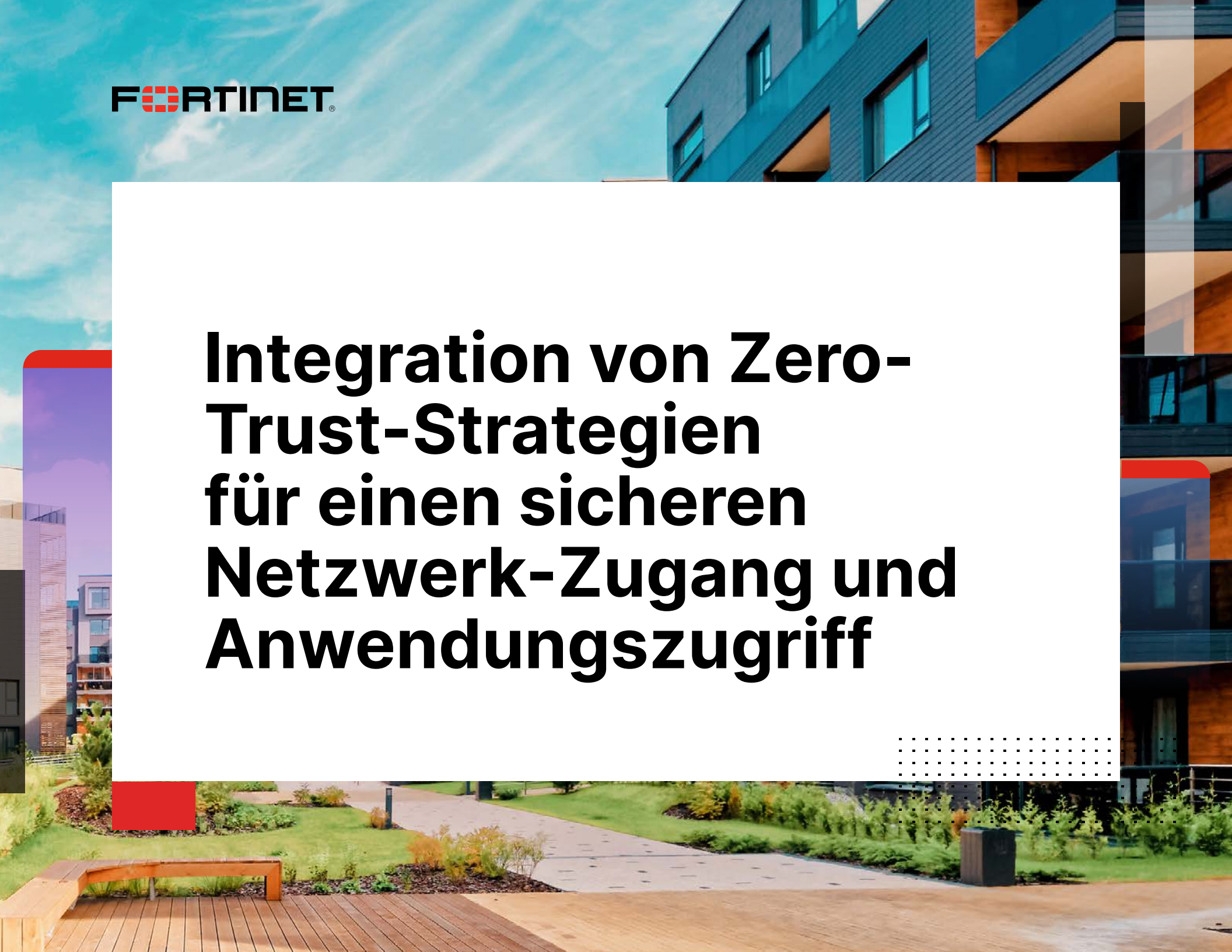

Integration von Zero-Trust-Strategien für einen sicheren Netzwerk-Zugang und Anwendungszugriff

Inhaltsverzeichnis

Zusammenfassung	3
Einleitung	4
Erfolgsfaktoren einer effektiven ZTA-Strategie	6
Fortinet ZTA Framework	8
Wesentliche Vorteile des Fortinet ZTA Framework	12
Zusammenfassung	12

Zusammenfassung

Digitale Innovationen, Cloud-Anwendungen und ortsunabhängiges Arbeiten liegen im Trend, führen jedoch zu komplizierteren, dezentralen Unternehmensnetzwerken und immer mehr Netzwerk-Rändern (auch „Edges“ genannt). Was wir einst als Netzwerk-Perimeter kannten, löst sich zunehmend auf – und je mehr Menschen und Geräte mit einem Netzwerk verbunden sind, desto weniger Schutz bietet eine klassische Perimeter-Security.

Jedes Mal, wenn einem Gerät oder Benutzer automatisch vertraut wird, sind die Daten, Anwendungen und das geistige Eigentum eines Unternehmens gefährdet. CISOs müssen daher einen grundlegenden Paradigmenwechsel vollziehen: weg vom offenen Netzwerk mit seinem inhärenten „Vertrauensvorschuss“ hin zu einem Zero-Trust-Modell. Diese „Null-Vertrauen“-Strategie muss strenge Zugangskontrollen für das gesamte verteilte Netzwerk umfassen, damit Geräte, Benutzer, Endpunkte, Clouds, Software-as-a-Service (SaaS) und die Infrastruktur geschützt sind.

Das Fortinet Zero Trust Access (ZTA) Framework verwendet eine engintegrierte Sammlung von Security-Lösungen, mit denen Unternehmen alle Benutzer und Geräte identifizieren und klassifizieren können, die auf ihr Netzwerk und ihre Anwendungen zugreifen wollen.

Einleitung

Immer mehr Unternehmen passen ihre Netzwerke für Remote-Mitarbeiter, Multi-Cloud-Architekturen und digitale Innovationen an. Die Security darf dabei nicht zu kurz kommen: Unternehmen müssen heute von jedem Standort aus einen geschützten, vertrauenswürdigen Zugang zu zahlreichen cloudbasierten Diensten und Unternehmensressourcen bereitstellen.

Herkömmliche Security-Modelle gehen davon aus, dass alles im Netzwerk eines Unternehmens als vertrauenswürdig gilt. Eine derart automatische Ausweitung des Vertrauens auf Geräte und Benutzer gefährdet jedoch das Unternehmen, wenn diese absichtlich oder unbeabsichtigt kompromittiert werden.

Die Zunahme von BYOD-Initiativen (Bring-Your-Own-Device) und IoT-Projekten (Internet der Dinge) hat zu mehr Zugangspunkten und Endgeräten geführt, wodurch der klassische Netzwerk-Perimeter nicht mehr gegeben ist. Die Folge? Angreifer, Malware und infizierte Geräte, die Security-Kontrollpunkte am Netzwerk-Rand umgehen, erlangen oft ungehinderten Zugang zum gesamten Netzwerk.

Der ZTA-Ansatz verändert das grundlegende Paradigma – weg vom „Vertrauensvorschuss“ offener Netzwerke hin zu einem grundsätzlichen Misstrauen. Diese Strategie verwendet strengere Netzwerk-Zugangskontrollen, um Benutzer und Geräte inner- und außerhalb des Netzwerks zu identifizieren, zu authentifizieren und zu überwachen.

Nur 15 % der Unternehmen haben komplett auf ein Zero-Trust-Security-Modell umgestellt, das nicht automatisch davon ausgeht, dass jeder im Netzwerk vertrauenswürdig ist.[1]

Erfolgsfaktoren einer effektiven ZTA-Strategie

Heutige Netzwerke haben große, dynamische und in einigen Fällen sogar temporäre Randbereiche (Edges). Zusätzlich erschwert wird eine permanente Risiko- und Vertrauensbewertung dadurch, dass viele Geräte häufig offline sind. Da die Vertrauenswürdigkeit von Benutzern oder Geräten inner- oder außerhalb des Netzwerks nicht überprüft werden kann, sollten Security-Verantwortliche davon ausgehen, dass jedes Gerät im Netzwerk möglicherweise infiziert ist und jeder Anwender absichtlich oder versehentlich kritische Ressourcen gefährden kann.

Eine effektive ZTA-Strategie betrifft sowohl die Netzwerk-Verbindung als auch den Anwendungszugriff. Sie basiert auf der Annahme, dass kein Benutzer oder Gerät per se vertrauenswürdig ist und prüft vor jeder Transaktion, ob ein Benutzer bzw. Gerät auf etwas zugreifen darf. Damit eine ZTA-Strategie funktioniert, müssen drei Hauptfaktoren erfüllt sein:

1. Keine unbekannten Geräte im Netzwerk

Wegen des erweiterten Netzwerk-Perimeters aufgrund der Zunahme von Anwendungen und Geräten müssen jetzt u. U. Milliarden von Randbereichen verwaltet und geschützt werden. Die dafür notwendige Transparenz über die Netzwerk-Umgebung lässt sich mit NAC-Tools (Network Access Control) erreichen.

2. Kein Netzwerk-Zugriff für unbekannte Benutzer

Um eine effektive ZTA-Strategie zu etablieren, muss bekannt sein, wer jeder Benutzer ist und welche Rolle er im Unternehmen spielt. Beim Zero-Trust-Modell wird einem Benutzer grundsätzlich nur der absolut notwendige Zugriff auf die Ressourcen gewährt, die für seine Rolle oder seine Aufgabe benötigt.

3. Wissen, wie Assets inner- und außerhalb des Netzwerks geschützt werden

Eine effektive ZTA-Strategie kann auch Geräte außerhalb des Netzwerks schützen, indem die Endpunkt-Transparenz verbessert wird. Mehr Mobilität und Remote-Arbeit führt nämlich auch dazu, dass Benutzer ihre Geräte und Unternehmensressourcen unbeabsichtigt Bedrohungen aussetzen, z. B. wenn sie mit dem gleichen Gerät auf ein unsicheres Heimnetzwerk oder einen öffentlichen Hotspot zugreifen. Melden sie sich dann wieder beim Unternehmensnetzwerk an, können sie unabsichtlich Unternehmensressourcen mit Viren und Malware infizieren.

Angriffe auf Endpunkte werden häufiger, doch die Erkennung ist schwierig.
68 % der Befragten geben an, dass die Angriffe in den letzten 12 Monaten zugenommen haben.[2]

Fortinet ZTA Framework

Das Fortinet Zero Trust Access (ZTA) Framework verwendet eine engintegrierte Sammlung von Security-Lösungen, mit denen Unternehmen alle Benutzer und Geräte identifizieren und klassifizieren können, die auf ihr Netzwerk und ihre Anwendungen zugreifen wollen. Damit lässt sich z. B. beurteilen, wie gut interne Sicherheitsrichtlinien eingehalten werden. Auch können Benutzern und Geräten automatisch Kontrollzonen zugewiesen und diese sowohl im Netzwerk als auch außerhalb des Netzwerks kontinuierlich überwacht werden.

1. Zugangskontrolle für Endpunkte

Endpunkte werden häufig zuerst infiziert oder angegriffen. Das bestätigt auch eine aktuelle Studie. Demnach gehen 30 % der Verstöße[3] auf Malware zurück, die auf Endgeräten installiert wurde. Fortinet verbessert die Endpunkt-Security durch eine integrierte Transparenz, Kontrolle und proaktive Bedrohungsabwehr. Risiken für Endpunkte werden erkannt, überwacht und bewertet. Diese Fähigkeit trägt dazu bei, die Regelkonformität von Endpunkten zu gewährleisten sowie Risiken und Anfälligkeiten zu verringern. FortiClient – die Fortinet-Lösung für den Endpunkt-Zugang – bietet u. a.:

- Unterstützung sicherer, verschlüsselter Verbindungen über unsichere Netzwerke mit Split-Tunneling und SASE-Diensten (Secure Access Service Edge)
- Bereitstellung kontinuierlicher Telemetriedaten zur Endpunkt-Sicherheit, einschließlich Betriebssystem und Anwendungen des Geräts, bekannter Schwachstellen, Patches und Sicherheitsstatus

2. Identitäts- und Zugangsverwaltung

Heutige Enterprise-Identity-Umgebungen bestehen aus unterschiedlichsten Systemen, die Anmeldedaten von Benutzern speichern – von Netzwerk-Geräten, Servern und Verzeichnisdiensten bis hin zu Cloud-Anwendungen. Durch diese Fülle an Systemen ist das Verwalten von Benutzeridentitäten mit enormem Verwaltungsaufwand verbunden. Dazu kommt, dass viele der gravierendsten Sicherheitsverstöße erst möglich werden, weil Benutzer zu weit gefasste Zugriffsrechte oder – noch schlimmer – statische Passwörter verwenden, die auch Hacker kennen. Benutzer, Administratoren und Anwendungsentwickler haben damit gleichermaßen zu kämpfen. Ein sicheres, effektives Management der Identitätsauthentifizierung und -autorisierung für alle Systeme und Anwendungen ist notwendig, um Sicherheitsverletzungen zu minimieren. Fortinet-Lösungen für die Identitäts- und Zugangsverwaltung bieten genau das:

- Feststellen der Identität bei der Anmeldung durch Multi-Faktor-Authentifizierung (MFA) und Zertifikate, die sich mit einer kontinuierlichen kontextbezogenen Authentifizierung erweitern lassen
- rollenbasierte Informationen aus der Authentifizierungsquelle für privilegierte Zugriffe
- rollenbasierte Richtlinien für den geringsten Zugriff und deren Durchsetzung
- zusätzliche Sicherheit mit einmaliger Anmeldung (SSO, Single Sign-On) für mehr Compliance und höhere Benutzerakzeptanz

3. Netzwerk-Zugangskontrolle

Die Netzwerk-Zugangskontrolle ist eine ZTA-Lösung (Zero Trust Access), die Unternehmen vor der immer größer werdenden Angriffsfläche schützt. Sie bietet Transparenz über die Netzwerk-Umgebung zur Durchsetzung und dynamischen Steuerung von Richtlinien. Unabhängig davon, ob Geräte inner- oder außerhalb des Netzwerks eine Verbindung herstellen, kann FortiNAC automatisch auf gefährdete Geräte oder anomale Aktivitäten reagieren.
Mit FortiNAC können Unternehmen:

- alle Geräte identifizieren, profilieren und auf Schwachstellen überprüfen
- eine kontinuierliche Netzwerk-Kontrolle einrichten und durchsetzen
- Richtlinien einrichten und durchsetzen, die den Netzwerk-Zugang eines Geräts auf das absolut Notwendige beschränken
- automatisch und abgestimmt im gesamten Netzwerk Bedrohungen abwehren (Orchestrierung)

4. Kontrolle über den Anwendungszugriff

Beim Zero-Trust-Modell sollte der Anwendungszugriff pro Sitzung kontrolliert werden. Bei jedem Benutzer und jedem Gerät sollte überprüft werden, ob die Verbindung per Fernzugriff oder aus einem firmeneigenen Netzwerk aufgebaut wird. Der Anwendungszugriff richtet sich dabei nach der individuellen Rolle, damit nur für den Benutzer relevante Anwendungen verfügbar sind. Mit ZTA-Mechanismen lassen sich Anwendungen auf On-Premises-Servern, in Private Clouds oder in Public Clouds kontrollieren. Fortinet ZTA-Lösungen bieten verschiedene Möglichkeiten für die Anwendungszugriffskontrolle, z. B. mit SASE-Diensten oder mit On-Premises-Firewalls für Appliances oder virtuelle Maschinen (VMs). Diese Lösungen:

- überprüfen Benutzer und Geräte pro Anwendungssitzung
- steuern den Benutzerzugriff auf Anwendungen basierend auf Richtlinien
- setzen Richtlinien für den Anwendungszugriff unabhängig davon durch, wo sich der Benutzer befindet
- erstellen eine sichere, automatische Verbindung zwischen dem Benutzer und dem ZTNA-Proxy-Punkt
- arbeiten mit Firewalls, VM-Firewalls und SASE-Diensten zusammen

Die geschilderten Angriffsformen machen deutlich, wie wichtig bessere Security-Ansätze – insbesondere Zero-Trust-Modelle – sind. Nur so können Unternehmen Netzwerke vor Bedrohungen schützen, die Mitarbeiter aus unsicheren Heimnetzwerken einschleppen.[4]

Wesentliche Vorteile des Fortinet ZTA Framework

Für eine wirksame Sicherheit müssen Unternehmen ihr Security-Konzept grundlegend umstellen: weg vom Netzwerk-Perimeter als „Verteidigungsbollwerk“ hin zum Schutz von Daten, die über unzählige Netzwerk-Ränder, Benutzer, Systeme, Geräte und kritische Anwendungen verteilt sind. Die Fortinet-Plattform bietet die dafür notwendige, umfassende Transparenz und Sicherheit für Geräte, Benutzer, Endpunkte, Clouds, SaaS und Infrastruktur. Die wesentlichen Vorteile des Fortinet ZTA Framework auf einen Blick:

- vollständige, kontinuierliche Kontrolle darüber, wer auf Anwendungen zugreift – unabhängig davon, wo sich diese Anwendungen oder Benutzer befinden
- vollständige, kontinuierliche Kontrolle darüber, wer im Netzwerk ist
- vollständige, kontinuierliche Kontrolle darüber, was sich im Netzwerk befindet
- integrierte ZTA-Lösung für die Fortinet Security Fabric, die alles schützt: LAN, WAN und Remote-Tunnel
- integrierte Komplettlösung von einem einzigen Anbieter

Fazit

Mit jahrzehntelanger Erfahrung in der Unterstützung von Unternehmen bei der Aufrechterhaltung einer umfassenden Security für schnell wachsende Netzwerke bietet Fortinet ein hochwirksames ZTA-Framework, das Transparenz und Kontrolle in vier Kernbereichen gewährleistet: Anwendungszugriff, Benutzer im Netzwerk, Geräte im Netzwerk sowie Offline-Aktivitäten dieser Benutzer und Geräte.

[1] „2019 Zero Trust Adoption Report“. Cybersecurity Insiders, November 2019.

[2] Larry Ponemon: „The state of endpoint security risk: it’s skyrocketing“. Ponemon Sullivan Privacy Report, Mai 2020.

[3] „2020 Data Breach Investigations Report“. Verizon, 2020.

[4] „Global Threat Landscape Report“. FortiGuard Labs, August 2020.

www.fortinet.com/de

E-Book-Integration-von-Zero-Trust-Strategien_DE

885304-A-0-DE