FORTINET

Sicheres SD-WAN: Der SD-WAN-Leitfaden für Netzwerk-Verantwortliche

Sicherheitsorientierte Netzwerke für einen leistungsstarken WAN-Edge

Inhaltsverzeichnis

Zusammenfassung

Digitale Innovationen wie das Cloud-on-Ramping von Software-as-a-Service-Anwendungen (SaaS) und Infrastructure-as-a-Service (IaaS) sind besonders für dezentrale Unternehmen der Schlüssel zu mehr Umsatz und Effizienz. Allerdings steigt durch diese Technologien der Datenverkehr auf eine Weise, dass es bei WAN-Infrastrukturen (Wide Area Network) mit MPLS-Verbindungen (Multiprotocol Label Switching) zu Netzwerk-Engpässen kommt und die Kosten explodieren. Viele Netzwerk-Verantwortliche möchten daher veraltete WAN-Infrastrukturen durch ein softwaredefiniertes Wide Area Networking (SD-WAN) ersetzen. Zehntausende Kunden haben sich bereits für das Fortinet Secure SD-WAN entschieden, das Netzwerk- und Security-Funktionen in einer einheitlichen Lösung vereint, die die Anwendungsleistung optimiert, das Management konsolidiert und einen intelligenten Bedrohungsschutz bietet.

Einleitung

Digitale Innovationen erfordern eine höhere Bandbreite, um eine optimale Benutzererfahrung zu gewährleisten – was die Anforderungen an das SD-WAN und verändert und zugleich offenbart, welche Funktionen bei vielen Lösungen fehlen. Probleme wie eine begrenzte Skalierbarkeit, keine Automatisierung zur Vereinfachung von Betriebsabläufen oder unzureichende Cloud-On-Ramp- und SaaS-Integrationen können die Nutzererfahrung beeinträchtigen und somit den Wert einer SD-WAN-Implementierung schmälern. Wichtig ist daher, dass SD-WAN-Lösungen robuste Netzwerk- und Konnektivitäts-Tools bieten, die mit der Dynamik von digitalen Innovationen mithalten können und sich problemlos anpassen lassen – insbesondere, wenn Unternehmen in kürzester Zeit die Cloud stärker nutzen, regionale Bereitstellungen weltweit vereinheitlichen oder mehr regionale Niederlassungen gründen wollen.

Nur Fortinet bietet eine Secure SD-WAN-Lösung mit speziellen SD-WAN-ASIC-Chips, die eine bessere Anwendungserfahrung und Kosteneffizienz sowie eine höhere Leistung ermöglichen.

Welcher Weg zum SD-WAN?

Mit einem SD-WAN lassen sich verfügbare WAN-Dienste effektiver und wirtschaftlicher nutzen. Mitarbeiter in dezentralen Unternehmen erhalten damit mehr Flexibilität bei der persönlichen Kundensprache, der Optimierung von Geschäftsprozessen und innovativen Neuerungen. WAN-Innovationen mit zusätzlichen Verbindungen (z. B. über das Mobilfunknetz) eröffnen Vorteile wie Redundanz, Lastausgleich und Optimierung des Datenverkehrs von Anwendungen. Zudem senkt ein softwaredefiniertes WAN die Kosten des WAN-Managements – einer der Hauptgründe, warum SD-WAN-Lösungen auf absehbare Zeit ein robuster Wachstumsmarkt bleiben dürften.

Zur Befriedigung dieser Nachfrage kamen in den letzten Jahren viele SD-WAN-Lösungen auf den Markt, aber nicht alle bieten die gleichen Vorteile.

Welches SD-WAN für ein Unternehmen optimal ist, hängt laut SD-WAN-Experten und Branchenanalysten von den Anforderungen an die Anwendungsleistung, ein schnelleres Cloud-On-Ramp für mehrere Clouds und der angestrebten Vereinfachung der Betriebsabläufe mit einem zentralen Management ab, um die Komplexität zu reduzieren. Es wird auch generell empfohlen, dass Unternehmen das SD-WAN mit einer NGFW-Lösung kombinieren, um Sicherheitsprobleme zu vermeiden, die durch den direkten Breitband-Internetzugang von Niederlassungen entstehen können. Um diese Geschäftsanforderungen zu erfüllen, benötigen Unternehmen ein umfassendes SD-WAN-Angebot wie das Fortinet Secure SD-WAN – die einzige Lösung mit integrierten Security- und Performance-Funktionen, die sich flexibel in Unternehmen jeder Größe bereitstellen und skalieren lässt.

Erstklassig und modern: Die SD-WAN-Lösung von Fortinet

Das Fortinet Secure SD-WAN ersetzt separate WAN-Router, WAN-Optimierung und Security-Komponenten wie Firewalls und Secure Web Gateways (SWGs) durch eine einzige Fortinet NGFW. Diese bietet eine branchenweit unübertroffene Leistung mit Funktionen wie Anwendungserkennung, automatisierter Pfadintelligenz und WAN-Overlay-Unterstützung für VPNs. Mit dem Fortinet Secure SD-WAN erhalten Unternehmen sicherheitsorientierte Netzwerke für Niederlassungen mit herausragender Leistung dank der schnellen Anwendungsidentifikation und dem automatisierten, intelligenten Routing.

Anwendungserkennung für verbesserte Service Levels

Das Fortinet Secure SD-WAN arbeitet mit dem neuen SOC4-Security-Chip (ASIC), der eine schnellere Anwendungssteuerung und eine konkurrenzlose Anwendungserkennung bietet – einschließlich tiefgehender SSL/TLS-Prüfung (Deep Secure Sockets Layer/Transport Layer Security) mit geringstmöglichem Leistungsabfall. Zu den Funktionen zur Verschlüsselungsprüfung gehört auch die Inspektion von Paketen, damit die SD-WAN-Lösung den Datenverkehr korrekt weiterleitet.

Technisch gesehen sorgt ein SD-WAN dafür, dass für Anwendungen zu jedem Zeitpunkt die effizienteste WAN-Verbindung gewählt wird. Um eine optimale Anwendungsleistung zu gewährleisten, müssen SD-WAN-Lösungen in der Lage sein, ein breites Anwendungsspektrum zu identifizieren und Routing-Richtlinien auf einer sehr granularen Ebene anzuwenden. Ohne diese Funktionen können SaaS-, Video- und Sprach-Anwendungen die Produktivität der Endanwender ausbremsen und beeinträchtigen.

Damit es erst gar nicht zu solchen Problemen kommt, verwendet das Fortinet Secure SD-WAN eine Application-Control-Datenbank mit den Signaturen von mehr als 5000 Anwendungen (mit regelmäßigen Updates von den FortiGuard Labs Threat Intelligence Services). Kurz: Das Fortinet Secure SD-WAN identifiziert und klassifiziert Anwendungen – auch verschlüsselten Datenverkehr von Cloud-Anwendungen – vom ersten Paket an.

Das Fortinet Secure SD-WAN bietet:

- **optimale Anwendungserfahrung mit präziser Erkennung**
- **effektive Geschäftsrichtlinien pro Anwendungssignatur**
- **ständige Aktualisierungen der Anwendungsdatenbank anhand neuer Research-Daten der FortiGuard Labs**

Das Fortinet Secure SD-WAN erkennt über 5000 Anwendungen automatisch und leitet sie über die optimale Verbindung weiter.

Fortinet NGFWs können so eingestellt werden, dass sie die Kritikalität von Geschäftsanwendungen erkennen. Geschäftskritische Anwendungen (z. B. Office 365, Salesforce, SAP), allgemeine Produktivitätsanwendungen (wie Dropbox) und Social Media (z. B. Twitter, Instagram) können unterschiedliche Routing-Prioritäten erhalten. Auf tieferer Ebene lassen sich einzigartige Richtlinien für Sub-Anwendungen einrichten (z. B. Word oder OneNote in Office 365). Diese detaillierte, umfassende Transparenz auf Anwendungsebene über Verkehrsmuster und Auslastung ermöglicht eine bessere Zuordnung der WAN-Ressourcen je nach den Geschäftsanforderungen.

Mühelose WAN-Effizienz

Das Fortinet Secure SD-WAN vereinfacht die Modernisierung älterer WAN-Edge-Infrastrukturen erheblich und bietet eine stärkere Anwendungsleistung, bessere Benutzererfahrung und höhere Sicherheit. Sobald die WAN-Richtlinien auf der Grundlage von Anwendungskritikalität, Leistungsanforderungen, Sicherheitsrichtlinien und anderen Kriterien festgelegt wurden, übernimmt die Fortinet Secure SD-WAN-Lösung die restliche Arbeit. Dank spezieller Security-Chips (SOC4 ASIC) bieten Fortinet NGFWs eine 10-mal schnellere Sicherheitsleistung als vergleichbare Firewalls.[1]

Im Bereich der WAN-Effizienz stellt Fortinet Secure SD-WAN alle wichtigen Funktionen bereit:

Automatisierte Pfadintelligenz: Die Anwendungserkennung ermöglicht ein priorisiertes Anwendungs-Routing über die gesamte Netzwerk-Bandbreite, abgestimmt auf die jeweilige Anwendung und den Benutzer. Mit dem neuen SOC4 ASIC verfügt das Fortinet Secure SD-WAN über die schnellste Anwendungssteuerung der Branche. Service-Vereinbarungen (SLAs) für das SD-WAN lassen sich leicht definieren, indem man dynamisch die beste WAN-Verbindung für die spezifischen Geschäftsumstände auswählt. Für Anwendungen mit geringer bis mittlerer Priorität können Unternehmen die Qualitätskriterien vorgeben, und die FortiGate wählt dann eine passende Verbindung aus. Für Anwendungen mit hoher Priorität und geschäftskritische Anwendungen können strenge SLAs definiert werden, die kombinierte Faktoren wie Jitter, Paketverlust und Latenzzeiten berücksichtigen.

Automatisches Failover: Die Multi-Path-Technologie kann automatisch auf die beste verfügbare Verbindung umschalten, wenn sich der primäre WAN-Pfad verschlechtert. Diese Automatisierung ist in die Fortinet NGFW integriert, wodurch sich die Komplexität für den Endbenutzer reduziert und gleichzeitig seine Anwendungserfahrung und Produktivität verbessert.

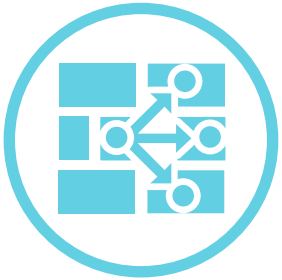
WAN-Pfadkorrektur: Die WAN-Pfadkorrektur nutzt die Vorwärtsfehlerkorrektur (Forward Error Correction, FEC), um widrige WAN-Bedingungen, wie schlechte Verbindungen oder Leitungsrauschen zu kompensieren. Dies erhöht die Datenzuverlässigkeit und bietet eine bessere Benutzererfahrung für Anwendungen wie Sprach- oder Videodienste. FEC fügt dem ausgehenden Datenverkehr Fehlerkorrekturdaten hinzu, damit die Empfängerseite Paketverluste und andere Fehler während der Übertragung beheben kann. Das alles verbessert die Qualität von Echtzeitanwendungen.

Priorität von Anwendungen: Mit dem Fortinet Secure SD-WAN können Sie anwendungsspezifische Geschäftsrichtlinien vorgeben. Für kritische Anwendungen lässt sich mit genauen QoS-Prioritäten (Dienstgüte) die optimale Bandbreite reservieren und somit die bestmögliche Leistung und Nutzererfahrung garantieren, während unwichtigere Anwendungen nur begrenzten Durchsatz erhalten.

Aggregation der Tunnelbandbreite: Für Anwendungen, die eine größere Bandbreite erfordern, bietet das Fortinet Secure SD-WAN eine Lastverteilung und Übertragung pro Paket. Hierzu werden zwei Overlay-Tunnel zur Maximierung der Netzwerk-Kapazität kombiniert.

Einfacheres Management und branchenweit geringste Gesamtbetriebskosten

Netzwerk-Verantwortliche haben oft Probleme bei der Bereitstellung von SD-WAN-Edge-Geräten in zahlreichen Remote-Standorten und Niederlassungen. Der Einsatz von IT-Experten vor Ort ist teuer und mit personell begrenzten Teams schwer realisierbar. Andererseits ist der Versand von komplett vorkonfigurierten Geräten nicht sicher. Außerdem müssen Mitarbeiter nach der Implementierung der Edge-Geräte sowohl die WAN-Optimierung als auch die Security-Funktionen selbst verwalten können und müssen sich dafür oft in zwei verschiedenen Benutzeroberflächen zurechtfinden. Das Fortinet Secure SD-WAN löst solche Implementierungs- und Management-Probleme, wodurch sich die Gesamtbetriebskosten (Total Cost of Ownership, TCO) erheblich verringern.

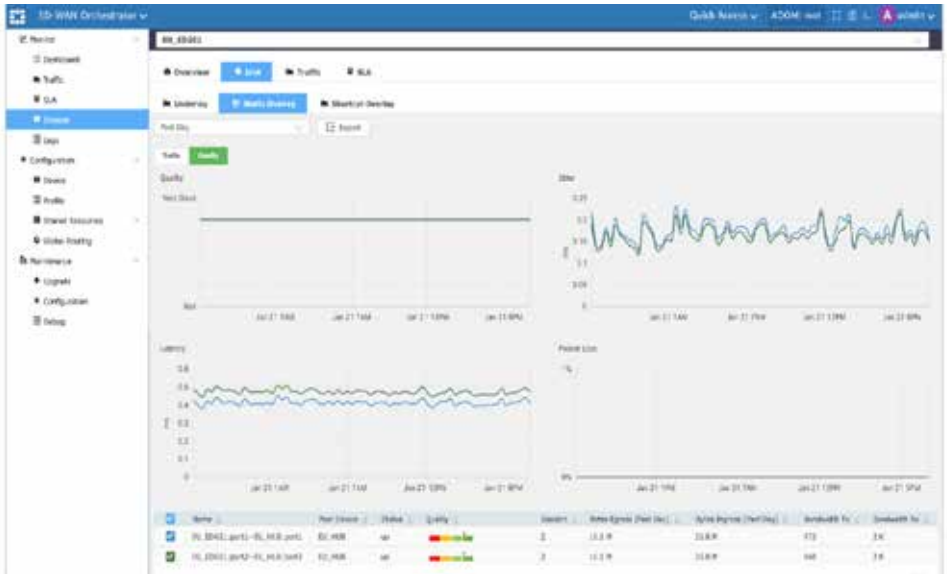


Das Fabric Management Center ermöglicht effektive Network Operations und ein agiles Netzwerk-Management für das gesamte SD-WAN und alle Sicherheitsprojekte.[2]

Zero-Touch-Bereitstellung: Dank der vereinfachten Implementierungsfunktionen des Fortinet Secure SD-WAN können Unternehmen einfach Fortinet NGFW-Appliances an alle Remote-Standorte liefern. Beim Anschließen verbindet sich die FortiGate automatisch mit dem FortiDeploy-Dienst in der FortiCloud. FortiDeploy authentifiziert das Remote-Gerät innerhalb von Sekunden und vernetzt es dann mit einem zentralen FortiManager-System.

Management über eine zentrale Konsole: Das Fortinet Fabric Management Center schafft zentrale Transparenz über alle unternehmensweit implementierten Fortinet NGFWs, die das Secure SD-WAN unterstützen. Zudem lassen sich Richtlinien mit dem Fortinet Secure SD-WAN-Orchestrator mit nur wenigen Klicks in einfachen Schritten erheblich leichter implementieren und aktualisieren.

Der SD-WAN-Orchestrator baut automatisch übergelagerte Verbindungen (Full Mesh Overlay Links) auf und verwaltet diese sicheren Verbindungen zwischen Standorten.
Mit geführten Workflows, automatisiertem Overlay-Start und vereinfachten Geschäftsrichtlinien verkürzt der SD-WAN-Orchestrator die Infrastrukturbereitstellung und -änderung durch IT-Teams von Monaten auf Minuten.



Das Fabric Management Center bietet erweiterte Telemetrie-Daten für mehr Transparenz über Anwendungen und die Netzwerk-Leistung, um Probleme schneller zu lösen und IT-Support-Anfragen zu reduzieren. SD-WAN-Berichte liefern bei Bedarf weitere Informationen über die Bedrohungslage, die Vertrauensstufe und den Zugriff auf Ressourcen, die für Compliance-Zwecke vorgeschrieben sind.

SD-WAN-Berichte und -Analysen: Dank verbesserter Analysen der Verfügbarkeit von WAN-Verbindungen, der Erfüllung von Service-Vereinbarungen (SLA), des Anwendungsverkehrs zur Laufzeit sowie rückblickender Statistiken kann das Infrastruktur-Team Fehler schnell eingrenzen und Netzwerk-Probleme beheben.

Dazu gehören Berichte zur Bandbreiten-Überwachung und Datensätze zum SD-WAN, eine SLA-Protokollierung für Service-Level-Vereinbarungen sowie eine rückblickende Vorgangsüberwachung (History Monitoring) anhand von Datensätzen, Diagrammen und Reports. Außerdem bietet die Fortinet-Lösung anpassbare SLA-Warnungen, Berichte zur Anwendungsnutzung, Dashboards, adaptive Response Handler für SD-WAN-Ereignisse, eine Ereignis-Protokollierung (Event Logging) sowie die Archivierung von Vorfällen bei Anwendungen und Schnittstellen im Zusammenhang mit SLAs.

Zugang zu Distributed Clouds mit geringer Latenz:
Mit dem Fortinet Secure SD-WAN erhalten Unternehmen einen schnellen Cloud-Zugang, was die Zusammenarbeit vereinfacht. Benutzer können direkt auf mehrere Clouds zugreifen und die Teamfunktionen von Anwendungen wie Office 365 nutzen. Die integrierte Security fügt eine weitere Sicherheitsstufe für den Anwendungszugriff hinzu, während Verbindungen über das öffentlich zugängliche Internet mit geringen Latenzzeiten laufen. Unternehmen erhalten damit eine vertrauenswürdige, zuverlässige Erweiterung der WAN-Infrastruktur.

Dies ist besonders wichtig, wenn Remote-Mitarbeiter und deren Haushaltsmitglieder funktionsreiche Cloud-Anwendungen für Sprach- und Videokonferenzen verwenden. Solche cloudgehosteten Applikationen mit ihren modernen Sprach- und Videofunktionen benötigen eine höhere Bandbreitenverfügbarkeit. Oft ist dieser Datenverkehr auch verschlüsselt, was leistungsstarke Sicherheitsfunktionen erfordert, um u. a. auch diesen Traffic überprüfen zu können. In all diesen Bereichen bietet das Fortinet Secure SD-WAN entscheidende Vorteile: Die Fortinet-Lösung erkennt Sub-Anwendungen und kann verschlüsselte Anwendungen mit SSL-Inspektionsfunktionen in Leitungsgeschwindigkeit bereitstellen. Dadurch laufen kritische Anwendungen immer über die leistungsstärkste WAN-Verbindung, womit eine optimale Leistung gewährleistet ist.

Für Benutzer, die eine sichere Kommunikation über öffentliche Internetverbindungen benötigen, können mit nur einem Klicks VPNs eingerichtet werden. All dies spart Zeit, vereinfacht die SD-WAN-Administration (On-Premises oder über die Cloud) und entlastet personell begrenzte Netzwerk-Teams. Fortinet bietet eine der wenigen Lösungen, mit der man das SD-WAN-Netzwerk, die Security und den Access Layer von derselben Management-Konsole aus verwalten kann.

Gesamtbetriebskosten (TCO): Das Fortinet Secure SD-WAN bietet die branchenweit niedrigsten Gesamtbetriebskosten pro Mbit/s – und eine Zero-Touch-Bereitstellung von neuen Niederlassungen in unter Minuten.[3] Durch den Umstieg auf das öffentliche Breitband lassen sich teure MPLS-Verbindungen durch kostengünstigere Optionen ersetzen. Mit der transportunabhängigen Lösung von Fortinet können Unternehmen die gesamte verfügbare Bandbreite nutzen, indem sie Verbindungen im Aktiv/Aktiv-Modus laufen lassen.

Fortinet ist der Marktführer bei Secure SD-WAN-Innovationen mit Lösungen, die sich vom Homeoffice bis zu Niederlassungen und Distributed Clouds skalieren lassen.[4]

Sicherheitsorientierte Netzwerke

Fortinet bietet ein erstklassiges, zertifiziertes SD-WAN, das sowohl leistungsstark als auch geschützt ist. Fortinet NGFWs mit dem SOC4 ASIC liefern die branchenweit schnellste SD-WAN-Security-Leistung. Im „Software-Defined Wide Area Networking Test Report" der NSS Labs von 2019 erhielt Fortinet das zweite Mal in Folge die Bewertung „Empfohlen".[5]

Beispielsweise verfügt das Fortinet Secure SD-WAN über einen robusten SD-WAN-Bedrohungsschutz, einschließlich Layer-3- bis Layer-7-Sicherheitskontrollen, die in anderen kombinierten Lösungen mit SD-WAN und Firewall oft fehlen. Die wesentlichen Vorteile auf einen Blick:

- umfassender Schutz vor Bedrohungen, einschließlich Firewall, Antivirus, Intrusion Prevention System (IPS) und Application Control
- Überprüfung von Deep-Packet-Verschlüsselungen für SSL/TLS (Secure Sockets Layer/Transport Layer Security) mit hohem Durchsatz und minimalen Leistungseinbußen, damit der Komplettschutz vor Bedrohungen nicht zu Lasten der Bandbreite geht
- Web-Filter zur Durchsetzung einer sicheren Internet-Nutzung, ohne dass ein separates sicheres Web-Gateway (SWG) notwendig ist
- hohe WAN-Leistung für Cloud-Anwendungen mit erstklassiger VPN-Overlay-Leistung für eine überlegene Benutzererfahrung und geringe Latenz[6]

Secure SD-WAN-fähige Fortinet NGFWs überwachen auch Firewall-Regeln und Richtlinien und nutzen Best Practices, um das allgemeine Sicherheitsprofil des Unternehmens zu verbessern. Dies trägt dazu bei, die Compliance mit Security-Standards sowie Datenschutzgesetzen und Branchenvorschriften zu vereinfachen. Automatisierte Audit- und Berichts-Workflows sparen Mitarbeitern viele Stunden Arbeit und reduzieren das Risiko von Pflichtverletzungen und Fehlern.

Erfolgreiche SD-Branch-Transformation

Viele Niederlassungen wollen WAN- und LAN-Geräte gleichzeitig durch eine besser integrierte Lösung ersetzen, die sich auch einfacher verwalten lässt. Aus gutem Grund: Getrennte WAN- und LAN-Infrastrukturen verschlimmern die Komplexität (mehr Geräte-Implementierungen und Updates mit verschiedenen Management-Konsolen), verringern die Transparenz und Kontrolle über Betriebsabläufe – und erhöhen zugleich das Risiko von Sicherheitslücken, die Hacker ausnutzen können. Um solche Probleme zu lösen und eine erfolgreiche SD-Branch-Transformation zu unterstützen, bietet das Fortinet Secure SD-WAN eine schnellere Security-Erweiterung bis zum Access Layer.

In einem volatilen SD-WAN-Markt ist Fortinet die sichere Wahl

Da cloudbasierte Anwendungen und Tools wie Sprache und Video für dezentrale Organisationsstrukturen immer wichtiger werden, können Unternehmen mit dem Fortinet Secure SD-WAN von den Vorteilen digitaler Innovationen profitieren, ohne die Anwendungsleistung zu verlangsamen, die Produktivität der Endanwender zu beeinträchtigen oder Daten zu gefährden.

Das Fortinet Secure SD-WAN ist skalierbar und hilft Unternehmen dabei, mehr Remote-Standorte, mehr bandbreiten-empfindlichere geschäftskritische Anwendungen, mehr Cloud-Services – und alles, was Niederlassungs-Netzwerke benötigen – zuverlässig zu unterstützen.

Das Fortinet Secure SD-WAN wird weltweit in den verschiedensten Branchen eingesetzt – von der Finanzwirtschaft über den Einzelhandel bis hin zur Fertigung und im Kundenservice. Unabhängig davon, ob Ihr Unternehmen einige Hundert mobile Endgeräte oder zehntausende Niederlassungen unterstützen muss: Mit Fortinet Secure SD-WAN können Sie Ihren optimalen Mix aus erstklassiger Security und SD-WAN-Funktionalität individuell realisieren.

[1] „Fortinet wird im SD-WAN-Gruppentest der NSS Labs das zweite Mal als empfehlenswert bewertet“. Fortinet, 19. Juni 2019.

[2] „Fortinet ist der Marktführer bei Secure SD-WAN-Innovationen“. Fortinet, Mai 2020.

[3] „SD-WAN-Infrastrukturmarkt soll 2023 5,25 Milliarden US-Dollar erreichen“. Juli 2019.

[4] „Erfahren Sie mehr über einen Fortinet-Kunden aus den Fortune 500, der 65 % Kostensenkungen realisiert hat.“ Fortinet, 24. April 2020.

[5] Ebd.

FORTINET®

www.fortinet.com/de

16. Mai 2022, 10:45 Uhr

eb-network-leaders-guide-to-secure-sd-wan_DE

372656-C-0-DE