VMWARE WORKSPACE ONE TRUST NETWORK

Sicherheit bei der Weiterentwicklung des digitalen Arbeitsplatzes

AUF EINEN BLICK

VMware Workspace ONE™ Trust Network™ bietet Unternehmen einen umfassenden und modernen Ansatz für Enterprise-Sicherheit im Hinblick auf Mitarbeiter, Anwendungen, Endpunkte und Netzwerke. Mit Funktionen zum Schutz vor modernen Bedrohungen sowie zu deren Erkennung und Beseitigung erweitert Workspace ONE Trust Network die inhärenten Sicherheitsfunktionen der informationsgesteuerten Workspace ONE-Plattform. Dies geschieht mithilfe zahlreicher Partner, deren integrierte Lösungen kontinuierliche Risikoüberwachung und schnelle Eindämmungsreaktionen für den gesamten digitalen Arbeitsplatz gewährleisten.

DIE WICHTIGSTEN VORTEILE

Workspace ONE Trust Network vereinfacht Sicherheit und Management mit einem Framework aus Vertrauenswürdigkeit und Verifizierung. Das ermöglicht Workspace ONE Trust Network IT-Organisationen:

- Abschaffung isolierter Sicherheitslösungen dank eines aktionsbasierten Frameworks, das eine zusammengefasste Ansicht des gesamten digitalen Arbeitsplatzes bietet und Komplexität reduziert
- Einzigartige Kombination von Zugriffs-, Geräte- sowie Anwendungssicherheit und -management mit Informationen und Automatisierung zur Risikominimierung beim End-User Computing
- Offenes und bewährtes Partnernetz, Kosteneinsparung durch Nutzung vorhandener Investitionen

Sicherheit – die größte Herausforderung einer modernen Strategie für digitale Arbeitsplätze

Ein digitaler Arbeitsplatz kann die Mitarbeiterproduktivität um das Fünffache[1] steigern. Er ermöglicht Mitarbeitern den einfachen und sicheren Zugriff auf Anwendungen und Daten über das Gerät ihrer Wahl. Die digitale Transformation ist weiter auf dem Vormarsch und digitale Arbeitsplatzsysteme mit Mitarbeitern, Anwendungen, Endpunkten und Netzwerken entwickeln sich über herkömmliche Perimeter hinaus – mit Trends wie der Umstellung auf BYOD-Programme und der Konsumerisierung der IT. Und die Auflösung des herkömmlichen Perimeters schafft Raum für neue raffinierte Cyberbedrohungen wie Zero-Day-Angriffe, Man-in-the-Middle-(MiTM-) Angriffe, Phishing, Bots und Ransomware.

Sicherheit ist der Hauptmotivator für Investitionen in Mobilitätslösungen und in den digitalen Arbeitsplatz[2]. Aber vorhandene Sicherheitstools mit Legacy-Funktionen bieten der IT nur begrenzte Sichtbarkeit und isolierte Sicherheitsstrukturen. Das Ergebnis sind provisorische Lösungen zur Absicherung des digitalen Arbeitsplatzes, die teuer, komplex und arbeitsaufwendig sind. Aus diesem Grund ist die Sicherheit die größte Herausforderung bei der Umstellung auf eine moderne Strategie für den digitalen Arbeitsplatz.

Umfassende und prädiktive Sicherheit im perimeterlosen Unternehmen

Es müssen neue Sicherheitsanforderungen erfüllt werden, ohne dabei die Anwendererfahrung zu beeinträchtigen:

1. Für eine zusammengefasste Ansicht benötigen Unternehmen ein Framework, das Vertrauenswürdigkeit zwischen den Sicherheitskomponenten ihres Systems schafft.
2. Und zur kontinuierlichen Risikominimierung müssen Umgebungsdaten erfasst werden, die aussagekräftige und automatisierte Entscheidungen bezüglich der Sicherheit des digitalen Arbeitsplatzes zulassen.

Workspace ONE Trust Network bietet Unternehmen einen umfassenden und modernen Ansatz für Enterprise-Sicherheit im Hinblick auf Mitarbeiter, Anwendungen, Endpunkte und Netzwerke. Die Funktionen von Workspace ONE Trust Network zum Schutz, zur Erkennung und zur Beseitigung von Bedrohungen für das sich entwickelnde digitale Arbeitsplatzsystem basieren auf einem Framework von Vertrauenswürdigkeit und Verifizierung. Und mit der richtigen Vertrauenszone für den gesamten digitalen Arbeitsplatz können Mitarbeiter risikolos in einem vernetzten System mit minimalen Zugriffsrechten arbeiten. Dabei „folgt“ ihnen die Sicherheit. Zur Handhabung der Risiken moderner Cyberbedrohungen kombiniert Workspace ONE Trust Network Daten aus der informationsgesteuerten Workspace ONE-Plattform mit bewährten Sicherheitslösungen von Partnern und bietet so prädiktive und automatisierte Sicherheit für den digitalen Arbeitsplatz.

1 Quelle: https://www.vmware.com/radius/impact-digital-workforce/

2 CCS Insights: Mobile Technology Buyer Survey, Dezember 2017

Schutz, Erkennung und Behebung

Kein Unternehmen ist gegen Cyberangriffe immun. Aber IT-Ops- und Sicherheitsteams können Cyber-Security-Risiken in Schach halten, indem sie die Zuordnung der Sicherheitsfunktionen eines Frameworks wie zum Beispiel NIST Cybersecurity Framework zu den Funktionen von Workspace ONE Trust Network vereinfachen:

- Der Schutz des digitalen Arbeitsplatzes mit Sicherheitsfunktionen beginnt beim Schutz vor Malware durch maschinelles Lernen, bei der Verhinderung von Datenexfiltration aus Cloud-basierten Unternehmensanwendungen und bei der Mikrosegmentierung von Netzwerken zum Schutz vor fortgeschrittenen, andauernden Bedrohungen (Advanced Persistent Threats, APT).
- Bedrohungen werden durch eine kontinuierliche und adaptive Überwachung des digitalen Arbeitsplatzes erkannt. IT-Abteilungen und Sicherheitsteams haben somit die Möglichkeit, Bedrohungen auf Mobilgeräten, Desktops und in Anwendungen aufzuspüren.
- Und Workspace ONE Trust Network ermöglicht eine automatisierte Behebung erkannter Bedrohungen auf Basis eines leistungsstarken Entscheidungsmoduls. Wenn zum Beispiel aufgrund von Anomalien ein Angriff erkannt wird, kann eine automatisierte Richtlinie zur Blockierung des Zugriffs auf Unternehmensdaten in Kraft gesetzt werden.

Einheitliches Management der Zugriffs-, Geräte- und Anwendungssicherheit mit Analysefunktionen

Workspace ONE Trust Network kombiniert die Sicherheitsfunktionen der informationsgesteuerten Workspace ONE-Plattform (Zugriffs-, Geräte- und Anwendungssicherheit) mit Analysefunktionen, sodass durch isolierte Sicherheitslösungen entstandene Managementsilos zusammengeführt werden. Der Workspace ONE Intelligence-Service stellt Analysefunktionen auf der Workspace ONE-Plattform bereit. Das ermöglicht die Aggregation und Korrelation von Arbeitsplatzdaten mit Empfehlungen für integrierte Informationen und Automatisierung. Die Integration der Workspace ONE Trust Network-Funktionen in den Intelligence-Service bietet Unternehmen eine kontinuierliche Überwachung auf Sicherheitsrisiken in der perimeterlosen Datenwelt von heute. Und falls ein Risiko erkannt wird, erfolgt eine schnelle Reaktion.

Mithilfe eines Entscheidungsmoduls werden Informationen korreliert. Das sind zum Beispiel Daten zum Anwenderverhalten auf Unternehmensgeräten außerhalb des Netzwerks, sodass Bedrohungen erkannt und mit automatisierten Richtlinien zur Beschränkung des Datenzugriffs unschädlich gemacht werden können. Bessere Sicherheit für den digitalen Arbeitsplatz: Erkennen und mindern Sie Sicherheitsprobleme in Echtzeit mit integrierten Erkenntnissen zu Bedrohungsdaten und detailliertem Compliance-Gerätestatus. Mit dem Entscheidungsmodul kann die IT Regeln zur Automatisierung und Optimierung häufiger Aufgaben erstellen, beispielsweise die Installation wichtiger Patches für Windows 10-Endpunkte oder die Einrichtung von Kontrollen für den bedingungsbasierten Zugriff auf Anwendungen und Services für Gruppen oder einzelne Anwender.

Umfangreiches Partnernetz mit vertrauenswürdigen Lösungen

Ein umfassender Sicherheitsansatz für digitale Arbeitsplatzumgebungen, die sich ständig weiterentwickeln, ist nur möglich, wenn zwischen den einzelnen Komponenten eine Vertrauensbasis vorhanden ist. Workspace ONE Trust Network bietet dieses Vertrauens-Framework mit APIs auf Basis der Workspace ONE-Plattform. Dank dieser APIs können die Sicherheitslösungen unseres umfangreichen Partnernetzwerks mit Workspace ONE kommunizieren. Das ermöglicht letztlich die zusammengefasste Ansicht, die Administratoren für eine Vereinfachung von Sicherheit und Management brauchen. Isolierte Sicherheitslösungen werden vernetzt. So haben Kunden die Möglichkeit, ihre vorhandenen Investitionen zu nutzen, um die kontinuierliche Überwachung und Risikoanalyse exponentiell zu verbessern und schneller auf Bedrohungen reagieren zu können. Das Ergebnis: eine prädiktive Sicherheitsstrategie, die auf Trends und Mustern basiert und mit der Umgebung wächst.

WEITERE INFORMATIONEN

Weitere Informationen zu Workspace ONE Trust Network finden Sie auf unserer Website: www.vmware.com/products/de/workspace-one/security

Kostenlos in einem Hands-on Lab testen: https://www.vmware.com/go/workspace-hol

WENN SIE EIN VMWARE-PRODUKT ERWERBEN MÖCHTEN ODER WEITERE INFORMATIONEN BENÖTIGEN,

SETZEN SIE SICH UNTER DER FOLGENDEN TELEFONNUMMER DIREKT MIT VMWARE IN VERBINDUNG:
0800 100 6711.

SIE KÖNNEN AUCH UNSERE WEBSITE UNTER
http://www.vmware.com/de/products
besuchen oder online nach einem autorisierten Händler suchen.

Hauptfunktionen

Mit Workspace ONE Trust Network profitieren Unternehmen von diesen wichtigen Sicherheitsfunktionen zum Schutz vor sich ständig weiterentwickelnden Cyberbedrohungen sowie zu deren Erkennung und Beseitigung.

FUNKTION	BESCHREIBUNG
Eine Basisplattform für den digitalen Arbeitsplatz, die Sicherheitslösungen verbindet	Vereinfachen Sie Sicherheit und Management mithilfe eines Vertrauens-Frameworks und APIs für die Kommunikation zwischen einem offenen Partnernetz aus Sicherheitsanbietern und Workspace ONE.
Zugriffsmanagement, das Ihr Business vereinfacht	Ermöglichen Sie der IT Anwendungs-Provisioning sowie die Bereitstellung eines Self-Service-Katalogs, Mehrfach-Authentifizierung und Single Sign-On (SSO) für alle Anwendungen.
Optimierte Anwendererfahrung und Sicherheit durch kontextbezogene Richtlinien	Steuern Sie die Authentifizierung mit Richtlinien für bedingungsabhängigen Zugriff anhand des Compliance-Gerätestatus, der Stärke der Anwenderauthentifizierung, der Datensensibilität, des Anwenderstandorts und weiterer Kriterien.
Data Loss Prevention- (DLP-) Richtlinien zur Vermeidung von Datenverlust	Sie profitieren von Verschlüsselung auf Geräteebene, Datenverschlüsselung und Hardwaresicherheitsrichtlinien. Zu den konfigurierbaren Richtlinien zählen Blacklists für Anwendungen, Gerätekopplung, WLAN-Sicherheit und TLS-Erzwingung. Überwachen Sie Bedrohungen wie Malware, schädliche Anwendungen, In-Memory-Angriffe und Jailbreaking-Geräte und beheben Sie Bedrohungen automatisch – mit Funktionen wie Remote-Sperren, Gerätelöschung, Zugriffssperren oder anpassbaren Quarantänekontrollen für Geräte.
Sichere Anwendungen ohne Kompromisse bei der Anwendererfahrung	Nutzen Sie die Sicherheitskontrollen in den sicheren Produktivitätsanwendungen von VMware – VMware Boxer™, Browser™ und Content Locker™. Erkennen Sie Bedrohungen und automatisieren Sie deren Behebung für alle anderen Anwendungen und Cloud-Services.
Verschlüsselung von ruhenden Daten und Daten während der Übertragung	Authentifizieren und verschlüsseln Sie den Datenverkehr von Anwendungen auf Geräten im Rechenzentrum mit VMware Tunnel. Sichern Sie Anwendungsdaten bei der Speicherung und Übertragung mit AES-256-Bit-Verschlüsselung.
Netzwerkübergreifende Automatisierung von Sicherheit durch Mikrosegmentierung	Minimieren Sie die Angriffsfläche im Rechenzentrum durch Mikrosegmentierung mit VMware NSX® und automatisieren Sie die Sicherheit im gesamten Netzwerk.
Integrierte Informationen und Automatisierung für prädiktive Sicherheit	Erkennen und mindern Sie Sicherheitsprobleme in Echtzeit mit integrierten Erkenntnissen zu Bedrohungsdaten und detailliertem Compliance-Gerätestatus, die von Workspace ONE Intelligence geliefert werden.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com Zweigniederlassung Deutschland Freisinger Str. 3 85716 Unterschleißheim/Lohhof Telefon: +49 89 370 617 000 Fax: +49 89 370 617 333 www.vmware.com/de