SOLUTION BRIEF

Sicherer, skalierbarer Remote Access für Mitarbeiter

Zusammenfassung

Jedes Unternehmen sollte gut auf Notfallsituationen wie Epidemien, Naturkatastrophen oder Stromausfälle vorbereitet sein und einen Plan implementieren, der den kontinuierlichen Geschäftsbetrieb selbst unter widrigsten Umständen sicherstellt.

Ein solcher Plan muss auch Szenarien abdecken, bei denen der normale Betrieb im Firmensitz unmöglich wird und größtenteils oder vollständig auf die Arbeit im Homeoffice umgestellt werden muss. Denn die Fähigkeit, auswärts arbeitende Mitarbeiter zu unterstützen, ist zur Gewährleistung eines kontinuierlichen Geschäftsbetriebs und der Security entscheidend. Lösungen von Fortinet berücksichtigen bereits die Umstellung auf Telearbeit. So bieten z. B. FortiGate Next-Generation-Firewalls (NGFWs) eine integrierte Unterstützung für virtuelle private IPsec-Netzwerke (VPNs), um auswärts arbeitende Mitarbeiter sicher mit dem Unternehmen zu verbinden. Gemeinsam mit dem Endpunkt-Schutz von FortiClient und der Multi-Faktor-Authentifizierung (MFA) mit FortiAuthenticator können Unternehmen so Homeoffices, mobile Mitarbeiter und Remote-Arbeitsplätze sicher unterstützen und einen kontinuierlichen Geschäftsbetrieb gewährleisten.

Eine effektive Security für auswärts arbeitende Mitarbeiter ist ein zentraler Punkt in jedem Business-Continuity- und Disaster-Recovery-Plan. Bei einem Stromausfall oder ähnlichen Ereignissen lässt sich womöglich der normale Betrieb vor Ort nicht mehr aufrechterhalten. Auch Epidemien oder Naturkatastrophen können dazu führen, dass Mitarbeiter nicht mehr auf sichere Weise zur Arbeit kommen können.

In diesen Szenarien muss ein Unternehmen in der Lage sein, eine sichere Remote-Konnektivität zum Unternehmensnetzwerk zu unterstützen. Über 400.000 Fortinet-Kunden verfügen über diese Funktionalität, die bei ihrer vorhandenen Technologie-Implementierung bereits integriert ist: FortiGate NGFWs unterstützen von Hause aus IPsec-VPNs und ermöglichen sichere Verbindungen für Mitarbeiter, die vom Homeoffice arbeiten oder bei alternierender Telearbeit zeitweise einen externen Arbeitsplatz nutzen.

Remote Working verringert die unproduktive Zeit der Mitarbeiter um durchschnittlich 27 %.[1]

Mitarbeiter arbeiten im Homeoffice durchschnittlich 16,8 Tage mehr im Jahr als im Firmensitz.[2]

85 % der Mitarbeiter geben an, dass sie im Homeoffice ihre maximale Produktivität erreichen.[3]

Durch die Einführung von Remote Working stieg die Mitarbeiterbindung in 95 % der Unternehmen.[4]

FortiGate NGFWs: Sicherheit für auswärts arbeitende Mitarbeiter

Die in jeder FortiGate NGFW integrierten IPsec- und SSL-VPNs bieten ein äußerst flexibles Implementierungsmodell. Extern arbeitende Mitarbeiter können ohne Client oder über einen Thick-Client – der zum Endpunkt-Schutz von FortiClient gehört – auf erweiterte Funktionen zugreifen. Für Poweruser und Superuser ist zudem ein FortiAP oder eine FortiGate NGFW für zusätzliche Funktionen sinnvoll.

Fortinet-Lösungen sind so konzipiert, dass sie von der Anschaffung bis zur Ausmusterung einfach zu bedienen sind, z. B. mit einer Zero-Touch-Bereitstellung wie bei FortiGate NGFWs und FortiAP Wireless Access Points. Auch können Appliances vor dem Transport an einen Remote-Standort vorkonfiguriert und automatisch am alternativen Arbeitsplatz eingerichtet werden. Ein kontinuierlicher Geschäftsbetrieb und die Unterstützung von Telearbeit ist somit sichergestellt.

Die Fortinet Security Fabric nutzt das gemeinsame Fortinet-Betriebssystem und eine offene API-Umgebung, um eine breite, integrierte und automatisierte Sicherheitsarchitektur zu schaffen. Mit der Fortinet Security Fabric können alle Geräte eines Unternehmens zentral überwacht und verwaltet werden, einschließlich der Geräte für die Telearbeit an entfernten Standorten. Mit einer FortiGate NGFW oder dem FortiManager als zentralisierte Management-Plattform erhält das Security-Team vom Hauptsitz aus – unabhängig von der jeweiligen Implementierung – einen vollständigen Überblick über alle Geräte im Netzwerk.

Bei einer Naturkatastrophe oder einer anderen grundlegenden Störung des normalen Geschäftsbetriebs muss ein Unternehmen in der Lage sein, schnell die gesamte Belegschaft auf die Arbeit im Homeoffice umzustellen. Tabelle 1 zeigt die Anzahl der gleichzeitigen VPN-Benutzer, die die verschiedenen FortiGate NGFW-Modelle unterstützen.

Fortinet-Lösungen bieten neben der Datenverschlüsselung bei VPN-Übertragungen viele weitere Funktionen, mit denen ein Unternehmen auswärts arbeitende Mitarbeiter besser schützen kann. Diese Funktionen umfassen:

- **Multifaktor-Authentifizierung (MFA):** FortiToken und FortiAuthenticator ermöglichen die Zwei-Faktor-Authentifizierung für Remote Worker.
- **Data Loss Prevention (DLP):** FortiGate und FortiWiFi bieten Funktionen für Remote Worker, die bei Telearbeit vor Datenverlusten schützen. Unerlässlich für Führungskräfte im Homeoffice, die häufig auf vertrauliche Unternehmensdaten zugreifen müssen.

- **Schutz vor komplexen Bedrohungen:** FortiSandbox bietet eine Analyse von Malware und anderen verdächtigen Inhalten in einer Sandbox-Umgebung, bevor diese ihr Ziel erreichen können.
- **WLAN-Verbindungen:** FortiAPs stellen einen sicheren WLAN-Zugang für Remote Worker mit vollständiger Integration und zentralem Konfigurations-Management bereit.
- **Telefonie:** FortiFone ist eine sichere Lösung für die VoIP-Telefonie (Voice-over-IP). Alle Übertragungen werden von einer FortiGate NGFW geschützt, verwaltet und überwacht. Erhältlich als Soft Client und in verschiedenen Hardware-Optionen.

Modell	Gleichzeitige SSL-VPN-Benutzer	Gleichzeitige IPsec-VPN-Benutzer	Managed FortiAPs (Tunnel-Modus)
100E	500	10.000	32
100F	500	16.000	64
300E	5.000	50.000	256
500E	10.000	50.000	256
600E	10.000	50.000	512
1100E	10.000	100.000	2.048
2000E	30.000	100.000	2.048
Alle größeren Modelle*	30.000	100.000	2.048
*Modell 3300E unterstützt 1.024 APs im Tunnel-Modus.			

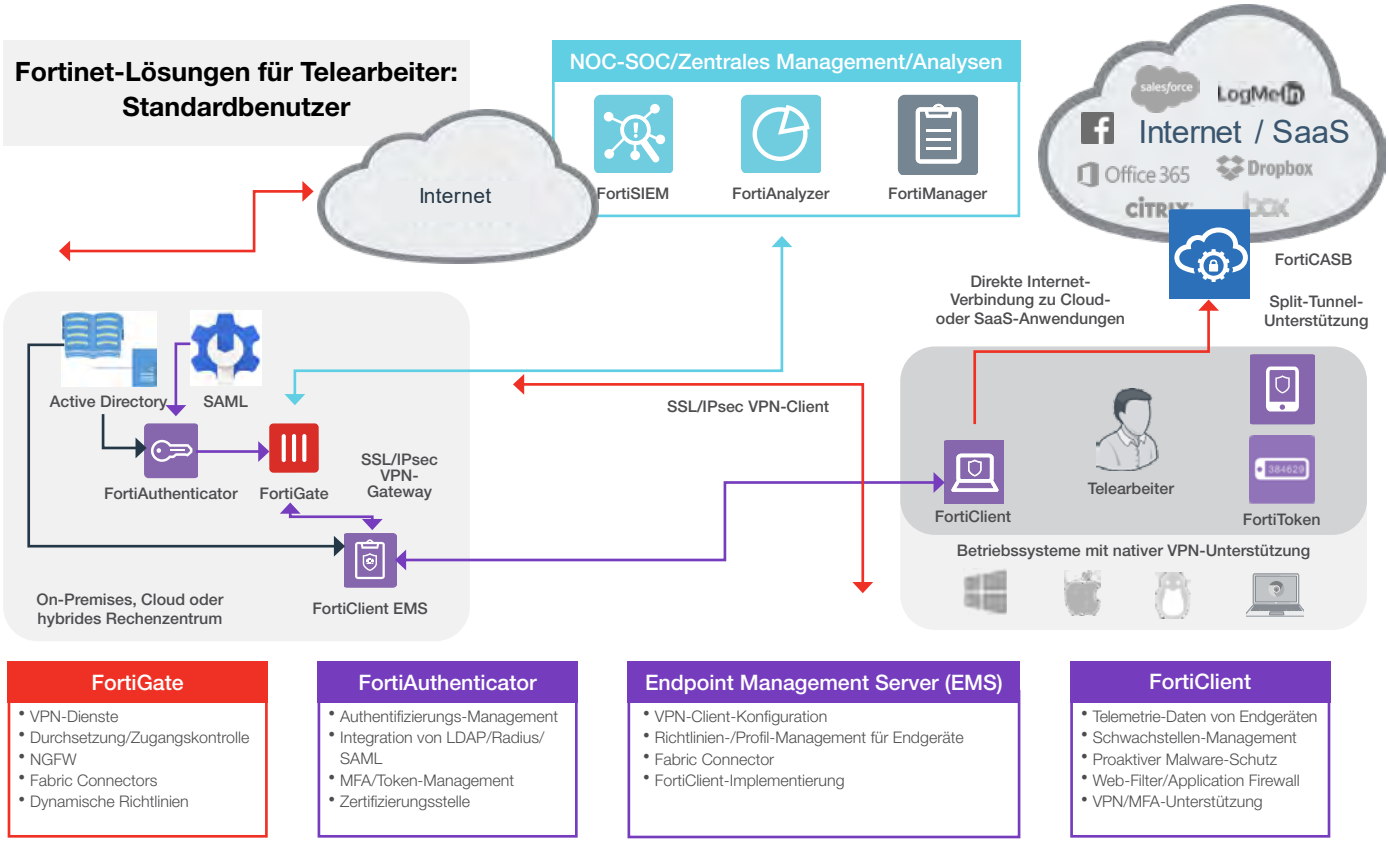
Tabelle 1: Anzahl der gleichzeitigen VPN-Verbindungen, die verschiedene FortiGate NGFW-Modelle unterstützen.

Anwendungsfälle für Fortinet-Produkte, die Remote Working unterstützen

Nicht jeder Mitarbeiter benötigt den gleichen Zugriff auf Unternehmensressourcen, wenn er von auswärts arbeitet. Fortinet bietet deshalb maßgeschneiderte Telearbeitslösungen für unterschiedliche Arten von externen Mitarbeitern an:

1. **Normaler Telearbeiter:** Der Standardbenutzer benötigt für die Telearbeit lediglich Zugriff auf E-Mails, das Internet, Telefonkonferenzen sowie eine eingeschränkte Dateifreigabe und aufgabenspezifische Funktionen (Finanzen, HR usw.). Dies umfasst auch den Zugriff auf SaaS-Anwendungen (Software-as-a-Service) in der Cloud wie Microsoft Office 365 sowie eine sichere Verbindung zum Unternehmensnetzwerk.

   Telearbeit-Standardbenutzer können sich mit der im FortiClient integrierten VPN-Client-Software mit dem Unternehmensnetzwerk verbinden. Die Identitätsprüfung erfolgt mit der Multifaktor-Authentifizierung von FortiToken. Hinweis: Beim Roaming vom festgelegten Telearbeitsplatz zu einem anderen Ort werden Poweruser und Superuser automatisch zu Standardbenutzern herabgestuft.



FortiGate
- VPN-Dienste
- Durchsetzung/Zugangskontrolle
- NGFW
- Fabric Connectors
- Dynamische Richtlinien

FortiAuthenticator
- Authentifizierungs-Management
- Integration von LDAP/Radius/SAML
- MFA/Token-Management
- Zertifizierungsstelle

Endpoint Management Server (EMS)
- VPN-Client-Konfiguration
- Richtlinien-/Profil-Management für Endgeräte
- Fabric Connector
- FortiClient-Implementierung

FortiClient
- Telemetrie-Daten von Endgeräten
- Schwachstellen-Management
- Proaktiver Malware-Schutz
- Web-Filter/Application Firewall
- VPN/MFA-Unterstützung

Abbildung 1: Fortinet-Lösung für Telearbeiter – Standardbenutzer (Implementierungsbeispiel)

2. **Poweruser:** Poweruser sind Mitarbeiter, die bei der Arbeit außerhalb des Unternehmens einen umfassenderen Zugriff auf Unternehmensressourcen benötigen, z. B. auf mehrere IT-Umgebungen. Typische Poweruser sind Systemadministratoren, IT-Supporttechniker und Notfall-Teams.

   Für Poweruser bietet ein FortiAP Access Points im Homeoffice das erforderliche Maß an Zugriff und Security. Dies ermöglicht bei alternierender Telearbeit auch vom externen Standort aus eine geschützte WLAN-Verbindung über einen sicheren Tunnel zum Unternehmensnetzwerk. FortiAPs können mit Zero-Touch-Provisionierung (ZTP) bereitgestellt und zentral über FortiGate-NGFWs im Firmensitz verwaltet werden. Muss der Mitarbeiter telefonisch über eine Geschäftsnummer erreichbar sein, wird das Telefon einfach an den FortiAP angeschlossen und ist dann mit der Unternehmenszentrale verbunden.

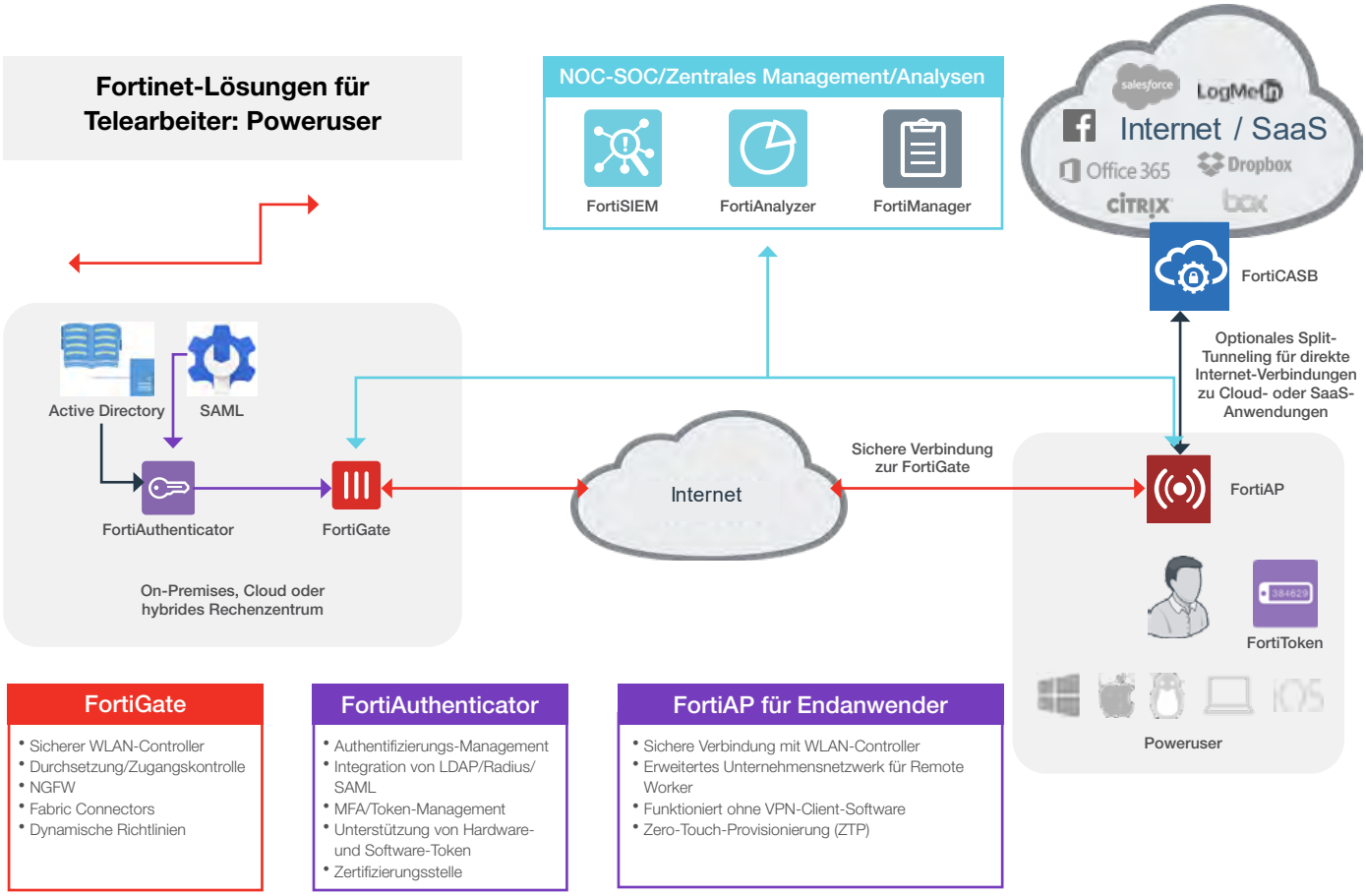


Abbildung 2: Fortinet-Lösung für Poweruser (Implementierungsbeispiel)

3. **Superuser:** Ein Superuser arbeitet oft mit äußerst sensiblen Informationen und benötigt für die alternierende Telearbeit vom Homeoffice einen erweiterten Zugriff auf vertrauliche Unternehmensressourcen. Dieses Mitarbeiterprofil umfasst Administratoren mit privilegiertem Systemzugriff, Supporttechniker, wichtige Partner für einen kontinuierlichen Geschäftsbetrieb, Notfall-Teams und die Geschäftsleitung.

   Für Superuser sollte der alternative Arbeitsplatz wie ein Bürostandort konfiguriert werden. Neben den gleichen Lösungen wie für Standardbenutzer und Poweruser werden zusätzliche Funktionen benötigt: Für sichere WLAN-Verbindungen mit integriertem Schutz vor Datenverlusten (DLP) kann ein FortiAP in eine FortiGate NGFW- oder FortiWiFi-Appliance integriert werden. Die Telefonie über VoIP wird mit FortiFone (als Soft-Client- oder Hardware-Version) bereitgestellt. Management und Security werden mit einer FortiGate-NGFW direkt am Telearbeitsplatz oder zentral mit dem FortiManager im Hauptsitz gewährleistet.

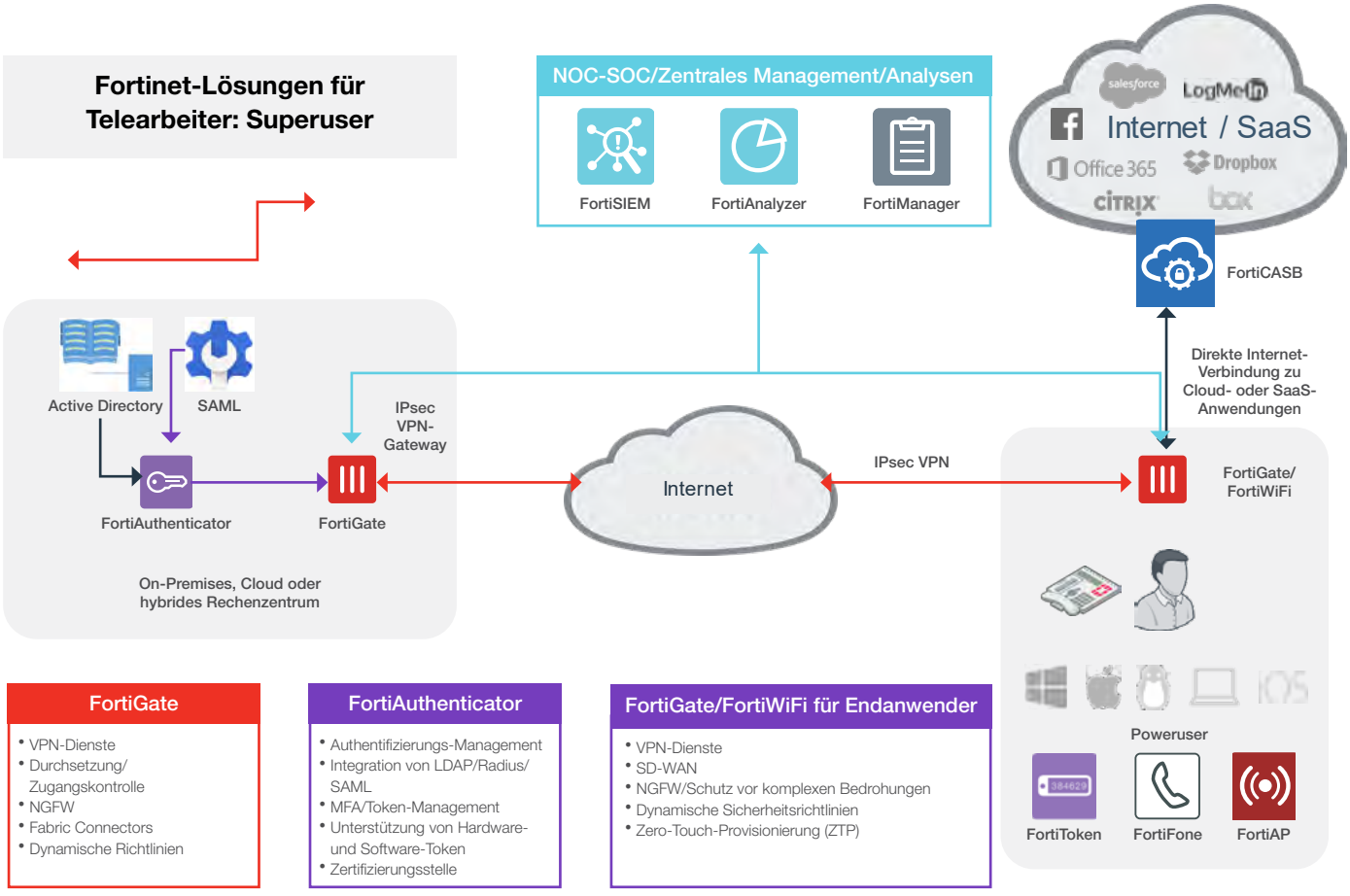


Abbildung 3: Fortinet-Lösung für Superuser (Implementierungsbeispiel)

Unterstützung von auswärts arbeitenden Mitarbeitern

Fortinet-Lösungen lassen sich problemlos an externen Arbeitsplätzen bereitstellen. Ein Unternehmen benötigt jedoch auch Ressourcen vor Ort oder in der Cloud, um Telearbeiter sicher zu unterstützen.

Viele Unternehmen verfügen bereits über diese Ressourcen als Teil ihrer vorhandenen Security-Architektur. Als Next-Generation-Firewall kann die FortiGate NGFW z. B. den gesamten verschlüsselten und Klartext-Datenverkehr eines Unternehmens bei minimalen Leistungseinbußen überprüfen. Weiter bietet die NGFW ein integriertes VPN-Gateway, das als Endpunkt für verschlüsselte Verbindungen zu Telearbeitern fungiert.

Eine FortiGate NGFW umfasst auch die Integration in weit verbreitete IT-Infrastrukturen, z. B. in Corporate Director Services wie Microsoft Active Directory (AD) oder MFA- und Single-Sign-On-Lösungen (SSO). FortiAuthenticator dient als dabei als einziger zentraler Integrationspunkt für Authentifizierungslösungen, der neben FortiToken – erhältlich als Hard-, Soft-, Smartphone- oder E-Mail-Option – auch Drittlösungen unterstützt.

Beim Management einer auswärts arbeitenden, geografisch verteilten Belegschaft ist eine zentralisierte Security-Transparenz und -Verwaltung unerlässlich. Alle Fortinet-Lösungen können über die Fortinet Security Fabric integriert werden. Das Security-Team erhält mit dem FortiManager eine zentrale Transparenz und Kontrolle über eine einzige Konsole. Log-Aggregierung und Security-Analysen lassen sich mit dem FortiAnalyzer durchführen, während FortiSIEM potenzielle Bedrohungen schnell erkennt und abwehrt.

Vollständig integrierte Security mit Fortinet-Lösungen

Die Fortinet Security Fabric ermöglicht die nahtlose Integration der Remote-Belegschaft eines Unternehmens. Alle Fortinet-Lösungen sind über die Fortinet Security Fabric vernetzt und bieten so eine zentrale Transparenz, Konfiguration und Überwachung. Verschiedene Fabric Connectors, eine offene API-Umgebung, Unterstützung der DevOps-Community und das große erweiterte Ecosystem der Security Fabric ermöglichen zudem die Integration mit über 250 Drittlösungen.

Dies ist für die Planung eines kontinuierlichen Geschäftsbetriebs entscheidend, da ein Unternehmen womöglich gezwungen ist, ohne oder mit geringer Vorlaufzeit komplett auf die Arbeit vom Homeoffice umzustellen. Eine Security-Architektur, die eine zentrale Transparenz und Verwaltung bietet, gewährleistet in einer solchen Situation, dass durch die Unterstützung von Telearbeit die Cyber-Sicherheit des Unternehmens nicht gefährdet wird.

Die folgenden Lösungen sind Teil der Fortinet Security Fabric und unterstützen eine sichere Telearbeit:

- **FortiClient:** FortiClient stärkt die Endgeräte-Security durch integrierte Transparenz, Kontrolle und proaktive Bedrohungsabwehr. Unternehmen können damit Risiken durch Endpunkte in Echtzeit erkennen, überwachen und einschätzen.
- **FortiGate:** FortiGate NGFWs nutzen spezielle Security-Prozessoren. Das gewährleistet einen erstklassigen Schutz sowie eine durchgängige Transparenz, zentrale Kontrolle und hohe Leistung für verschlüsseltem und Klartext-Traffic.
- **FortiWiFi:** FortiWiFi WLAN-Gateways kombinieren die Sicherheitsvorteile von FortiGate NGFWs mit einem drahtlosen Access Point zu einer integrierten Netzwerk- und Security-Lösung für Telearbeiter.
- **FortiFone:** FortiFone ermöglicht eine einheitliche Sprachkommunikation über VoIP-Verbindungen. Schutz und Management erfolgen über FortiGate NGFWs. Mit dem FortiFone-Softclient können Mitarbeiter Anrufe tätigen oder empfangen, auf Voicemails zugreifen, Anruferlisten anzeigen und das Telefonverzeichnis des Unternehmens direkt mit dem Smartphone durchsuchen. Mehrere Hardware-Optionen erhältlich.
- **FortiToken:** FortiToken bestätigt zusätzlich die Identität von Benutzern. Dem Authentifizierungsprozess wird durch Hardware- oder Software-Tokens (Smartphone App) ein zweiter Faktor hinzugefügt.
- **FortiAuthenticator:** FortiAuthenticator bietet zentralisierte Authentifizierungsdienste, einschließlich Single-Sign-On (SSO), Zertifikatsverwaltung und Gäste-Management.
- **FortiAP:** FortiAP bietet einen sicheren WLAN-Zugang für dezentrale Unternehmen und Remote Worker. Der Access Point lässt sich einfach mit einer FortiGate NGFW oder über die Cloud verwalten.
- **FortiManager:** FortiManager zentralisiert das Management und die Kontrolle von Richtlinien für das gesamte erweiterte Unternehmen und bietet Einblick in netzwerkweite Bedrohungen durch den Datenverkehr. Der FortiManager umfasst Funktionen zum Eindämmen komplexer Bedrohungen und lässt sich für die Verwaltung von bis zu 10.000 Fortinet-Geräten skalieren.
- **FortiAnalyzer:** FortiAnalyzer bietet eine analysebasierte Cyber-Sicherheit und ein Log-Management, was die Bedrohungserkennung und den Schutz vor Sicherheitsverletzungen verbessert.
- **FortiSandbox:** Fortinet Sandboxing-Lösungen arbeiten mit einer leistungsstarken Kombination aus innovativer Erkennung, automatisierter Abwehr, umsetzbaren Erkenntnissen und flexibler Implementierung, um gezielte Angriffe und dadurch bedingte Datenverluste zu stoppen. Verfügbar als Cloud-Dienst (in den meisten FortiGuard-Subscriptions inbegriffen).

Eine sichere Grundlage für einen kontinuierlichen Geschäftsbetrieb

Die Vorbereitung für die Aufrechterhaltung eines kontinuierlichen Geschäftsbetriebs und die Wiederherstellung nach einem Katastrophenfall (Disaster Recovery) ist für jedes Unternehmen von kritischer Bedeutung. Ein zentrales Element stellt dabei die Fähigkeit dar, ohne oder mit geringer Vorlaufzeit die Belegschaft größtenteils oder vollständig auf die Arbeit im Homeoffice umzustellen.

Bei der Entwicklung eines Plans für einen kontinuierlichen Geschäftsbetrieb muss sichergestellt werden, dass das Unternehmen über die richtigen Ressourcen verfügt, um auswärts arbeitende Mitarbeiter zu schützen. Fortinet-Lösungen lassen sich einfach bereitstellen, konfigurieren und ermöglichen Unternehmen – unabhängig von der Implementierungsumgebung – die Gewährleistung einer lückenlosen Security, Transparenz und Kontrolle.

1 „The Benefits of Working From Home“. Airtasker, 9. September 2019.

2 Ebd.

3 Abdullahi Muhammed: „Here's Why Remote Workers Are More Productive Than In-House Teams“. Forbes, 21. Mai 2019.

4 Ebd.

FORTINET®

www.fortinet.com/de

26. Mai 2020, 14:22

618770-0-1-DE

sb-FA-secure-remote-access-for-your-workforce-at-scale-3132020_A4_DE