Symantec by Broadcom | Carbon Black. by Broadcom | ARROW

GUIDE

Ein praktischer Leitfaden

Sicherheit und Ausfallsicherheit mit Symantec ZTNA

Ihr virtuelles privates Netzwerk (VPN) verspricht sicheren Fernzugriff, aber was es tatsächlich anbietet, ist eine offene Tür zu Ihrem Netzwerk. Herkömmliche VPNs gehen davon aus, dass jeder innerhalb des Netzwerkperimeters vertrauenswürdig ist, und das ist ein Problem. Dadurch wird jeder Auftragnehmer, Partner und Drittanbieter zu einem potenziellen Angriffsvektor.

Wenn Angreifer die Anmeldedaten eines einzelnen Auftragnehmers kompromittieren, greifen sie nicht nur auf eine Anwendung zu, sondern können sich frei in Ihrem gesamten Netzwerk bewegen. Jüngste, viel beachtete Sicherheitsverletzungen haben gezeigt, dass der Zugriff durch Dritte zum Schwachpunkt der Unternehmenssicherheit geworden ist.

Symantec Zero Trust Network Access (ZTNA) geht diese Rechnung nicht mehr auf. Blindes Vertrauen wird durch kontinuierliche Überprüfung und der netzwerkweite Zugriff wird durch präzise, anwendungsspezifische Verbindungen ersetzt.

Darum sollten Sie sich jetzt mit dem Problem des Zugriffs durch Dritte befassen

Herkömmliche VPNs gewähren standardmäßig vollständigen Netzwerkzugriff, da sie nicht vorhersagen können, welche Anwendungen die Benutzer benötigen werden. Dieser „Alles-oder-nichts"-Ansatz bedeutet, dass ein Remote-Mitarbeiter, Berater oder Auftragnehmer, der mit der Aktualisierung Ihrer Website beauftragt wurde, potenziell Zugriff auf Ihre Finanzsysteme, Kundendatenbanken und Ihr geistiges Eigentum erhalten kann. Schwachstellenscans und Mapping-Techniken legen Ihre gesamte Netzwerktopologie für jeden offen, der über grundlegende Anmeldedaten verfügt.

Eine Sichtbarkeitslücke verstärkt dieses Risiko zusätzlich. Wichtige Daten für Compliance und Reaktion auf Vorfälle sind über mehrere Server, Geräte und Standorte in unterschiedlichen Formaten verteilt. Dadurch haben Sicherheitsteams bei der Reaktion auf Vorfälle Schwierigkeiten, an Informationen zu gelangen, da die Aktivitäten der Benutzer über getrennte Systeme verlaufen. Man kann nicht verteidigen, was man nicht sehen kann.

Der BYOD-Zugang (Bring-your-own-Device) stellt ein weiteres Problem dar. Auftragnehmer und Partner bringen häufig ihre eigenen Geräte mit. Möglicherweise erlauben die Unternehmensrichtlinien nicht, dass diese Geräte Ihr VPN verwenden, oder Ihr VPN unterstützt sie einfach nicht.

Schließlich bedeutet VPN-Unterstützung den Einsatz komplexer DMZ-Konfigurationen und Firewall-Regeln, die IT-Ressourcen beanspruchen. Dies zwingt den Datenverkehr außerdem durch zentrale Rechenzentren, wodurch Engpässe entstehen, die die Remote-Arbeit beeinträchtigen.

Resilienz aufbauen mit ZTNA

Zero Trust kehrt die Netzwerk-Sicherheit um. Anstatt davon auszugehen, dass jeder innerhalb des Perimeters vertrauenswürdig ist, funktioniert er nach einem einfachen Prinzip: Niemals vertrauen, immer überprüfen.

Jede Zugriffsanfrage wird unter ZTNA einer genauen Prüfung unterzogen. Systeme bewerten die Identität des Benutzers, den Zustand des Geräts, den Standort, die Authentifizierungsmethode und sogar die spezifische Anwendungs-URI in einer Zugriffsanfrage.

Dieser softwaredefinierte Perimeter-Ansatz zielt darauf ab, einzelne Anwendungen zu schützen und sie vollständig vor unbefugten Benutzern zu verbergen. Es folgt einem Zugriffsmodell mit „minimalen Berechtigungen" und erlaubt nur den Zugriff auf Anwendungen, für die der Benutzer eine Berechtigung hat.

Symantec ZTNA ersetzt den breiten Netzwerkzugriff durch Punkt-zu-Punkt-Verbindungen und schafft so sichere Tunnel zwischen bestimmten Benutzern und bestimmten Anwendungen. Dies bietet drei wesentliche Vorteile:

Leistung

Punkt-zu-Punkt-Konnektivität beseitigt Engpässe und reduziert Latenzzeiten. Die Tests von Symantec zeigten, dass Nutzer im Vergleich zu herkömmlichen VPN-Verbindungen um 62 % schnellere Transaktionszeiten verzeichnen konnten. Und mit Symantec ZTNA auf Google Cloud dürfen Benutzer eine schnellere Leistung und verbesserte Skalierbarkeit erwarten, die allen Benutzeranforderungen gerecht wird.

Security

ZTNA begrenzt den Ausbreitungsradius einer Kompromittierung, da er nicht autorisierte Teile des Netzwerks vor dem Benutzer verbirgt. Wenn ein Angreifer eine Anmeldeinformation kompromittiert, erhält er Zugriff auf genau eine Anwendung und nichts weiter. Querbewegungen sind unmöglich, wenn es kein Netzwerk gibt, durch das man sich bewegen kann.

Resilienz

Die Systeme von Symantec nutzen die Google Cloud-Infrastruktur, um drei Verfügbarkeitszonen pro Präsenzpunkt und ein One-Click-Failover in allen Regionen weltweit bereitzustellen. Dadurch bleiben sie auch bei Naturkatastrophen betriebsbereit.

Sicherheit und Ausfallsicherheit mit Symantec ZTNA

Ihr Stufenplan zur ZTNA-Implementierung

Die Implementierung von ZTNA muss nicht unbedingt Störungen mit sich bringen. Symantec empfiehlt, in drei Phasen vorzugehen, um die Vorteile zu nutzen und Funktionen bereitzustellen, die ein VPN nicht bieten kann.

Phase 1 – Bereitstellung von Zugriff mit minimalen Berechtigungen für Remote-Benutzer

Das Modell des minimalen Zugriffsrechts von Symantec ZTNA gewährt jedem Benutzer nur Zugriff auf die Anwendungen, für deren Nutzung er berechtigt ist. Diese Anwendungen sind vor dem Rest des Netzwerks abgeschirmt, wodurch böswilliger oder unbeabsichtigter Zugriff auf sensible Anwendungen und Daten verhindert wird.

Beginnen Sie mit Ihren Remote-Mitarbeitern, wie etwa Mitarbeiter, die von zu Hause aus arbeiten, Außendienstmitarbeiter und dezentrale Mitarbeiter, die einen sicheren Zugriff auf Anwendungen benötigen. Diese Benutzer stellen Ihre größte Angriffsfläche dar und haben den größten Einfluss auf die Produktivität. Aktivieren Sie den agentenbasierten Zugriff für verwaltete Geräte und den agentenlosen Zugriff für BYOD-Szenarien. Symantec ZTNA unterstützt Webanwendungen, natives SSH für DevOps-Teams, RDP für Remote-Desktops und TCP für Legacy-Anwendungen.

Sobald Mitarbeiter einen sicheren Zugang haben, erweitern Sie denselben Schutz auf Auftragnehmer, Partner und Lieferanten. Dieser Ansatz bewährt sich schnell bei Ihren Kernnutzern und berücksichtigt gleichzeitig Risiken durch Dritte. Er eignet sich auch für Fusionen und Übernahmen, da das neue Unternehmen während des Vorgangs möglicherweise auf die Ressourcen der Muttergesellschaft zugreifen muss.

Ihr bestehendes VPN kann während dieser Umstellung weiterlaufen, sodass keine Unterbrechungen auftreten, während Sie das Zero-Trust-Modell validieren.

Phase 2 – Die Sicherheitskontrollen durch Hinzufügen von Schutzmaßnahmen gegen Bedrohungen und zum Schutz von Daten verbessern

In dieser Phase kommen Bedrohungs- und Datenschutz hinzu. VPNs bilden eine Sicherheitslücke. Sie können den Datenverkehr nicht auf Bedrohungen überprüfen oder Datenschutzrichtlinien durchsetzen.

Symantec ZTNA ändert dies grundlegend. Jede Verbindung zu privaten Anwendungen wird nun genauso auf Sicherheit überprüft wie jeder andere Datenverkehr. Symantec ZTNA lässt sich direkt in den Symantec Threat Intelligence Service integrieren, der alle Dateien auf Malware und schädliche Inhalte überprüft, sowie in Web Isolation, das Benutzer automatisch vor unbekannten oder verdächtigen Websites schützt.

Symantec ZTNA synchronisiert sich zudem mit Symantec Data Loss Prevention (DLP), sodass alle bestehenden DLP-Richtlinien auf den ZTNA-Datenverkehr angewendet werden können. Dadurch wird gewährleistet, dass dieselben Schutzmaßnahmen und Einschränkungen durchgesetzt werden.

Phase 3 – ZTNA im gesamten Unternehmen einführen

In dieser Phase wird Symantec ZTNA nicht nur für Remote-Benutzer, sondern für das gesamte Unternehmen bereitgestellt. Er bietet allen, einschließlich den Mitarbeitern vor Ort, eine sicherere Methode für den Zugriff auf Anwendungen und Ressourcen.

Mit Symantec ZTNA schützen dieselben Compliance-Regeln, die für SaaS und den Webzugriff gelten, nun auch interne Anwendungen. Die Verkehrsüberprüfung erfolgt in der Cloud, ohne Proxys einzusetzen oder Backhauling über Rechenzentren durchzuführen.

Dies gewährleistet einen konsistenten Schutz, unabhängig davon, ob Benutzer auf Cloud- oder lokale Ressourcen zugreifen. Richtlinien auf Anwendungsebene stellen sicher, dass alle Benutzer nur das sehen, wozu sie berechtigt sind, während alles andere verborgen und unsichtbar bleibt. Jeder Zugriffsversuch generiert zentralisierte Audit-Protokolle, die Ihnen die Transparenz bieten, die VPNs nicht bieten konnten.

Außerdem können Sie einen einzigen Agenten einsetzen, der ZTNA zusammen mit bestehenden Symantec-Tools wie Cloud SWG, Cloud Access Security Broker, DLP und Web Isolation verwaltet. Dies vereinfacht die Bereitstellung und Verwaltung erheblich, da ein einziger Agent für mehrere verschiedene Anwendungsfälle eingesetzt werden kann.

Sobald Sie positive Ergebnisse bemerken, können Sie Ihre VPN-Infrastruktur auslaufen lassen. Es ist kein Zufall, dass 80 % der Konzeptpilotprojekte zu Käufen führen.

Sicherheit und Ausfallsicherheit mit Symantec ZTNA

Die Vorteile der SSE für moderne Unternehmen erkennen

Die Konsolidierung beseitigt die unübersichtliche Vielzahl an Tools. Die Kombination von ZTNA mit Cloud SWG und DLP/CASB im Rahmen des Security Service Edge (SSE)-Frameworks stärkt, optimiert und vereinfacht Ihre Sicherheitsabläufe.

Kunden von Symantec SWG verfügen bereits über eine wichtige Komponente eines Zero-Trust-Frameworks. Jetzt können sie es nahtlos in ZTNA integrieren und dabei denselben Agenten, dieselbe Verwaltungskonsole und dasselbe Richtlinien-Framework nutzen.

Die operativen Vorteile liegen auf der Hand:

Schnelle Bereitstellung

Das System in wenigen Minuten statt in Wochen einführen.

Alles schützen

Der Threat Intelligence Service und die Remote Browser Isolation von Symantec funktionieren in allen Diensten und bieten einheitlichen Schutz vor Malware und neuen Bedrohungen.

Verwaltung vereinfachen

Verwalten Sie einen einzigen Sicherheits-Stack, anstatt sich mit mehreren Anbietern mit unterschiedlichen Schnittstellen, Lizenzmodellen und Supportprozessen herumzuschlagen.

Fazit

Die Bereitstellung von ZTNA ist eine effektive Maßnahme, um Transformationsrisiken zu beseitigen. Es geht nicht nur darum, Geld zu sparen (obwohl die Reduzierung der Anzahl der Anbieter sicherlich zum Budget beiträgt). Es geht darum, eine Sicherheitsarchitektur aufzubauen, die mit Ihrem Unternehmen mitwächst und dabei die Komplexität reduziert.

Unternehmen, die sich mit „ausreichend guten“ VPNs begnügen, gehen unnötige Risiken ein. Die Technologie, um Querbewegungen zu eliminieren, den Zugriff durch Dritte zu sichern und gleichzeitig die Benutzererfahrung und Leistung zu verbessern, ist heute bereits verfügbar.

Die Frage ist nicht, ob Zero Trust Network Access implementiert werden soll, sondern wie schnell Sie dies umsetzen können.