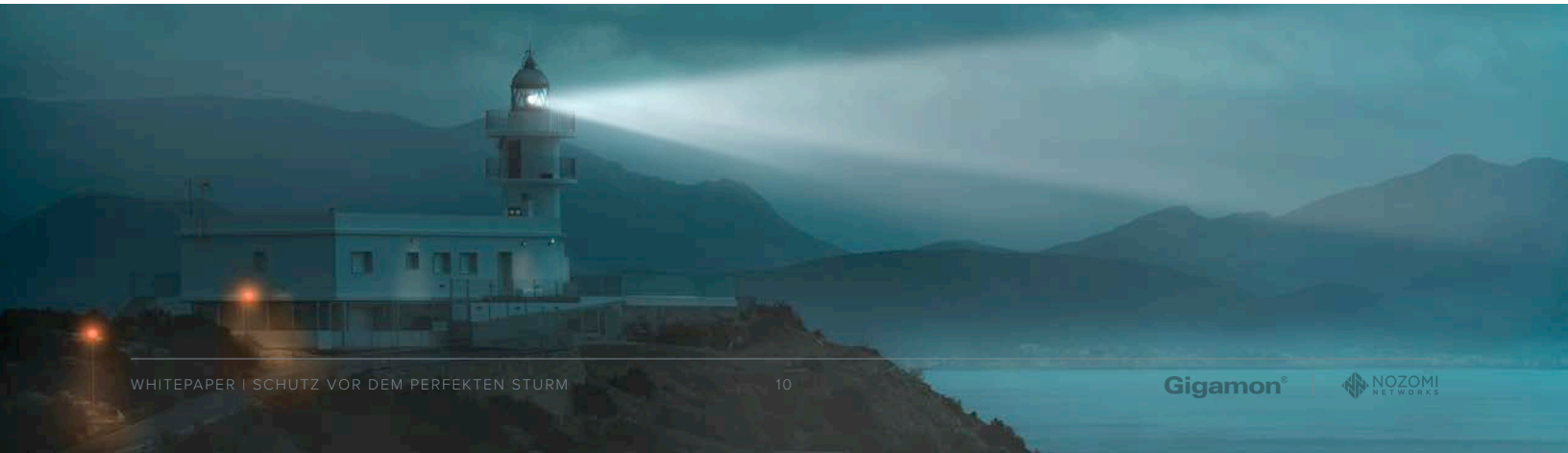
+ Die optionalen unidirektionalen TAPs von Gigamon verhindern eine Beeinträchtigung des OT Product Traffics.
+ Unabhängig von der Quelle des Gerätedatenverkehrs (u. a. WLAN-Quellen bei Ferngeräten) verhindert Gigamon die Entstehung blinder Flecken im gesamten Netzwerk. Dies reicht bis zur Visibilität von Aktionen des Identity und Access Managements, wodurch die grundlegende Sicherheit noch weiter gestärkt wird.
+ Verfügbarkeit ist für OT-Produktionsnetzwerke ein Muss. Die aktiven/passiven TAPs von Gigamon und der Inline-Bypass bieten eine Fail-Open Fähigkeit und sorgen damit für stetige Verfügbarkeit, auch wenn Wartungsarbeiten an Sicherheitstools anstehen.
+ Bei Bedarf bietet Gigamon eine zentrale TLS-/SSL-Entschlüsselung für verschlüsselten Datenverkehr an, in dem Malware vorzugsweise verborgen wird.
+ Nozomi Networks katalogisiert OT-Assets im gesamten Netzwerk, analysiert deren Schwachstellen und stellt eine Baseline für den Normalzustand auf, sodass Ausfallzeiten auf ein Minimum reduziert werden können.
+ Nozomi Networks bietet mit der einzigartigen AI- und Machine-Learning-Technologie die Anomalie-Erkennung von Betriebs- und Sicherheitsereignissen.

Zusätzlich bietet das Gigamon Deep Observability Pipeline:

+ Lastverteilung des Datenverkehrsvolumens auf mehrere Instanzen der Nozomi Networks Tools
+ Header Stripping zur Steigerung der Effizienz der Nozomi Networks Tools
+ Masking für die Datenschutz-Compliance
+ Zentrale Verwaltung zur Vereinfachung der Abläufe und zur Entlastung der Bediener und der Sicherheitsexperten

# DÉPLOIEMENT DE NOZOMI NETWORKS AVEC GIGAMON



# INFORMATIONEN ZU GIGAMON UND NOZOMI NETWORKS

Gigamon®

Gigamon® bietet eine Pipeline für Deep Observability, die sofort verwertbare Informationen auf Netzwerkebene nutzt, um die Leistungsfähigkeit von Observability-Werkzeugen zu maximieren. Diese effektive Kombination ermöglicht es IT-Organisationen, Sicherheit und Compliance umfassend zu gewährleisten, die Ursachen von Leistungsengpässen schneller zu identifizieren und den Verwaltungsaufwand zu senken, der ansonsten durch das Management hybrider und Multi-Cloud-Infrastrukturen entsteht. Das Ergebnis: Moderne Unternehmen realisieren das volle Transformationspotenzial der Cloud. Gigamon unterstützt mehr als 4.000 Kunden weltweit, darunter über 80 Prozent der Fortune-100-Unternehmen, 9 der 10 größten Mobilfunkanbieter und Hunderte von Behörden und Bildungseinrichtungen weltweit.

NOZOMI NETWORKS

Nozomi Networks schützt die unverzichtbaren Infrastruktur-, Industrie- und staatlichen Organisationen weltweit vor Cyberbedrohungen und beschleunigt so die digitale Transformation.

Unsere Lösung bietet eine herausragende Netzwerkund Asset-Visibilität, Bedrohungserkennung und tiefe operative Einblicke für OT- und IoT-Umgebungen. Die Kunden verlassen sich auf uns, wenn es darum geht, die Risiken zu minimieren und die Resilienz zu maximieren.



Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831 - 4000 | gigamon.com