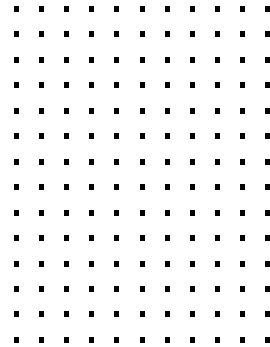


Work from Anywhere: Fünf Schlüsseltechnologien für eine sichere Telearbeit- und Homeoffice-Lösung



Hybride Arbeitsmodelle erfordern einen neuen Blick auf die Security. Unabhängig davon, wo Mitarbeiter arbeiten – ob Zuhause, in der Firma, beim Kunden oder auf Geschäftsreisen – müssen die gleichen strengen Sicherheitsrichtlinien gelten. Entscheidend ist, dass das Unternehmen eine Security der Enterprise-Klasse an jedem Ort bereitstellen und durchsetzen kann.

Neben Next-Generation Firewalls (NGFW) im Büro sorgen folgende fünf Schlüsseltechnologien dafür, dass Mitarbeiter unabhängig vom Arbeitsort produktiv bleiben und sicher geschützt sind:

✓ Endpunkt-Schutz

Mitarbeiter nehmen Geräte wie Laptops mit, wenn sie vom Büro ins Homeoffice wechseln oder auf Geschäftsreise gehen. Doch von dort erfolgen Zugriffe auf Unternehmensressourcen oft über unsichere Zugangspunkte, wie z. B. Hotspots auf dem Flughafen oder in Cafés. Angesichts der besorgniserregenden Zunahme von tückischer Malware bedeutet das, dass diese Geräte an praktisch jedem Ort angegriffen werden können. Unternehmen benötigen eine EDR-Lösung (Endpoint Detection and Response), die cloudbasierte künstliche Intelligenz mit automatisierten Abläufen (so genannte Playbooks) kombiniert, um Geräte und Mitarbeiter und somit die Produktivität zu schützen. Fortinet FortiEDR bietet einen fortschrittlichen Endpunkt-Schutz, der hochkomplexe Bedrohungen erkennt und Sicherheitsverletzungen sowie Ransomware-Schäden in Echtzeit stoppt.

✓ Kontrolle über den Anwendungszugriff

Unternehmen brauchen eine Access Policy Engine – eine systematische Zugangsregelung, die Anwendern an jedem Standort einen angemessenen, sicheren Zugriff anhand der Benutzer- und Geräteidentität, des Standorts, des Gerätetyps und des Sicherheitsprofils gewährt. Fortinet bietet dafür die bereits in FortiGate NGFWs integrierte ZTNA-Funktion (Zero Trust Network Access) und den FortiClient Fabric Agent an.

✓ Kontrolle und Sicherheit von Heimnetzwerken

Eine unternehmenstaugliche Security muss auch anfällige und oft überlastete Heimnetzwerke schützen. Das Unternehmen sollte für Telearbeit und Homeoffices ein sicheres – und vom Unternehmen kontrolliertes – Netzwerk bereitstellen, das die Bandbreite für Videokonferenzen optimiert und zugleich die Privatsphäre für die nichtberufliche Nutzung gewährleistet. Gemeinsam mit Linksys bietet Fortinet die Lösung *Linksys HomeWRK for Business | Secured by Fortinet* an, die die Sicherheit der Enterprise-Klasse von Fortinet mit der WLAN-Abdeckung von Linksys in privaten Umgebungen kombiniert.

✓ Cloudbasierte Security Services

Die Netzwerk-Sicherheit für mobile Mitarbeiter ist eine besondere Herausforderung. EDR und ZTNA schützen zwar das Endgerät und kontrollieren den Anwendungszugriff, aber der Internetzugang muss ebenfalls gesichert werden. Ein cloudbasiertes Secure Web Gateway (SWG) und Firewall-as-a-Service (FWaaS)-Dienste können diese sichere Konnektivität unterwegs gewährleisten. Fortinet FortiSASE ist dafür ideal: Dieser Security Service wird über die Cloud bereitgestellt und schützt Mitarbeiter überall – ob beim Arbeiten im Café oder auf dem Flughafen.

✓ Einheitliche Plattform für integrierte Sicherheit, die alles verbindet

Der Versuch, eine WFA-Umgebung mit verschiedenen Anbietern oder inkompatiblen Einzelprodukten für Sicherheitskomponenten wie Endpunkt-Schutz, EDR, Identitätsprüfung oder Firewalls zu schützen, ist nahezu unmöglich. Die Fortinet Security Fabric vereint deshalb ein breites Portfolio an Sicherheitslösungen für den Zero-Trust-Zugang, Endpunkt-Schutz und die Netzwerk-Sicherheit, die Benutzer mit einer vollintegrierten Security, Diensten und Bedrohungsinformationen überall nahtlos schützen – ob unterwegs, zu Hause oder im Büro.

Arbeiten überall – aber sicher

Der Schutz von Mitarbeitern beim Wechsel zwischen Büro, Homeoffice, Café, Flughafen und anderen Arbeitsorten ist für viele IT-Teams eine Herausforderung, insbesondere da Angriffe auf Remote-Mitarbeiter zugenommen haben. Fortinet bietet eine integrierte, umfassende Sicherheit, mit der Unternehmen ihre Belegschaft und Geräte vollkommen ortsunabhängig schützen und einen sicheren Zugriff auf kritische Anwendungen und Ressourcen bereitstellen können.