



3 Schritte zum SSE-Erfolg

Ein einfacher Leitfaden zur Sicherung von Arbeitskräften an jedem Ort und zu jeder Zeit

Inhalt

4 Der Ausgangspunkt: Warum SSE?

5 Bestandteile von SSE

5 Bewährte Methoden für den SSE-Erfolg

6 Schritt 1: Planen

6 Schritt 2: Ausführen

7 Schritt 3: Überprüfen

8 Auf dem Erfolg von SSE aufbauen

9 Mehr erfahren



In einer IT-Welt, in der Unternehmen-ressourcen über mehrere Cloud-Anbieter und verteilte interne Systeme verteilt sind – und Benutzer von überall aus eine Verbindung herstellen können – sind herkömmliche Sicherheitsansätze aufgrund begrenzter Skalierbarkeit, neuer Sicherheitslücken, verminderter Leistung und anderer Mängel nicht mehr so praktikabel wie früher.

Die Worte „irgendwo“ und „überall“ sind für die CISOs von heute vielleicht die furchterregendsten.

Für sich genommen mögen sie harmlos klingen. Aber sie sind ein großes Warnsignal für die Gewährleistung der IT-Sicherheit im Unternehmen. Eine kürzlich durchgeführte Umfrage hat ergeben, dass 94% der Unternehmen heute nach einem Remote- oder Hybridmodell arbeiten.¹

Im Gegensatz zur klar definierten IT-Umgebung von vor ein paar Jahren, die hauptsächlich aus in sich geschlossenen Ressourcen und eindeutigen Zugriffspunkten bestand, müssen CISOs heute Unternehmensressourcen schützen, die sich überall befinden können, und gleichzeitig den Zugriff von überall her ermöglichen.

Darüber hinaus hat die zunehmende Komplexität der IT in den Unternehmen neue Sicherheitsrisiken mit sich gebracht. Gleichzeitig haben die Veränderungen, die sich aus der Einführung von Cloud-Diensten, der zunehmenden Zahl dezentraler und mobiler Mitarbeiter und der Abhängigkeit von SaaS-basierten Lösungen ergeben, die IT-Sicherheit schwieriger, kostspieliger und zeitaufwändiger gemacht.

Daher gehen viele Unternehmen zu einem Security Service Edge (SSE) Ansatz über. SSE ist eine Untergruppe von Secure Access Service Edge (SASE) und besteht aus einer Kombination von Cloud-basierten Sicherheitsdiensten. Damit können Unternehmen Anwendern an beliebigen Standorten uneingeschränkten Zugang zu Unternehmensressourcen und -diensten gewähren – und zwar auf sichere Weise und ohne Risiko. Mit einem SSE-Ansatz können Sicherheitsteams einen verbesserten Schutz für die mobilen und Cloud-orientierten Umgebungen von heute bereitstellen – mit größerer Skalierbarkeit und Flexibilität, geringerer Komplexität, besserer Leistung, Kosteneffizienz und vielem mehr.

So erfreulich all dies auch ist, diese Vorteile kommen erst zum Tragen, wenn die Unternehmen die ersten Schritte in Richtung SSE unternehmen. Deshalb haben wir diese Roadmap für Unternehmen zusammengestellt, die sich selbstbewusst und schrittweise auf den Weg zu SSE machen wollen. Mit dem richtigen Ansatz können CISOs und Unternehmen die herkömmliche Unternehmenssicherheit so umgestalten, dass sie den komplexen IT-Herausforderungen von heute gerecht wird und gleichzeitig eine sichere, kosteneffiziente Grundlage für künftiges Wachstum und Flexibilität bietet.

Dieses Dokument bietet eine Anleitung zur beschleunigten SSE-Implementierung und einen Blueprint für langfristigen Erfolg.

¹ 2024 SSE Adoption Report, Cybersecurity Insiders



Der Ausgangspunkt: Warum SSE?



SSE Übersicht

SSE-Lösungen bestehen normalerweise aus einer Kombination wichtiger Dienste, darunter Zero Trust Network Access (ZTNA), Secure Web Gateway (SWG), Cloud Access Security Broker (CASB) und integriertes Digital Experience Monitoring (DEM). Die Dienste arbeiten zusammen, können aber auch für einen schrittweisen SSE-Ansatz separat eingesetzt werden.

Das große Interesse von CISOs und IT-Sicherheitsverantwortlichen an SSE ist vor allem auf zwei Dinge zurückzuführen: Veränderungen in der IT-Landschaft von Unternehmen und die Vorteile von SSE.

- **Veränderungen in der Unternehmens-IT.** Jahrelang funktionierten traditionelle, netzwerkzentrierte Sicherheitsansätze wie virtuelle private Netzwerke (VPNs) in konventionellen IT-Umgebungen von Unternehmen, in denen sich die meisten Anwendungen, Dienste, Daten und sogar Benutzer physisch innerhalb der Unternehmenseinrichtungen befanden, recht gut.

Diese Ansätze erwiesen sich jedoch als weit weniger praktikabel, als sich die Unternehmenslandschaft in den letzten fünf Jahren weiterentwickelte. Die rasche Umstellung auf Cloud Computing und Multi-Cloud-Ressourcen erfordert von den Unternehmen eine integrierte Sicherheit innerhalb und außerhalb ihrer physischen Standorte. Das Streben nach mehr mobilen Verbindungen und vermehrter Remote-Arbeit erfordert Sicherheit von jedem Ort aus und eine erhöhte Sicherheit der Unternehmensressourcen. Angesichts der zunehmenden Komplexität von Geschäftsumgebungen und Sicherheitsrisiken ist die Durchsetzung konsistenter Sicherheitsrichtlinien im gesamten Unternehmen heute wichtiger denn je. Mehrere andere übergreifende Trends tragen ebenfalls zu diesem Wandel bei. Dazu gehören die zunehmende Bedrohung der Cybersicherheit, der Übergang zu Zero Trust- Sicherheitsmodellen, die verstärkte Einhaltung gesetzlicher Vorschriften sowie die Notwendigkeit von Kosteneffizienz und besserer Benutzerfreundlichkeit.

- **Vorteile von SSE.** Ein SSE-Ansatz bietet eine Reihe bedeutender Vorteile. SSE erhöht die Gesamtsicherheit durch Zero Trust-Zugriff für alle Unternehmensanwendungen – egal, ob es sich um private, öffentliche, Cloud-basierte oder im Rechenzentrum bereitgestellte Anwendungen handelt. SSE verbessert die Compliance und das Risikomanagement durch die automatische und kontinuierliche Überprüfung und Durchsetzung von Sicherheitsrichtlinien. Dadurch wird die sichere Remote-Arbeit von überall aus machbar, handhabbar und effizient. Dieser Ansatz vereinfacht das Sicherheitsmanagement und die Verwaltung, erleichtert die Überwachung und zentralisiert gleichzeitig die Sichtbarkeit und Kontrolle. SSE verbessert außerdem das Benutzererlebnis, indem es Zugriffs- und Sicherheitsprozesse rationalisiert, Verbindungen optimiert und die Benutzerproduktivität steigert.

Zwar gibt es viele potenzielle Anwendungsmöglichkeiten für SSE, aber einige der typischen Anwendungsfälle, die für Unternehmen anfangs interessant sind, sind folgende:

- Sichere Unterstützung von Remote- und mobilen Mitarbeitern überall
- Schutz und Sicherung von Daten und Diensten überall
- Sicherung aller Cloud- und Webzugriffe
- Verbesserung der allgemeinen Cybersicherheitslage bei gleichzeitiger Reduzierung der Bedrohungslage



Bestandteile von SSE

Zero Trust Network Access (ZTNA). ZTNA stellt eine enorme Verbesserung gegenüber dem herkömmlichen VPN-Zugriff auf private Anwendungen dar, da es den Anwendungszugriff auf Remote-Benutzer ausweitet und nach der Authentifizierung nur den Zugriff auf autorisierte Ressourcen erlaubt. ZTNA stellt im Wesentlichen sicher, dass keinem Benutzer oder Gerät standardmäßig vertraut wird. Stattdessen müssen alle Benutzer und Geräte robuste Identitätsüberprüfungsprozesse durchlaufen, um Zugriff auf entsprechende Ressourcen zu erhalten. Darüber hinaus wird das Prinzip der geringsten Zugriffsrechte angewandt, d. h. die Benutzer können nur auf die von den Administratoren genehmigten Anwendungen und Daten zugreifen.

Secure Web Gateway (SWG). SWG ist ein zentraler SSE-Dienst, der den Internetzugang verwaltet, indem er Unternehmensrichtlinien anwendet und verhindert, dass unerwünschter und unbekannter Internetverkehr in das interne Netzwerk eines Unternehmens gelangt. SWG schützt Benutzer vor dem Zugriff auf bösartige Websites, aus dem Internet eingeschleuste Viren und Malware und ermöglicht ihnen gleichzeitig den Zugriff auf Ressourcen, die sie für ihre Arbeit benötigen.

Cloud Access Security Broker (CASB). Ein CASB stellt eine Erweiterung der SSE-Sicherheitsfunktion dar. Es setzt die Sicherheitsrichtlinien für den Zugriff und die Vermeidung von Datenverlusten durch, wenn Benutzer und Dienste auf verschiedene Unternehmensressourcen zugreifen (ob Cloud-basiert, private Anwendungen usw.), und trägt zur Einhaltung der Sicherheitsrichtlinien des Unternehmens und der Branche bei.

Digital Experience Monitoring (DEM). Mit DEM können Unternehmen ein Benutzererlebnis bieten, das die Produktivität und Sicherheit ihrer Mitarbeiter gewährleistet. DEM überwacht die digitale Erfahrung der Benutzer, um sicherzustellen, dass das System mit Spitzen in der CPU-Auslastung, Netzwerkausfällen und Leistungsproblemen von Anwendungen umgehen kann. Gleichzeitig erhält die IT-Abteilung Einblicke und Messdaten zu jedem Internet- und Netzwerkschritt.

Bewährte Methoden für den SSE-Erfolg

Unabhängig von der Größe oder Branche Ihres Unternehmens sollten Sie beim Einstieg in den SSE-Bereich die folgenden Best Practices berücksichtigen:

- **Gehen Sie schrittweise vor.** SSE kann zwar überzeugende Vorteile bieten, aber was CISOs und Unternehmen in der Regel zu ersten Schritten in Richtung SSE ermutigt, ist die Tatsache, dass sie schrittweise zu SSE übergehen können. Ein schrittweiser Ansatz zur Einführung von SSE ist für viele Unternehmen am sinnvollsten. Aus diesem Grund handelt es sich um eine der besten Vorgehensweisen für den Erfolg von SSE.
- **Nutzen Sie kleine Teams und konzentrieren Sie sich auf spezifische Probleme.** An SSE interessierte Unternehmen sollten kleine Teams einsetzen und sich auf kritische Fragen in bestimmten Bereichen konzentrieren. Dadurch wird das Umfeld für schnelle Erfolge geschaffen und das Unternehmen kann von dort aus weiter ausbauen.
- **Vergessen Sie nicht die Benutzererfahrung.** Ein großer Teil einer erfolgreichen SSE-Einführung ist die Gewährleistung, dass sie den Benutzern das Leben leichter macht. Der beste Ansatz hierfür ist die Berücksichtigung von Sicherheit und Erfahrung im gleichen Maße und nicht die Vernachlässigung des einen Aspekts zugunsten des anderen. SSE-Teams sollten bei der Bewertung von Lösungskomponenten und -prozessen die „Blickwinkel der Mitarbeitenden“ verwenden.
- **Konzentrieren Sie sich zunächst auf einen SSE-Dienst.** Eine weitere wichtige Best Practice der SSE für einen schnellen Erfolg liegt darin, nicht mehr aufzunehmen als bewältigt werden kann. Das erste SSE-Projekt sollte wahrscheinlich nur einige Komponenten einer SSE-Plattform verwenden. Entscheidend ist, dass die Umstellung auf SSE in Angriff genommen wird und dann je nach Bedarf zusätzliche Funktionen oder Dienste hinzugefügt werden, die auf dem anfänglichen Erfolg aufbauen.

ZTNA ist eine ausgezeichnete Wahl für den ersten SSE-Dienst, da diese Technologie in der Regel mehrere dringende IT- und Geschäftsprobleme löst und gleichzeitig eine solide Grundlage für zusätzliche Anwendungsfälle in der Zukunft bietet.

- **Betrachten Sie ZTNA als ersten Schritt.** Zero Trust Network Access (ZTNA) kann für viele Unternehmen ein idealer Ausgangspunkt für den SSE-Erfolg sein. ZTNA ersetzt eine Technologie, die ursprünglich nicht für die heutigen Anforderungen an Remote- Arbeit und Drittanbieter-Zugriff konzipiert war. Dieser neue Ansatz kann unabhängig implementiert werden und stellt häufig eine sofortige Verbesserung gegenüber dem herkömmlichen VPN-Benutzererlebnis dar, während er gleichzeitig die Leistung steigert und die Sicherheitsrisiken drastisch reduziert.

Zur Umsetzung dieser Best Practices für SSE sollten Sie bei Ihrem ersten SSE-Projekt am besten in drei Schritten vorgehen: 1. Planen, 2. Ausführen und 3. Überprüfen.

In diesem Dokument wird zur Veranschaulichung eine ZTNA-Dienstimplementierung als erster SSE-Schritt verwendet. Ihr Unternehmen kann jedoch auch mit einer anderen SSE-Komponente beginnen, z. B. mit den Secure Web Gateways (SWGs), wenn dies besser zu Ihren Geschäftsanforderungen passt. Die allgemeinen Schritte zum Erfolg werden ähnlich sein.

Schritt 1: Planen

Der erste Schritt zum schnellen SSE-Erfolg ist die Planung. Zwar ist es sinnvoll, die strategischen Auswirkungen einer vollständigen SSE-Implementierung auf Ihre IT-Umgebung zu untersuchen. Es ist jedoch durchaus angebracht, bei der Planung einen taktischen Ansatz zu wählen, der auf dem anfänglich implementierten SSE-Dienst und dem zu lösenden Geschäftsproblem basiert.

Zu den grundlegenden Schritten für die Planung einer ersten SSE-Implementierung gehören:

- **Bewertung und Planung.** Beginnen Sie mit einer Bewertung der Sicherheitsinfrastruktur und -lage Ihres Unternehmens, um mögliche Mängel und potenzielle Anforderungen zu ermitteln. Wählen Sie dann einen anfänglichen Projektumfang aus, der den spezifischen Geschäfts- oder IT-Anforderungen entspricht. Für viele Unternehmen ist die Implementierung von ZTNA für eine bestimmte Gruppe, einen bestimmten Anwendungssatz, bestimmte Ressourcen oder Benutzer ein guter Ausgangspunkt. Diese anfängliche Planung konzentriert sich zwar auf taktische Ziele, sollte aber auch eine längerfristige Betrachtung der Sicherheits- und Geschäftsanforderungen beinhalten. Dies wird bei der Entscheidung für weitere Schritte und die Wahl des SSE-Anbieters hilfreich sein.
- **Anbietersauswahl.** Die Auswahl eines SSE-Anbieters ist ein wesentlicher Schritt auf Ihrem Weg zum SSE und wirkt sich direkt sowohl auf das anfängliche Projekt als auch auf Folgeprojekte aus. Nach der ersten Beurteilung und Planung muss Ihr Unternehmen potenzielle SSE-Anbieter anhand ihrer spezifischen Fähigkeiten und Eigenschaften sowie ihrer Übereinstimmung mit Ihren spezifischen IT- und Geschäftsanforderungen bewerten. Die Auswahl des SSE-Anbieters sollte auf der Grundlage der im vorherigen Schritt durchgeführten Bewertung und Planung erfolgen. Zu den zu berücksichtigenden Faktoren gehören u. a. funktionale Fähigkeiten, Ansehen, Kosten, Skalierbarkeit, Zeitplan, Integrationsfähigkeit usw.
- **Definition der Implementierungsstrategie.** Wie bereits erwähnt, ist es oft ideal, wenn ein Unternehmen seine SSE-Implementierung mit einer einzigen SSE-Kernkomponente wie ZTNA, SWG oder CASB beginnt. Beim Definieren einer Implementierungsstrategie für das erste Projekt sollten Sie das Projekt verstehen und den Erfolg anhand messbarer Ergebnisse in den Bereichen Sicherheit, Produktivität und Betrieb definieren.

Schritt 2: Ausführen

Nach Abschluss der Komponenten von Schritt 1 – Bewertung, Auswahl eines Anbieters und Festlegung einer Implementierungsstrategie – sollte man sich auf die Ausführung des Implementierungsprozesses konzentrieren.

ZTNA ist eine ausgezeichnete Wahl für den ersten SSE-Dienst, da diese Technologie in der Regel mehrere dringende IT- und Geschäftsprobleme löst und gleichzeitig eine solide Grundlage für zusätzliche Anwendungsfälle in der Zukunft bietet.

ZTNA wurde zur Unterstützung der modernen Belegschaft mit Anwendungen außerhalb des Unternehmensnetzwerks entwickelt und unterstützt im Gegensatz zu herkömmlichen Zugangstechnologien die zunehmenden Anforderungen an den Remote-Zugriff und sogar den Zugriff durch Dritte.

Ein VPN-Ansatz für den Remote-Zugriff beruhte auf einer unflexiblen, schwer zu skalierenden Sicherheitsstrategie nach dem Prinzip „Castle-and-Moat“. Das bedeutete oft, dass ein Benutzer, sobald er Zugang zum VPN hatte, lateral auf alles im Unternehmensnetzwerk zugreifen konnte – ein erhebliches Risiko in der heutigen Welt. Darüber hinaus verwenden VPNs häufig nur eine Benutzername- und Kennwortauthentifizierung, was sie zu einem zunehmend leichteren Ziel für verschiedene Sicherheitsverletzungen und Bedrohungen macht.

Außerdem stellt ein ZTNA-Ansatz sowohl die Sicherheit als auch die Benutzer in den Mittelpunkt, da er eine viel bessere Benutzererfahrung als bestehende Lösungen wie VPNs bietet. Er verhindert die „Authentifizierungs- Müdigkeit“ oder die Notwendigkeit, dass Benutzer ständig Authentifizierungshürden über verschiedene IT-Ressourcen und -Systeme hinweg überwinden müssen. ZTNA bietet Benutzern ein wirklich reibungsloses Erlebnis.

ZTNA übertrifft herkömmliche VPN-Ansätze und bietet Teams eine Reihe unmittelbarer und wichtiger Vorteile, darunter:

- **Skalierbarkeit, Flexibilität und Agilität.** Aufgrund seiner Cloud-Bereitstellung zeichnet sich ZTNA durch Skalierbarkeit und Flexibilität aus. Mit der steigenden Nachfrage steigt auch der Umfang der Infrastruktur. Die übergreifende SSE-Plattform ist so ausgelegt, dass sie sich an sich ändernde Geschäftsanforderungen anpassen lässt. So können neue Anwendungen, Ressourcen, Benutzer oder Anwendungen schnell unterstützt werden.
- **Granulare Zugriffssicherheit.** Während die Benutzerfreundlichkeit ein entscheidender Faktor ist, ist für CISOs die Sicherheit von grundlegender Bedeutung. ZTNA verbessert die Sicherheit des Remote- und Hybridzugriffs mit feiner Granularität erheblich und stellt sicher, dass Remote-Benutzer und -geräte vor dem Zugriff auf Ressourcen gründlich authentifiziert werden. So können Benutzer auf Anwendungen zugreifen, ohne den Netzwerkzugang zu erweitern, und die Unternehmensumgebung bleibt für Bedrohungsakteure unsichtbar.
- **Integration über Cloud-Umgebungen hinweg.** ZTNA integriert und unterstützt Cloud-basierte Dienste und hybride Umgebungen bei gleichzeitiger Aufrechterhaltung der erweiterten Sicherheit. Auf diese Weise können Unternehmen mithilfe einer einzigen sicheren Zugriffslösung neue Ergänzungen schnell in die Geschäftsumgebung integrieren, ohne die Sicherheit zu beeinträchtigen oder die Komplexität zu erhöhen.
- **Deutlich vereinfachtes Onboarding und Offboarding von Benutzern.** Ein ZTNA-basierter Sicherheitsansatz vereinfacht das Hinzufügen (oder Entfernen) von Benutzern in verteilten Systemen und Ressourcen erheblich. Dieser Zero Trust-Ansatz stellt sicher, dass Benutzer den am wenigsten privilegierten Zugriff auf autorisierte Anwendungen erhalten, während die branchenüblichen SCIM-Funktionen (System for Cross-Domain Identity Management) eine sofortige Beendigung des Zugriffs ermöglichen – auch mitten in einer Sitzung.

Während die meisten Unternehmen einen schrittweisen Ansatz für SSE wählen und dabei auf dem Erfolg der Einführung aufbauen, erfordert die langfristige erfolgreiche Implementierung von SSE eine kontinuierliche Kombination aus strategischen Entscheidungen, technischen Lösungen, der Einbindung und Schulung von Anwendern sowie einer fortlaufenden Verwaltung und Verfeinerung.

Die Implementierung Ihres ersten SSE-Dienstes kann mit internen Ressourcen durchgeführt werden. Anbieter und viele Beratungsunternehmen können jedoch auch zusätzliche Ressourcen, Anleitung und Personal bereitstellen.

Schritt 3: Überprüfen

Der langfristige Erfolg mit SSE endet nicht mit der Implementierung eines SSE-Dienstes. Stattdessen muss Ihr Unternehmen den dritten und letzten Schritt zum SSE-Erfolg unternehmen: die Überprüfung. Zu diesem Schritt gehört auch die Optimierung der SSE-Dienstimplementierung im Zuge ihrer Weiterentwicklung und der Weiterentwicklung der IT-Umgebung.

69%

der Teams planen, SSE in den nächsten 2 Jahren einzuführen²

Da SSE-Implementierungen häufig iterativ erfolgen und erhebliche Auswirkungen auf die Benutzer sowie die Unternehmens- und IT-Funktionen haben können, müssen sich CISOs und ihre Organisationen die Zeit für eine Überprüfung aller SSE-Projekte nehmen, um sie für die Zukunft abzustimmen und Verbesserungsbereiche für künftige Implementierungen zu identifizieren. Zu den Bereichen, die Cybersicherheitsteams überprüfen sollten, gehören:

- Anwenderschulung
- Testen und Optimieren
- Überprüfungs- und Feedbackprozesse

Nachdem die Überprüfungen und Aktualisierungen der ersten SSE-Einführung abgeschlossen sind, sollten die Unternehmen den Prozess mit der Planung der nächsten Schritte zur Einführung der SSE-Komponenten wieder aufnehmen. Ein hervorragender Ausgangspunkt für die Überlegungen zu den Zielen der zweiten SSE-Phase ist die Identifizierung weiterer SSE-Technologien und Anwendungsfälle, die hinzugefügt werden können. Dabei sollte man sich auf eine zusätzliche Skalierbarkeit für den Ersteinsatz konzentrieren oder nach Möglichkeiten suchen, den Ersteinsatz zu erweitern. Hier ist ein Beispiel für eine typische SSE-Reise.

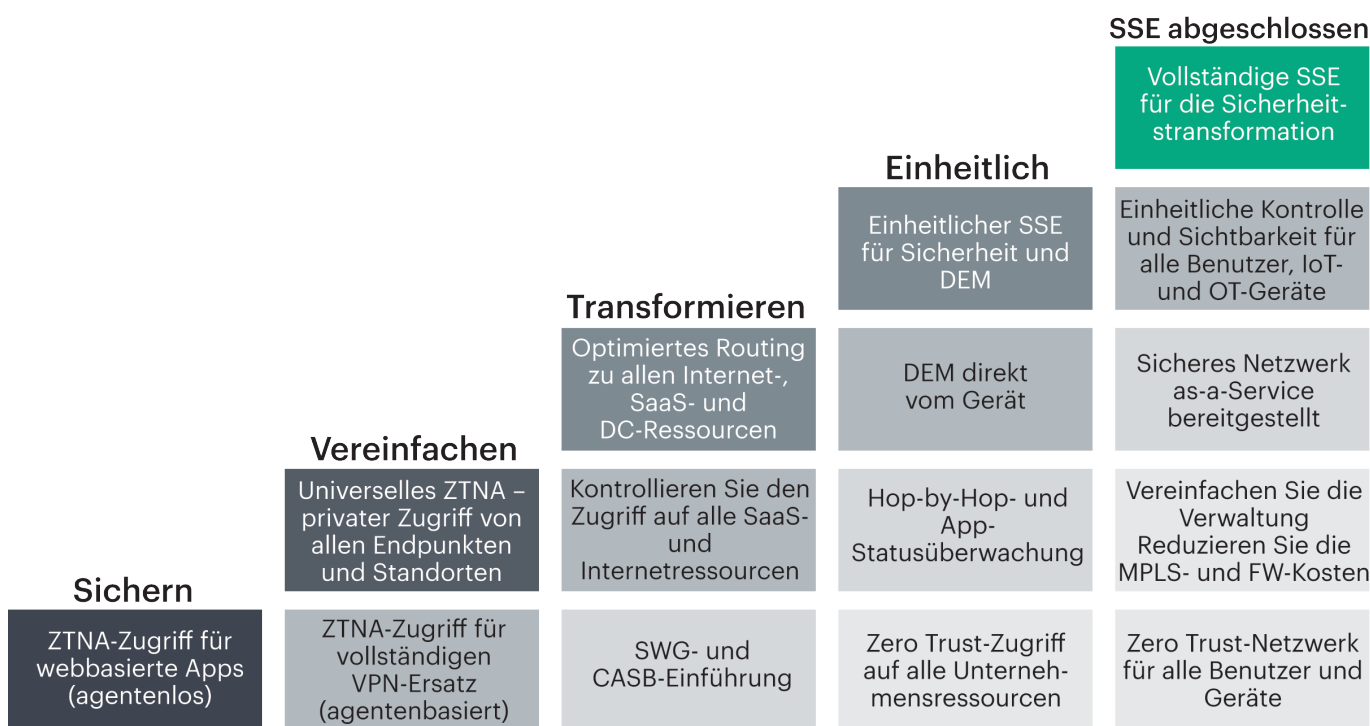


Abbildung 1. Phasenweiser Ansatz zur SSE-Einführung

Auf dem Erfolg von SSE aufbauen

Mit SSE müssen sich CISOs und Sicherheitsteams keine Gedanken mehr über „irgendwo“ und „überall“ machen. Mit SSE-Diensten wie ZTNA, SWG und CASB können Unternehmen nach und nach veraltete Sicherheitstechnologien und -prozesse durch effizientere, moderne ersetzen. Diese modernen Methoden erfüllen nicht nur dringende Sicherheits- und Benutzeranforderungen, sondern bieten auch eine flexible Plattform für zukünftige Anforderungen.

Während die meisten Unternehmen einen schrittweisen Ansatz für SSE wählen und dabei auf dem Erfolg der Einführung aufbauen, erfordert die langfristig erfolgreiche Implementierung von SSE eine kontinuierliche Kombination aus strategischen Entscheidungen, technischen Lösungen, der Einbindung und Schulung von Anwendern sowie einer fortlaufenden Verwaltung und Verfeinerung.

Der Erfolg der SSW ist also ein Prozess. Je nachdem, für welchen SSE-Anbieter Sie sich entscheiden, kann dieser Prozess schnell beginnen und enden. Wenn Sie HPE Aruba Networking SSE für Ihr SSE-Projekt auswählen, begleiten wir Sie bei jedem Schritt Ihrer Implementierung.

² 2024 SSE Adoption Report, Cybersecurity Insiders

Mehr erfahren

[HPE Aruba Networking SSE](#)

[Testen Sie SSE kostenlos für 24 Stunden](#)



[HPE.com besuchen](#)

[Chat mit Vertrieb](#)

© Copyright 2025 Hewlett Packard Enterprise Development LP. Die hier enthaltenen Informationen können jederzeit ohne vorherige Ankündigung geändert werden. Neben der gesetzlichen Gewährleistung gilt für Produkte und Services von Hewlett Packard Enterprise (HPE) ausschließlich die Herstellergarantie, die in den Garantieerklärungen für die jeweiligen Produkte und Services explizit genannt wird. Die hier enthaltenen Informationen stellen keine zusätzliche Garantie dar. Hewlett Packard Enterprise haftet nicht für technische oder redaktionelle Fehler oder Auslassungen in diesem Dokument.

Alle genannten Marken von Dritten sind Eigentum der jeweiligen Unternehmen.

a00138655DEE, Rev. 1

HEWLETT PACKARD ENTERPRISE

[hpe.com](#)

