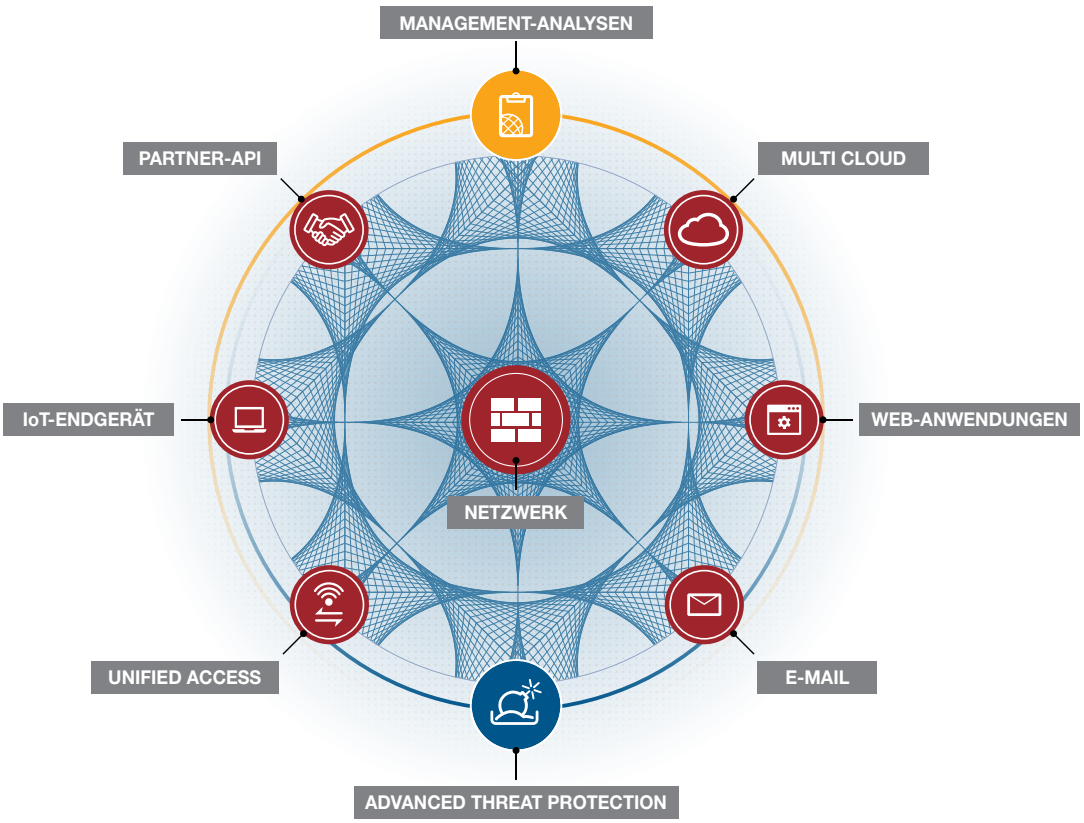
SECURITY TRANSFORMATION ERFORDERT EINE SECURITY FABRIC

Das Wachstum und die Einführung neuer Technologien in den vergangenen Jahren hat Unternehmen, Behörden und auch die Wirtschaft selbst stark verändert. Dies hat Auswirkungen darauf, wie Personen auf sozialer Ebene interagieren, ihre Geldgeschäfte erledigen, Einkäufe tätigen, Transaktionen durchführen, Nachrichten erhalten, Unterhaltung konsumieren und auch wie sie in ihrer Umgebung navigieren. Neue Technologien haben auch die Erwartungen und Einstellungen der Menschen als Verbraucher und als Mitarbeitern – bei ihren Interaktionen mit Unternehmen und Diensten grundlegend geändert.

Um wettbewerbsfähig zu bleiben, mussten Unternehmen reagieren und neu definieren, wie sie auf dem neuen digitalen Handelsplatz agieren und die sich ändernden Anforderungen von technisch versierten Benutzern erfüllen. Für die meisten Unternehmen führt die digitale Transformation zur Integration digitaler Technologien in allen Geschäftsbereichen. Dies verändert die Art und Weise, wie sie arbeiten und ihre Produkte an ihre Kunden liefern, grundlegend.

Hierzu müssen Unternehmen eine Vielzahl von Geräten, Technologien und Diensten in einem einzigen, integrierten Netzwerk zusammenführen, das dynamisch erweitert und angepasst werden kann, um sich entwickelnde Markt- und Benutzeranforderungen zu erfüllen. Das bedeutet gleichzeitig, dass zahlreiche Fragen gelöst werden müssen, wie IoT, SDN, OT und Multi Cloud-Umgebungen, die zunehmende Verbreitung interner und kundenbezogener Anwendungen, eine nie dagewesene Zunahme der Geschwindigkeit und Volumen der generierten und empfangenen Daten, die Erweiterung von Workloads über die Grenzen des Rechenzentrums hinaus und die Erwartungen der nächsten Generation von Mitarbeitern, ihre



Arbeit und ihr Privatleben auf einem beliebigen mobilen Gerät ihrer Wahl zu verschmelzen, das jederzeit und überall sofortigen Zugang auf alle Daten bereitstellt.

Diese digitale Transformation hat die IT-Teams an ihre Belastungsgrenze gebracht und gleichzeitig die Angriffsfläche, die es zu schützen gilt, exponentiell verbreitert. Multi Cloud-Umgebungen bedeuten zum Beispiel, dass Unternehmen sich um eine Angriffsfläche kümmern müssen, die möglicherweise für IT-Systeme nicht immer sichtbar ist, und die Konvergenz von IT- und OT-Umgebungen hat beispielsweise Fertigungsumgebungen, industrielle Steuerungssysteme und kritische Infrastruktur neuen Risiken ausgesetzt. Die Verbreitung von IoT-Geräten in all diesen Umgebungen, die sich ausschließlich auf die Sicherheit beim Netzwerkzugang verlassen, hat diese Herausforderungen verstärkt.

Während geschäftskritische und unternehmenseigene Daten in die Cloud verschoben oder von cloudbasierten Anwendungen und Diensten verwaltet werden, hat das Wachstum der Schatten-IT dazu geführt, dass Unternehmen keinen Überblick mehr darüber haben, wo ihre Daten gespeichert sind oder welche Sicherheitsmaßnahmen für ihren Schutz vorhanden sind. BYOD erschwert das Thema Data Governance noch weiter, da Benutzer von öffentlichen Orten aus auf kritische Daten zugreifen und diese auf persönlichen Geräten speichern können, auf denen sie ihre privaten ebenso wie Geschäftsdaten nutzen.

SECURITY TRANSFORMATION

Während unternehmerische und wirtschaftliche Kräfte die Entwicklung der Netzwerke schnell vorantreiben, haben IT-Security-Abteilungen Probleme, mit dieser Entwicklung Schritt zu halten. Ein erheblicher Teil des Problems besteht darin, dass die digitale Transformation nicht als einzelner, integrierter Vorgang abläuft. Vielmehr verläuft sie organisch über getrennte Projekte, die den Zeiger jeweils ein klein wenig weiterschieben. Es besteht die Tendenz, jedes neue Netzwerksegment zum Zeitpunkt seiner Entwicklung mithilfe der herkömmlichen Security Tools, die am einfachsten verfügbar sind, zu schützen. Dies führt schließlich zu einer komplexen und weitgehend zufällig strukturierten Sicherheitsinfrastruktur, die um isolierte Lösungen unterschiedlicher Anbieter herum gebaut ist.

Leider ist Komplexität gewöhnlich der Feind der Security. Da verschiedene Umgebungen unterschiedliche Formfaktoren für Lösungen erfordern, kann es schwierig sein, einen einzigen Anbieter als Standard zu nutzen, da zwischen einer physischen, virtuellen oder cloudbasierten Version eines Produkts große Variationen vorliegen können, sofern diese überhaupt verfügbar sind. Das hat zur Folge, dass Unternehmen durchschnittlich mehr als 30 verschiedene Sicherheitslösungen über ihre verteilten Netzwerke hinweg implementiert haben. Isolierte Sicherheitslösungen mit getrennten Management-Schnittstellen und fehlenden praktischen Möglichkeiten, Bedrohungsdaten zu sammeln oder an andere Geräte innerhalb des Netzwerks weiterzugeben, können die Sichtbarkeit behindern und die Kontrolle einschränken.

Die beste Antwort auf zunehmend komplexe Netzwerkumgebungen ist Einfachheit. Hierzu ist eine Security Transformation erforderlich, die mit der digitalen Transformation Schritt halten kann. Die Security Transformation erfordert die Integration von Sicherheit in alle Bereiche der digitalen Technologie und führt zu einer einheitlichen und ganzheitlichen Sicherheitsarchitektur. Sie ermöglicht einen effektiven Security-Lebenszyklus, der sich über das gesamte Ökosystem von Netzwerken hinweg erstreckt, und umfasst das Identifizieren der Angriffsfläche, den Schutz vor bekannten Bedrohungen, das Erkennen unbekannter Bedrohungen, schnelle und koordinierte Reaktionen auf Cyber-Ereignisse und die Bereitstellung kontinuierlicher Gefahrenbewertungen.

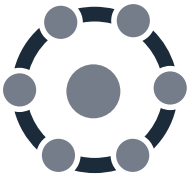
Eine effektive Security Transformation-Strategie muss kollaborative Informationen und Systemintegration einbeziehen, damit lokale und globale Bedrohungsdaten zwischen den Geräten weitergegeben und Reaktionen zwischen Lösungen

koordiniert werden können. Die Strategie muss die Orchestrierung einheitlicher Richtlinien und deren Durchsetzung ermöglichen ebenso wie die intelligente Segmentierung über physische und virtuelle Umgebungen hinweg, um eine tiefgehende Sichtbarkeit des Datenverkehrs bereitzustellen, der sich quer durch das Netzwerk und auch über Multi Cloud-Umgebungen hinweg bewegt. Infizierte Geräte müssen dann schnell identifiziert und isoliert werden. Automatisierte Funktionen müssen außerdem das zunehmende Netzwerkrauschen durchkämmen, Bedrohungsdaten in Beziehung setzen und in Echtzeit auf alle Bedrohungen reagieren, die entlang der erweiterten Angriffsfläche gefunden werden.

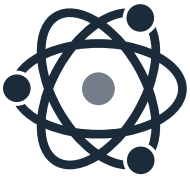
DIE FORTINET SECURITY FABRIC

Die Fortinet Security Fabric ist ein architektonischer Ansatz, der die Sicherheitstechnologien, die über das digitale Netzwerk hinweg verteilt sind – einschließlich Multi Cloud, Endgeräte, E-Mail- und Web-Anwendungen sowie Netzwerk-Access Points – in ein einziges Security-System einbezieht. Dies erfolgt über eine Kombination offener Standards und eines gemeinsamen Betriebssystems. Diese Lösungen werden dann durch die Integration moderner Advanced Threat Protection-Technologien und ein einheitliches Korrelations-, Verwaltungs- Orchestrierungs- und Analysesystem erweitert.

Der Fabric-basierte Security-Ansatz basiert auf drei Grundpfeilern:



Umfassende Abdeckung. Sichtbarkeit und Schutz müssen sich über die gesamte digitale Angriffsfläche hinweg erstrecken. Wenn Daten und Workloads zwischen einer Vielzahl von Geräte-Formfaktoren und Netzwerk-Ökosystemen übertragen werden, müssen IT-Teams eine ganzheitliche Sicht auf Geräte, Datenverkehr, Anwendungen und Ereignisse haben und die Fähigkeit besitzen, Bedrohungen an jedem beliebigen Ort entlang der Angriffsfläche zu stoppen. Dieser Ansatz muss physische Netzwerke, IoT, mobile Geräte und Benutzer ebenso einbeziehen wie zunehmend komplexe Multi Cloud-Umgebungen sowohl für IaaS- als auch für SaaS-Lösungen.



Integration. Die Integration von Geräten unter Verwendung offener Standards, gemeinsamer Betriebssysteme und einheitlicher Management-Plattformen ermöglicht die Weitergabe und Korrelation von Echtzeit-Bedrohungsdaten. Dieses gemeinsame Framework unterstützt auch die koordinierte Erkennung von komplexen Bedrohungen durch hochentwickelte, zentralisierte Analysefunktionen, die mit herkömmlichen isolierten Security-Implementierungen nur schwer oder überhaupt nicht zu erreichen sind.

Automatisierung. Wie das moderne digitale Geschäft, erfolgen auch Cyber-Angriffe mit digitaler Geschwindigkeit. Die Zeit zwischen dem Eindringen in ein Netzwerk und der Infizierung von Daten oder Systemen liegt im Bereich von Millisekunden. Security-Systeme müssen automatisch kontinuierliche Gefahrenbewertungen vornehmen und bei erkannten Bedrohungen sofortige koordinierte Abwehrmaßnahmen ergreifen. Da moderne Netzwerkumgebungen hochelastisch sind, muss Security auch in der Lage sein, sich dynamisch anzupassen, wenn sich Netzwerkanforderungen und Konfigurationen ändern.

Zur Bereitstellung dieser Funktionen ist die Fortinet Security Fabric um eine Reihe von Schlüsselelemente herum aufgebaut:

- Network Security. In einer Zeit, in der sich Netzwerke über ihre traditionellen Grenzen hinaus entwickeln, suchen komplexe Cyber-Angriffe nach Schwachstellen der erweiterten Angriffsfläche. Die Fortinet Produktfamilie von hochleistungsstarken Firewalls, die auf einem konsolidierten und integrierten System von fortschrittlichen Sicherheitslösungen basiert, ist die wichtigeste erste Verteidigungslinie eines jeden Unternehmens.
- Multi Cloud Security. Die Mehrzahl von Unternehmen nutzt eine Multi Cloud-Strategie, die mehrere IaaS-Anbieter und über ein Dutzend unterschiedlicher SaaS-Lösungen umfasst. Die Ausweitung von Daten und Workloads in eine verteilte Cloud-Umgebung erschwert die konsolidierte Bedrohungsabwehr und -erkennung. Die integrierten virtuellen und physischen Lösungen von Fortinet erweitern, unterstützt durch die Fortinet Security Fabric, die Sicherheit über Ihre verteilte Cloud-Implementierung hinweg und sind gleichzeitig die ersten, die erweiterte Sicherheitslösungen für alle fünf führenden Cloud Service Provider anbieten.
- Web Application Security. Ungeschützte oder anfällige Web-Anwendungen sind häufige Einfallstore in Ihr Netzwerk. Die FortiWeb Web Application Firewall verwendet die neuesten Erkennungs- und Schutztechnologien sowie erweiterte intelligente Funktionen zum Schutz von Web-Anwendungen vor komplexen Angriffen.
- Email Security. E-Mail ist nach wie vor der Hauptzugangspunkt für Malware zur Infizierung Ihres Netzwerks. E-Mail-Spammer und -Phisher verwenden infizierte Anhänge, schädliche Links und raffinierte betrügerische Maschen, um Benutzer dazu zu bringen, auf Malware zu klicken oder sie auszuführen. Im Jahr 2017 war E-Mail der Hauptvektor für Ransomware. Das sichere E-Mail-Gateway FortiMail überprüft eingehende und ausgehende E-Mail, blockiert schädliche Nachrichten und Anhänge und verhindert, dass sensible Daten abfließen.

- Secure Unified Access . Die meisten WLAN Access Points bieten Konnektivität, aber kaum echte Sicherheit. Wenn jedoch immer mehr Geräte Zugang über WLAN erhalten, ist für den Schutz von Geschäftsdaten, personenbezogenen Informationen (PII), mobilen Geräten und eine Vielzahl von Benutzeranforderungen wesentlich mehr erforderlich als einfache Zugangskontrolle. Die Fortinet Secure Access-Lösungen bieten leistungsstarken Zugang kombiniert mit umfassender Security und Application Control für sichere WLANs, die voll in Ihre Netzwerksicherheitsprotokolle und -richtlinien integriert sind.
- Endpoint Security . Netzwerke müssen äußerst mobile Arbeitskräfte und eine zunehmende Zahl von mit dem Netzwerk verbundenen privaten Endgeräten unterstützen. Es überrascht nicht, dass diese Geräte ein weiterer häufiger Eintrittspunkt für Bedrohungen sind. Die Herausforderung besteht darin, dass Endgerätelösungen häufig keine Bedrohungsdaten mit dem Rest des Netzwerks teilen. Dies erschwert es, heraus zu finden, ob ein Gerät infiziert ist, und kann die Bedrohungsabwehr verlangsamen, wenn ein Gerät beginnt, sich auffällig zu verhalten. FortiClient ermöglicht es IT-Teams, eine Stufe automatisierter Endgerätesicherheit in die Security Fabric für schnelleren und umfassenderen Netzwerkschutz zu integrieren.
- Advanced Threat Protection. Moderne komplexe Bedrohungen sind so konzipiert, dass sie ihrer Erkennung durch mehrstufige Angriffe, vielschichtige Angriffsvektoren und die Beobachtung und Nachahmung von legitimen Anwendungen und normalem Datenverkehr entgehen. FortiGuard Threat Intelligence hilft Unternehmen, diese komplexen Bedrohungen zu bekämpfen, indem Echtzeitdaten über neu erkannte Bedrohungen direkt an ihre Sicherheitslösungen geliefert werden, während Fortinet-Sandboxing-Lösungen unbekannte Bedrohungen erkennen und dann alle verdächtigen Dateien, die von Geräten innerhalb der Security Fabric erkannt werden, isolieren und überprüfen.
- Management und Analytics . In einem großen und äußerst elastischen Netzwerk sind Sichtbarkeit und Kontrolle wichtiger als jemals zuvor. IT-Teams müssen in der Lage sein, Bedrohungen und Ereignisse zu erkennen und zu verstehen, unabhängig davon, an welcher Stelle innerhalb des verteilten Netzwerks sie auftreten. Dies kann jedoch eine große Herausforderung für Unternehmen sein, die isolierte Security-Produkte implementiert haben. Fortinet-Lösungen für Protokollierung und Berichterstellung, SIEM und zentralisiertes Security Management erfassen Daten von Ihren Fortinet- und Fabric-Ready Security-Produkten, setzen diese in Beziehung und liefern so die kritische Sichtbarkeit und engmaschige Kontrolle, die erforderlich ist, um Security-Prozesse zu verwalten und automatisierte Reaktionen zu orchestrieren.

EINE LÖSUNG FÜR DAS MODERNE DIGITALE UNTERNEHMEN

Die digitale Transformation ist die größte Herausforderung, der sich IT-Security-Teams jemals gegenübersahen. Da die Entwicklung im Bereich Computer und Netzwerke fortschreitet und weiterhin über alle kritischen Geschäftsinfrastrukturen, Architekturen und Geschäftspraktiken hinweg für Veränderungen sorgt, brauchen Unternehmen einen innovativen Security Transformation-Ansatz, damit sie mit diesen Veränderungen Schritt halten können.

Wenn bislang isolierte Sicherheitslösungen in einem einheitlichen Security Fabric Framework integriert sind, können Unternehmen tief in das verteilte Netzwerk blicken und komplexe Bedrohungen erkennen. Sie können sich dynamisch an die sich entwickelnde Architektur und Bedrohungslandschaft anpassen und die kontinuierlichen Gefahrenbewertungen nutzen, die das moderne digitale Unternehmen braucht – von der innersten Netzwerkschicht bis in die Cloud.

Klicken Sie hier, wenn Sie mehr darüber erfahren möchten, was die Fortinet Security Fabric für Ihr Unternehmen leisten kann.

DEUTSCHLAND
Feldbergstraße 35
60323 Frankfurt
Deutschland
Telefon: +49 69 310 192 0

SCHWEIZ
Riedmuehlestr. 8
CH-8305 Dietlikon/Zürich
Schweiz
Telefon: +41 44 833 68 48

ÖSTERREICH
Wienerbergstrasse 11
Turm A
9.OG, 1100 Wien
Österreich
Verkaufsabteilung:
Telefon: +43 1 3760013 - 0

HAUPTSITZ
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
USA
Tel.: +1 408 235 7700
www.fortinet.com/sales

VERTRIEBSBÜRO
EMEA
905 rue Albert Einstein
06560 Valbonne
Frankreich
Tel.: +33 4 8987 0500

VERTRIEBSBÜRO
APAC
300 Beach Road 20-01
The Concourse
Singapur 199555
Tel.: +65 6513 3730

LATEINAMERIKA
ZENTRALE
Sawgrass Lakes Center
13450 W. Sunrise Blvd.,
Suite 430
Sunrise, FL 33323
Tel: +1 954 368 9990

171575-A-0-EN
Juli 13, 2018 10:29 vorm.