THE 7 PITFALLS TO AVOID WHEN SELECTING AN SSE SOLUTION

Building the Security Service Edge (SSE) on a Foundation of Zero Trust

By:

Sanjit Ganguli
VP Transformation Strategy/Field CTO, Zscaler

Nathan Howe
VP Emerging Technology & 5G, Zscaler

Sponsored by:

zscaler™

The 7 pitfalls to avoid when selecting an SSE solution

Table of Contents

SSE. What is it and why should I care?

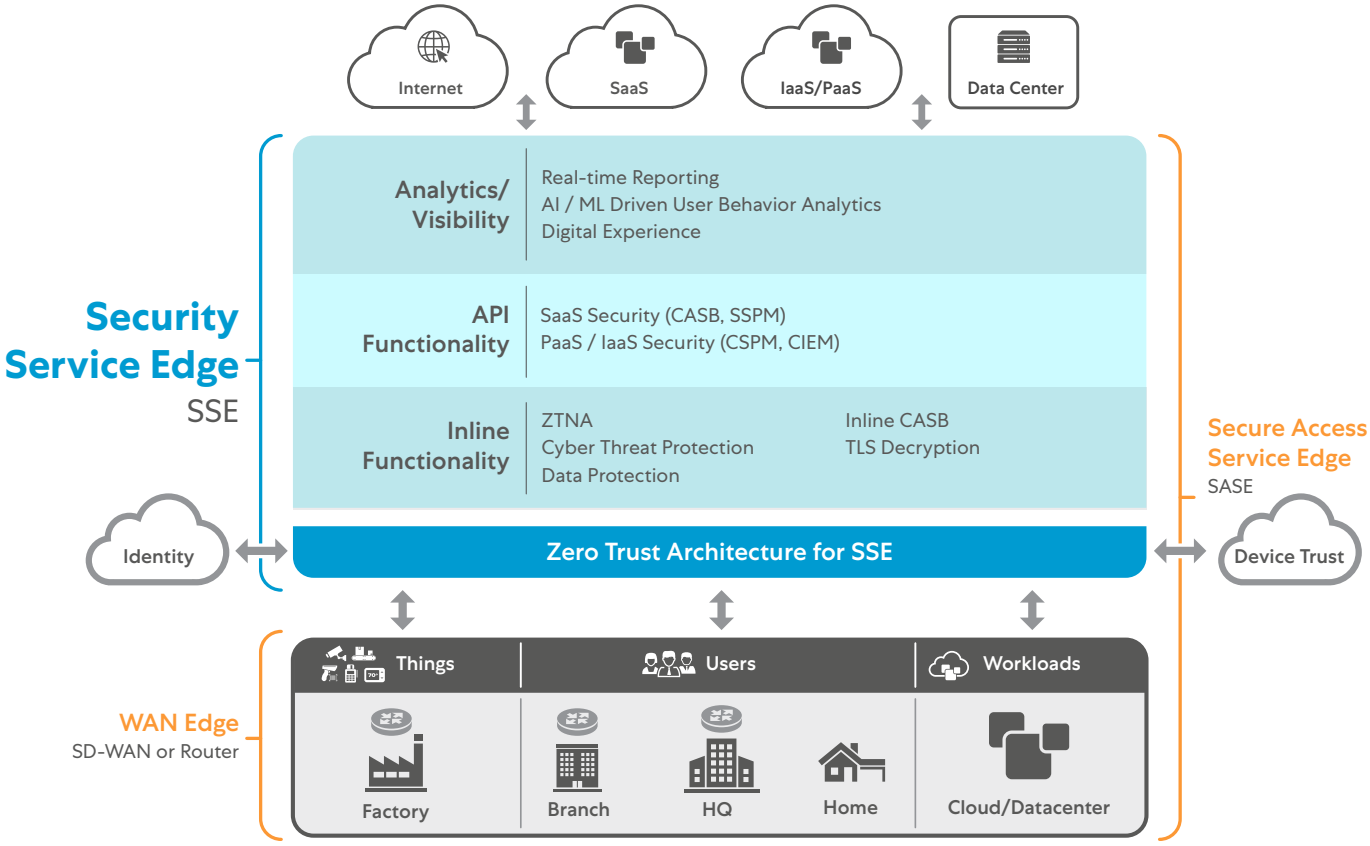


Figure 1: The Secure Access Service Edge (SASE) framework includes SSE for policy decision and enforcement. SASE requires the use of dedicated connectivity solutions from the requesting entity and the security edge where policy is enforced.

The Security Service Edge (SSE) is Gartner's specification of policy decision and enforcement as components of the Secure Access Service Edge (SASE) framework. SSE promises consolidated, simplified, cloud-delivered security and connectivity.

Architectural simplicity is always a benefit for an enterprise, especially when that simplicity minimizes technical debt and accelerates the business. But in many organizations, security is viewed as an inconvenience, an obstacle that creates bottlenecks, a gatekeeper limiting agility, or a hindrance to business success. SSE counters those stereotypes. Within an SSE environment, security offers protection and control delivered as an enabler of business progress.

Some background: Introduced in 2019, the SASE framework aims to guide enterprises through their digitalization journey, a journey driven primarily by the adoption of cloud and mobility. SASE converges network access and security, and serves both from the (highly-distributed) cloud edge **(see Figure 1)**. In that way, SASE ensures that security is no longer centralized, and that secure connections can be made to and from anywhere.

Consider how a mobile phone connects to various cellular and wireless networks. There is no dedicated network routing solution, yet the user demands security controls for traffic between the source and destination. Analogously, the edge, network, or location the user connects to should not matter when protecting enterprise traffic. This is what SSE delivers

Cybersecurity firms quickly jumped on the SASE bandwagon. Some marketers rather cynically appropriated the term for branding gain, implying the "Access" in SASE made them SASE-compliant (or competitors non-compliant): "I have a network function, therefore I am SASE; you're not building network routes, so you're not SASE.".

Figure 2: Deliver policy-based, validated entity-to-entity access at the edge for a mobile and cloud world. SSE lets you bring security to the user at the edge with no performance compromise while nullifying all your firewalls and VPNs

SSE refers to the suite of SASE services used to protect enterprise traffic. SSE ensures that the correct user (or workload) receives access, securely and under enterprise IT control, to the correct applications and services. Those services might be workloads in an IaaS or PaaS, SaaS applications, or Internet services like LinkedIn or YouTube. The service access must be granted following Zero Trust Access (ZTA) controls, outlined in much greater depth in the **second pitfall to avoid**.

To deliver on these lofty objectives, an SSE solution provider must provide a global, highly-available, scalable, network-agnostic solution that offers consistent policy, zero trust access, and a fast digital experience.

Without such functionality and availability, the SSE solutions cannot deliver on ubiquitous protection and availability **(see Figure 2.)** Unlike SASE, SSE does not prescribe any connection or access method. SSE presumes that it will work over any network and provide controls to any authorized service, anywhere that service might be.

The SASE ideal is to merge connectivity and protection, but in an enterprise setting, that pairing will only work if it is transparent to end user employees. Connectivity is direct, whether it's user-to-application, application-to-application, workload-to-workload, whatever-to-whatever. Users should never think, "Oh, I have to connect to the network before I can work." Instead, their focus should be "I'm going to get my work done now."

This integrated ideal simply can't be achieved in enterprise environments dependent on legacy network and security infrastructure. In that old architectural model, security was centralized, and data traffic—regardless of location (e.g., remote or branch), regardless of source (e.g., user, app, or workload), and regardless of destination (e.g., the Internet, cloud, data center) - had to first be connected and routed via the corporate network to (and through) the physical location of the hardware appliance-based security controls.

The true business value of SSE-driven digital transformation

SSE adoption can require significant enterprise digital transformation. But embracing that change can deliver tangible impact:

Control:

SSE starts with zero. SSE validates each person, machine, workload, network, and edge. Without correct identification further paired with context supplied by behavioural analysis, there is no access, allowing an enterprise complete control of what or who accesses any service within the enterprise.

Direct connectivity:

SSE policy enforcement resides in-line between the originating entity and the destination service. Access decisions are made on a per-application basis, not at a network level.

Business-driven security:

Policies of which entities can connect to which services are defined using least privilege. Users, machines, workloads, etc., can only connect to what they are allowed to connect to, and nothing more. No other connectivity is available, and all other access is blocked.

Global enforcement:

SSE must have global enforcement so that any entity can have controls applied on the access path based on context provided by policy, insight engines, and external learnings (threat monitoring, deception, etc.). This global enforcement must scale to the requirements of your enterprise.

Comprehensive:

SSE provides full, in-line assessment to inspect traffic at scale and in depth. SSE provides protection against advanced threats, defends corporate assets (cloud and beyond), prevents data loss, and ensures in-line control. When needed, the solution should provide control of content stored within cloud services.

Dark:

SSE prevents unwanted access and exposure of enterprise assets by removing the attack surface. It is not possible to attack what is not accessible.

From anywhere:

SSE delivers this connectivity for all parts of the enterprise from anywhere. SSE protects and connects a flexible user base while ensuring workloads, things, and machines can move, relocate, and transform without losing control.

SSE can be a catalyst for change in an organization just by securing the business in a remarkably comprehensive way. But not all solutions are created equal. IT leaders looking to adopt SSE must evaluate and select the right solution, one that allows their organization to simplify security.

There are seven pitfalls to avoid on the enterprise digital transformation journey to SSE. Avoiding these missteps will allow those IT leaders to select the right set of services, architecture, and functions to deliver on the SSE value proposition. This journey should be a path away from the "old ways of working," such as anchoring to networks or allowing blanket access to services, which limits the ability to transform and meet the needs of business.

Pitfall #1:
Choosing an SSE solution lacking a proven track record of operating a global cloud platform that scales for performance and availability

Pitfall #2:
Choosing an SSE solution that isn't built on a Zero Trust Architecture foundation

Pitfall #3:
Choosing an SSE solution that promises advanced threat protection and advanced DLP, but can't inspect encrypted traffic at scale

Pitfall #4:
Choosing an SSE solution that is "one-size-fits-all" and doesn't support flexible, scalable, and diverse deployment and management options

Pitfall #5:
Choosing an SSE solution that provides a mediocre user experience by not optimizing application connectivity or diagnosing UX degradations

Pitfall #6:
Choosing an SSE solution with limited integration and orchestration with an ecosystem of third-party vendors

Pitfall #7:
Choosing an SSE solution that can't easily show value in a production environment pilot

Who should be reading this?

Moving to SSE is not just about security transformation and involves more than just **security architects**. The best practices outlined in this e-book are meant for **security architects**, **network architects**, **enterprise architects**, **cloud architects**, and **application architects**.

#1 Pitfall

Choosing an SSE solution lacking a proven track record of operating a global cloud platform that scales for performance and availability

Instead, consider SSE solutions that:

- Offer a diverse, global set of public service policy enforcement edges with SLA-backed performance, availability, throughput, and function. The solution runs policy enforcement local to customer locations.
- Are born in the cloud with best-in-class resilience, infrastructure, geographic diversity, functional capabilities, and optimal user experience. Deliver SSE services in-line at carrier-neutral data centers and not as a service run on top of a destination managed cloud or DC provider.
- Have a proven and transparent pedigree of scale, growth, and delivery validated by customer references, historical reporting, third-party certifications, and external open source data repositories (https://www.peeringdb.com/org/12297).

How the right SSE vendors make this work:

Building and running a multi-tenant, SSE platform for billions of transactions is much more than the level of compute and is not a simple thing. **The SSE solution will be entrusted with the protection, connectivity, and enablement of your enterprise**, and therefore it must deliver the set of SSE services uniformly and timely to all parts of the organization.

The correct SSE solution will deliver services to your enterprise through a globally distributed service. Architecturally, the most effective way of delivery is through a proxy-based service. Not anchored to the network state, a proxy service focuses on delivering SSE to the application access,allowing for greater comprehension without offloading to additional platforms for insights like inspection at scale **(see Pitfall #3)**.

Note that true proxy architecture takes significant R&D effort and many years of refinement to achieve the scale requirements of the modern enterprise. The right SSE solution will have scores of examples of large deployments where the proxy architecture was shown to scale.

This service must be delivered through a uniform set of policy edges where any and all data transmission functions of your enterprise are protected and it should not just be the number of nodes, but rather the number of SLA guaranteed sites that offer services needed by the customer. The SSE provider should not provide public PoPs if it cannot guarantee the SLA in that region due to poor peering or other reasons.

Adopting SSE means you'll consolidate, invigorate, and share the responsibility of your enterprise security, connectivity, and control with a trusted security vendor. This shared model will simplify the means by which you deliver protection and connectivity for your users, workloads, services, and branches, amongst others. The SSE provider must deliver on a set of defined, proven SLAs to ensure the function of your enterprise, while also delivering protection.

When your enterprise service connects, it needs an effective path to consume the destination function. This can only be achieved through an SSE solution with highly effective peering within carrier-neutral data centers. Therefore controls must be applied in-line, between the source and destination—regardless of the location of a source and/or destination.

Solutions that host the security service within central compute clouds, often within hyperscalers and have ingress gateways, as shown in Figure 3 (often referred to as on-ramp services), rely on distributed ingress edges, but process policy control and application centrally, thus introducing unwanted latency and resulting in poor user experiences.

SSE vendors must have a demonstrated complete, massive, and scalable cloud platform. Beyond SLAs, the SSE platform should also provide evidence of scalability, stability, availability, and geographic deployment, etc. To validate this review, consult publicly provided historical data and speak with existing customers to understand their experiences.

Uniform Edge Policy Enforcement

An SSE vendor´s set of service edges must deliver policy enforcement. They cannot be edges of connectivity to a larger, cloud-based network, solely to route or "on-ramp" your traffic to the central enforcement infrastructure. Such schemes defeat the purpose of providing highly effective, low latency services

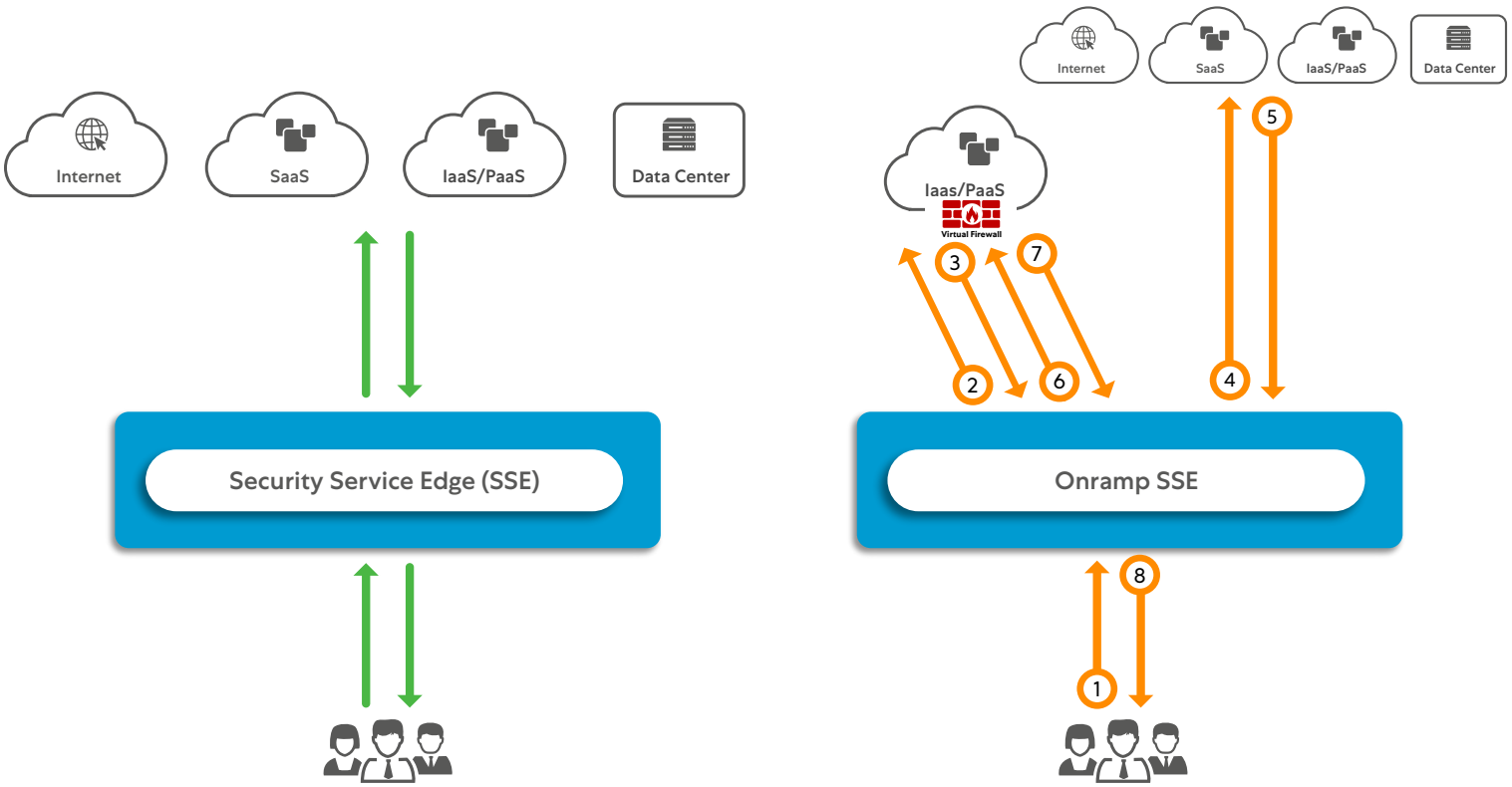


Figure 3: In-line SSE services (left) apply security controls to traffic in-line. On-ramp security controls (right) provide ingress gateways in the edge, only to forward to a central cloud compute-hosted control, adding latency, inefficiency and delivering a poor user experience.

The vendor needs to address the following design considerations, ensuring that the edges must:

- Be hosted in vital peering locations within carrier-neutral data centers, thus ensuring minimal latency between the source and destination. When assessing an SSE vendor, review the statistics from public references like PeeringDB and partner deployments **(see Pitfall #6 for partner integration details)**.
- Be supported with a valid SLA. This will reassure the stability of the business functions and indicate that the SSE vendor is working in regions to guarantee the SLAs.
- Be deployed privately on a per-customer basis in locations where local conditions require more nuanced deployments, such as on-premises or within an edge compute node **(Pitfall #4 contains more details)**.
- Demonstrate a historical path of throughput growth.
- Deliver fault tolerance deployed in active-active mode to ensure availability and redundancy. (The vendor monitors and maintains its public service edges to ensure continuous availability.)
- Promote data privacy to ensure that customer traffic is not passed to any other component within the infrastructure and no data is ever stored to disk.
- Provide uniform controls for enterprise resources at all edges and not route or "on-ramp" traffic from remote edges to central locations.
- Enforce global scale protection to protect all enterprise services once a threat is detected

⚠ What should I be aware of?

- Public edges that do not provide enforcement. Instead on-ramp traffic to larger enforcement data centers where compute resources are available.
- Claims of a 100´s of public edges without sharing the function and capacity of each edge
- Edges without SLAs on availability, throughput and resiliency.
- Edge services without multi-tenancy and force traffic via on-ramp/route to other locations.
- SSE services that have no proven evidence of deployment with large customers.
- Services without publicly consumable information about the stability and availability of the service

Outcomes:

Selecting an SSE solution that scales for your business today and, more importantly, for your future goals is a critical investment. Scalability is not simply the mechanism to build out, but more importantly, address your enterprise needs without sacrificing the function, stability, and protection of your business by selecting a solution that:

- Provides evidence and transparency of its global and diverse deployment.
- Has documented and validated SLAs for the loss of or degradation of SSE services.
- Has deployed a large number of customers of similar size and complexity as your enterprise.
- Has public, reviewable information for each PoP using public tools (e.g., PeeringDB).
- Delivers all critical functions at all sites without hairpinning traffic.
- Provides protection in-line between the source and destination.
- Is designed for infrastructure and operational and functional resilience.
- Is consumable in multiple forms across multiple sites.

#2 Pitfall

Choosing an SSE solution that isn't built on a Zero Trust Architecture foundation

Instead, consider SSE solution(s) that:

- Only allow access for contextually validated identities, regardless of location/network. This least-privileged path is for all services, not just users. By connecting authorized sources through the correct SSE controls to valid destinations and nothing more, enterprises remove lateral movement, which is often exploited by threat actors.
- Focus solely on connecting dynamic, per-session access. Zero trust is not delivered with firewalls, SD-WAN, and other network services. It must be a network-agnostic overlay.
- Never expose enterprise assets to an unauthorized source, therefore reducing the attack surface and ensuring correct controls are applied to all services.

How the right SSE vendors make this work:

Zero trust for all enterprise communication means that no access is granted from any source (including users, third parties, networks, and so forth) to any destination without explicit permission and approval to do so.

Delivering zero trust within an enterprise has traditionally been challenging due to the shared network context of connecting the source to destination, relying on either a physical or logical network path to interconnect the two entities. Figure 4 outlines these shared physical concerns. You cannot build or add on zero trust with SD-WANs or firewalls.

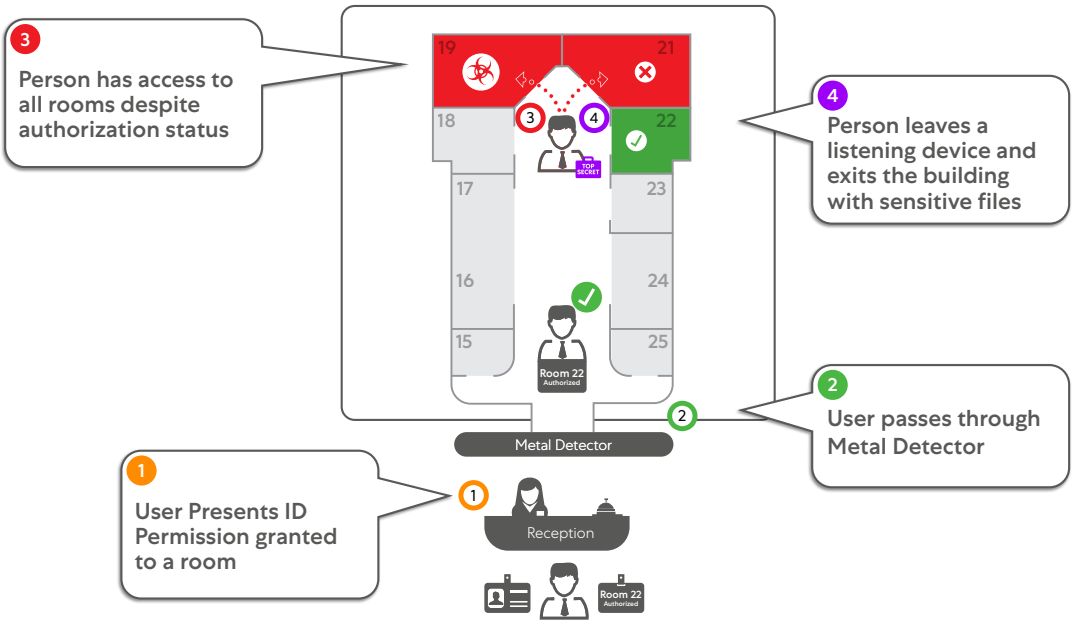


Figure 4: How not to enable access—the old world of network security analogy. Connecting users to your corporate network is like allowing unescorted visitors wander around inside your headquarters, potentially stealing sensitive data.

SSE can help you enforce enterprise-wide user access and restrictions for your workloads. By expanding these controls beyond employees, you can protect your enterprise from risks such as an exposed attack surface or lateral threat movement.

Among many other things, Zero Trust Architecture enforces granular controls, ensuring that each requester communicates with the correct destination on a per-session basis, as Figure 5 illustrates. Such rules require knowledge of the source and destination entities and are why most enterprises begin their zero trust (and SSE) journey with their user base. Users are often assigned an identity, allowing them to differentiate themselves from various services. However as networks are flat, exposed, and open, the risk of a user having access to more information just because they shared a network is a major concern to the stability of enterprises.

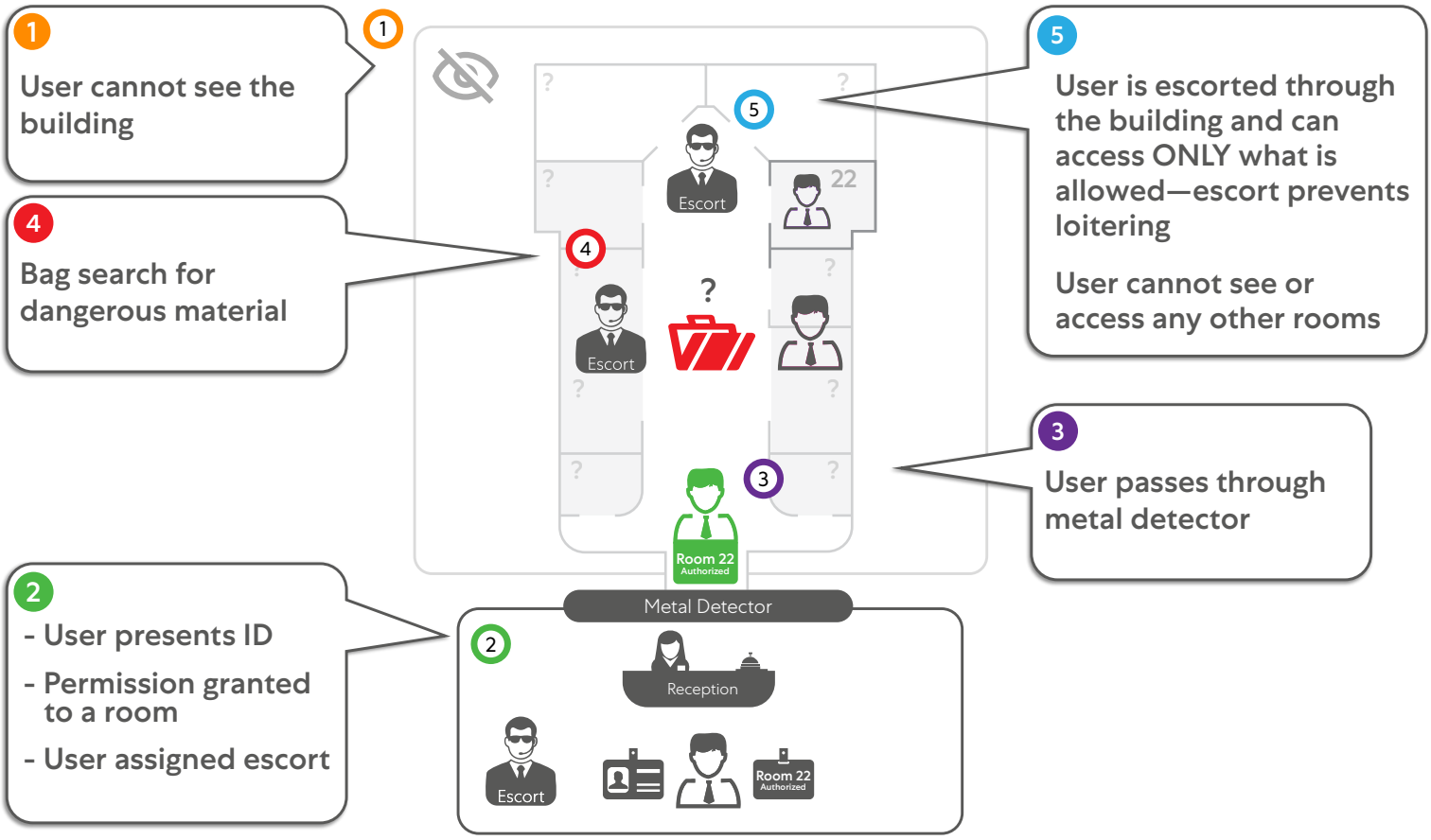


Figure 5: The correct way to provide access is through end-to-end control. Zero trust access is like escorting a blindfolded visitor to a meeting in your headquarters and then escorting her out. The visitor can't wander or snoop around.

Consider all business use cases like protecting users and key business assets and apply SSE controls to all traffic. Establish connections after dynamically and contextually reviewing the riskiness of the following four connection values (see Figure 6):

Initiator of the connection

What is the identity and trust of the user/device/network? How does this identity differentiate the access for this source and under which conditions?

Example: Sarah in HR needs access to the cloud-hosted HR system as well as the internal hosted expense system. Access is granted through the SSE platform as long as her identity and device trust have the rights defined to get access.

Control of policy

Where, how and which controls will be applied? Criteria for control includes effectiveness of path, the risk and trust of the initiator, the function of the requested destination and the policy of the enterprise.

Example: Pierre has a valid identity to access Salesforce, but his company only wants him to view, not download or manipulate data. The SSE solution thus only allows Pierre the access to view the content of the application and nothing more.

Destination of the connection

Which service is the requester accessing? Is it public SaaS or an internal workload? What controls are to be applied? Access can change based on the context of the identity and control policy.

Example: A valid initiator may have approval to access a specific cloud PaaS service, and if it is a cloud service, the SSE will inspect the workload to ensure it is not leaking corporate secrets. That same initiator may then speak to an internal service with a similar trust, thus simply establishing an initiator to service connection, without additional controls.

Establishment of connection

Finally, taking the previous inputs, the conditional insights on workloads, network or edge capacities, enterprise-defined policy, etc. and establish access. The SSE solution should identify variations, e.g. a changed location and steer the access through the best applicable path.

Example: Once the source, control and destinations are validated, the connection will be built, for that session and nothing more. The per-session enforcement end-to-end flow is outlined in Figure 6.

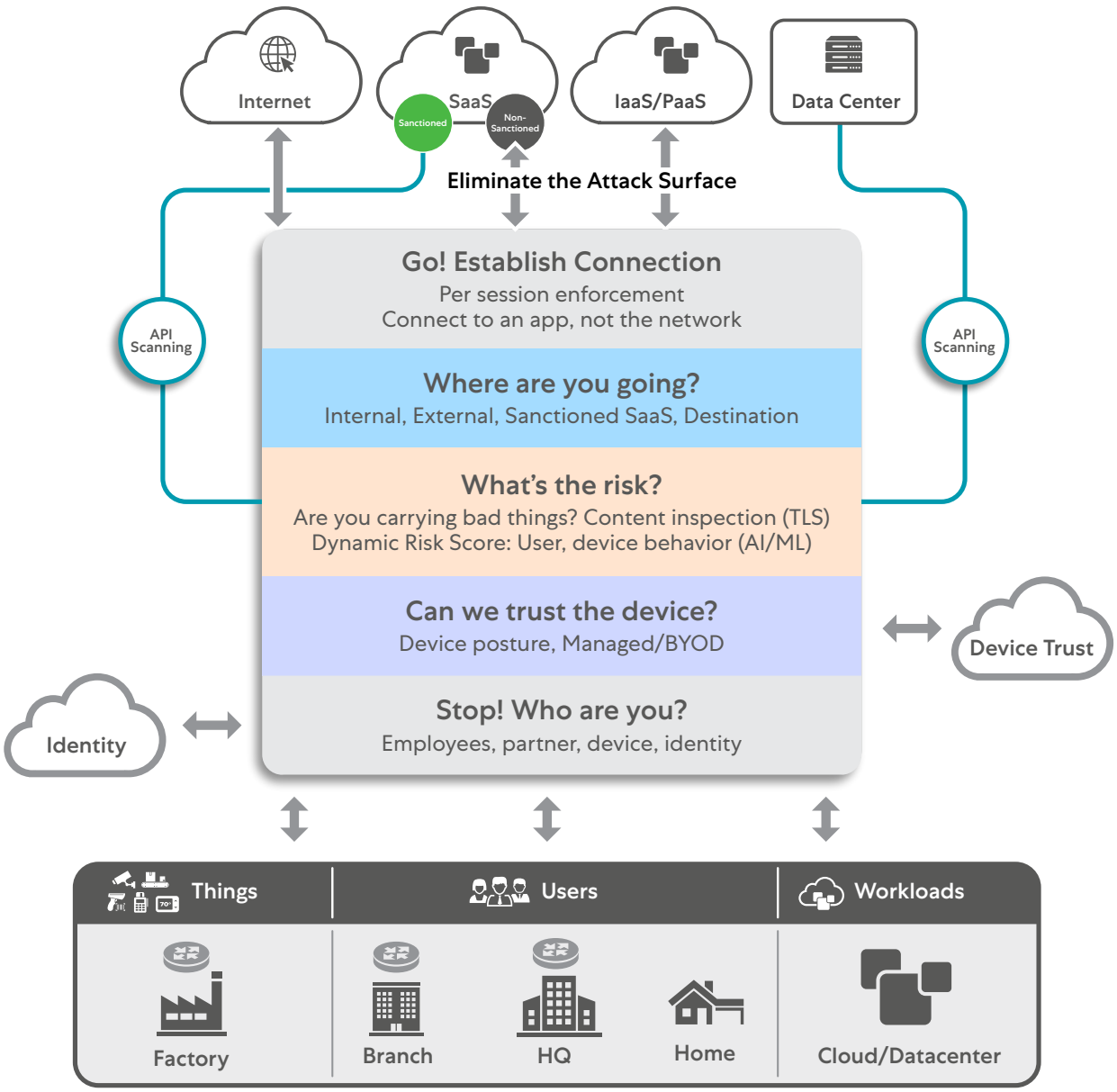


Figure 6: Steps of a zero trust architecture, showing policy control and enforcement at each step

Defining the connection controls within an SSE solution **ensures that only the correct source can consume the correct destination**, through the correct SSE solution. This least-privilege use of SSE delivers multiple benefits to an enterprise, including:

- Applying the correct SSE controls to the correct source
- SSE protected services are not exposed to unauthorized sources, reducing cybersecurity risks
- Waste reduction, e.g. don't allow a Linux server to connect to a Windows patch system.
- Granular visibility and learning of flows - per-access request, not network IP to IP
- Consolidation of access based on identity and not on network, allowing networks function (and infrastructure) to be rationalized

SSE phased journey with zero trust:

By selecting an SSE solution that delivers the control under all of the following use cases–and only user based control–you can extend protection across all your business functions (see Figure 7):

User to Workloads

Enabling user access to workloads means you can remove the network context from user access, whilst simultaneously gaining visibility of the workloads that are being accessed by users. This one-two punch typically delivers the quickest value.

Consider granular control for users across the entire application landscape. For instance, internet services like YouTube can be limited to an organization's PR team.

Allowing for greater development of inventory of enterprise services and allowing for more granular rules such as access to isolated OT and R&D platforms, without ever exposing the entire ecosystem to the user base.

Third-party Access

Implementing zero trust access for third-party partners removes the risk of network connectivity and exposed attack surface that comes with legacy partner access. The least-privilege control of zero trust allows you to control partner access from untrusted or personal devices to specifically designated apps and nothing more, whilst giving greater visibility of what is being accessed.

The third party controls of the SSE solution should provide multiple mechanisms for access control. Options include authorized client access from multiple identity providers, through to specific applications, isolated browser-only access, or complete isolation of access to a rendered image presented to the third party (streaming pixels to the user device like BYOD).

Workloads to Workloads

Workload-to-workload controls are requests for access to applications and services. Generally, a Windows machine will request Windows patches, not Linux. Thus it is critical for an enterprise to categorize which systems should get access to what.

As with users, workload controls must provide a valid identity to consume a service. If the workload consumes public resources such as PaaS-based IoT/OT services, the security edge must validate and understand its context and block any attempted misuse.

Conversely, should the workload access a local, private service, this can only be done through in-line SSE controls, after the approval of the identity, as per a zero trust validation.

Location to Location

As access and control evolve across your enterprise, consider zero trust for inter-site connectivity. You'd need to isolate a set of services to a network, site, VPC, etc. The connection between the location and the known site should not be over a shared network. Zero trust enables a valid location to connect to a valid set of workloads within another location. Zero trust does not use network link-layer access; it calls for app-to-app connectivity uniformly across any site, VPC, VLAN, etc.

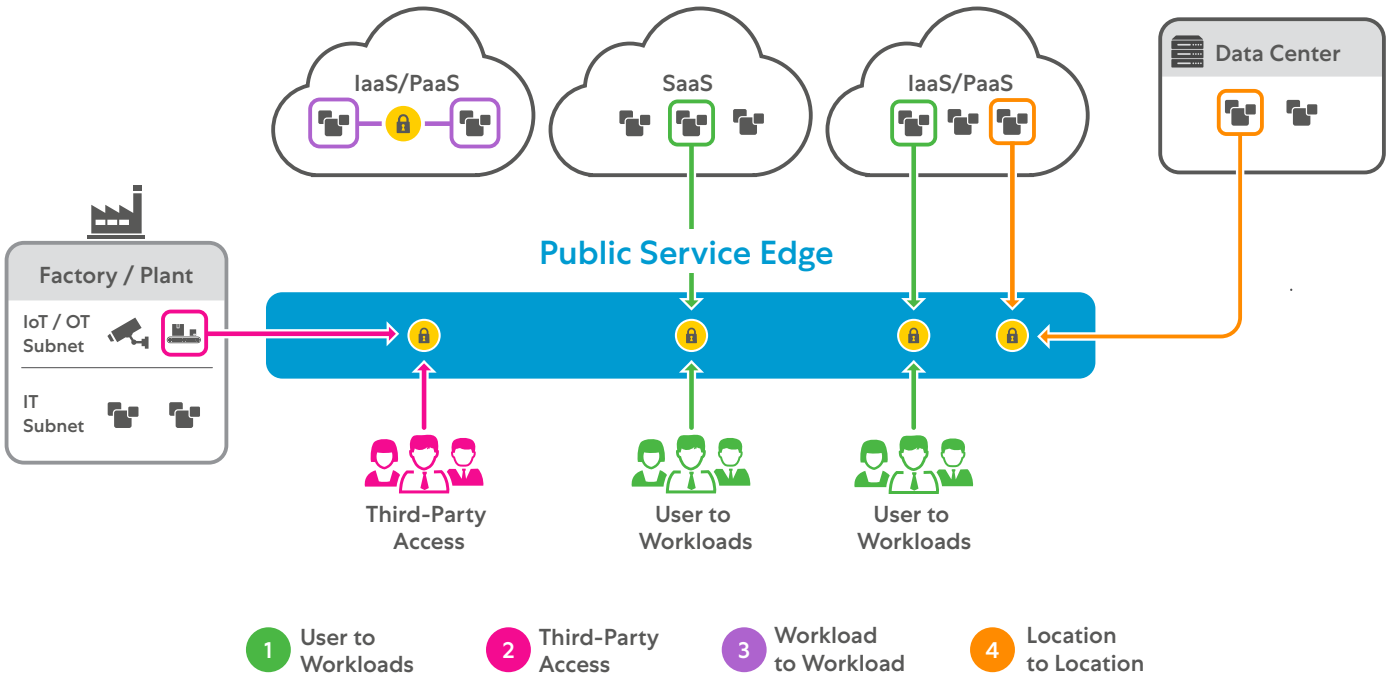


Figure 7: A suggested approach for enterprise segmentation. Allowing a phased approach of control, learning, further segmentation and isolation - as part of a zero trust implementation

As a recent example, when security researchers discovered the Log4j zero-day vulnerability, every customer running the vulnerable Apache Java-based logging utility was at risk of full remote code execution. However, those adopting a zero trust architecture would have their internal apps completely invisible to the Internet—this meant that attackers could not find and exploit them, safeguarding even susceptible versions of Apache Log4j from this and future vulnerabilities. This would have been impossible with legacy, exposed services like VPNs and firewalls. **Zero trust ensures that only authorized users can access apps; it prevents lateral movement with user-to-app and app-to-app microsegmentation, and it can inspect both inbound and outbound traffic**.

This was similarly true with the Colonial Pipeline attack in which stolen VPN credentials (that didn't have MFA enabled) gave hackers access to laterally move across the network and access sensitive data. A zero trust architecture that connects only authorized users to applications, and not networks, prevents lateral movement by segmenting user-to-app and app-to-app communications

What should I be aware of?

- Avoid SSE services that don't follow Zero Trust Architecture principles, such as the NIST Special Publication 800-207.
- Ensure that the SSE service offers zero trust controls to all enterprise resources, not solely users.
- Zero trust is not a firewall or SD-WAN function. It is network-independent and network-agnostic. An SSE from a provider that is network-dependent can expose you to a zero trust architectural deficiency.
- Ensure that the zero trust controls start at zero access; no enterprise assets should be accessible until validated.
- Address all aspects of your enterprise. Don't limit your zero trust controls to one part of the business.

Outcomes:

Protecting an enterprise and its user must be approached in a way that delivers access on a need-to-know, least-privileged basis. **Zero trust must be the foundation control when picking an SSE solution**, so that:

- The SSE vendor protects all enterprise services and validates the identity of the entities before allowing access; everything else must be blocked.
- Solutions that force network connectivity should be avoided and access should be network-agnostic, everywhere.
- The SSE service delivers a zero attack surface for your private enterprise services.

#3 Pitfall

Choosing an SSE solution that promises advanced threat protection and advanced DLP, but can't inspect encrypted traffic at scale

Instead, consider SSE solution(s) that:

- Provide SSL/TLS inspection of traffic at production scale with minimal impact on performance. This requires a scalable proxy architecture.
- Capture and analyze deep insights gained from inspection to apply advanced threat protection for encrypted traffic and apply advanced data classification policies for data loss prevention.
- Inspect all traffic, including encrypted, from users, things, workloads, etc.

How the right SSE vendors make this work:

SSE vendors cannot claim to have best-in-class advanced threat protection and data loss prevention without the ability to inspect all traffic at production scale, including encrypted traffic.

Be wary of SSE vendors' claims in this area, as much depends on the underlying architecture of the solution. Those SSE vendors that have built their cloud proxy as cloud-native from the ground up have a distinct advantage in this area.

With the vast majority (estimated around 85%) of Internet traffic encrypted, SSE vendors must inspect this traffic at scale and in depth for adequate threat protection and data loss prevention required in the face of the exponential growth in security risks posed by encrypted channels. Why is SSL/TLS decryption at scale so important (see Figure 8)?

- SSL/TLS encryption can hide harmful content such as viruses, spyware, and other malware.
- Attackers build their websites with TLS and SSL encryption or inject malicious content into well-known and trusted SSL- and TLS-enabled sites.
- SSL/TLS can hide data leaks, such as the transmission of sensitive financial documents from an organization.
- SSL/TLS can hide the browsing of websites that belong to legal-liability classes.
- The ability to control and inspect traffic to and from online services using HTTPS has become an important piece of an organization's security posture.

Figure 8: Pass-through architecture employed by some vendors doesn't provide the inspection of encrypted traffic at scale, similar to a basic security checkpost allowing a car to pass without checking its trunk for malicious cargo

Given these risks, an SSE vendor's architecture must scale to function as an SSL/TLS person-in-the-middle proxy that provides complete inbound and outbound content analysis and immediately blocks any threat detected anywhere in the cloud.

Threat actors continue to evolve their tools, techniques, and procedures when targeting organizations, which include abuse of legitimate storage service providers like Dropbox, Box, OneDrive, and GDrive for hosting malicious payloads. These connections will use wildcard SSL/TLS certs of these reputed vendors when serving the malicious payloads, which if not inspected will result in a successful attack. The malicious payloads (executables, office documents, etc.) are also polymorphic in nature, as the goal is to evade basic fingerprinting detections. SSE vendors' architecture must allow full payload extraction from these SSL/TLS encrypted connections and must be capable of unpacking and deobfuscating these files for accurate detection (see Figure 9).

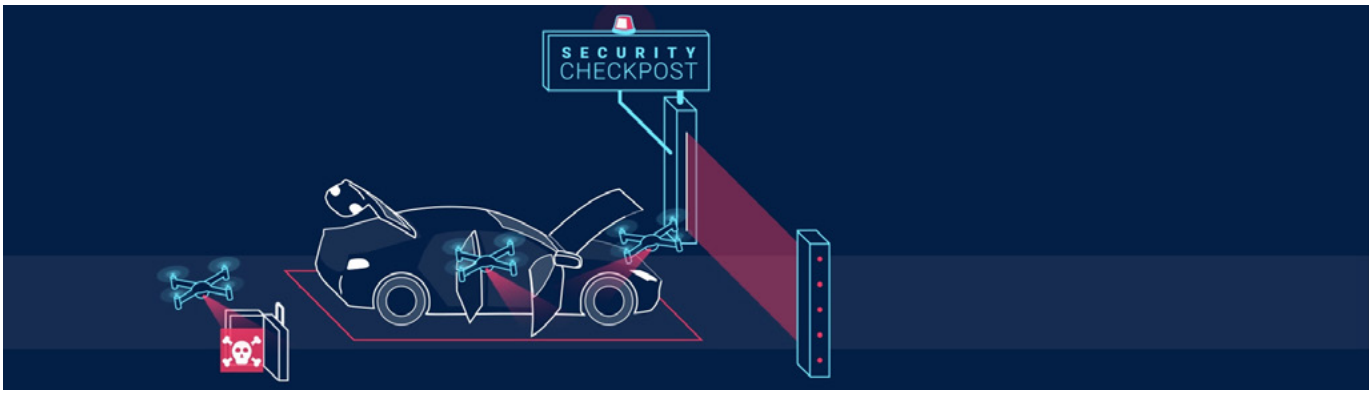


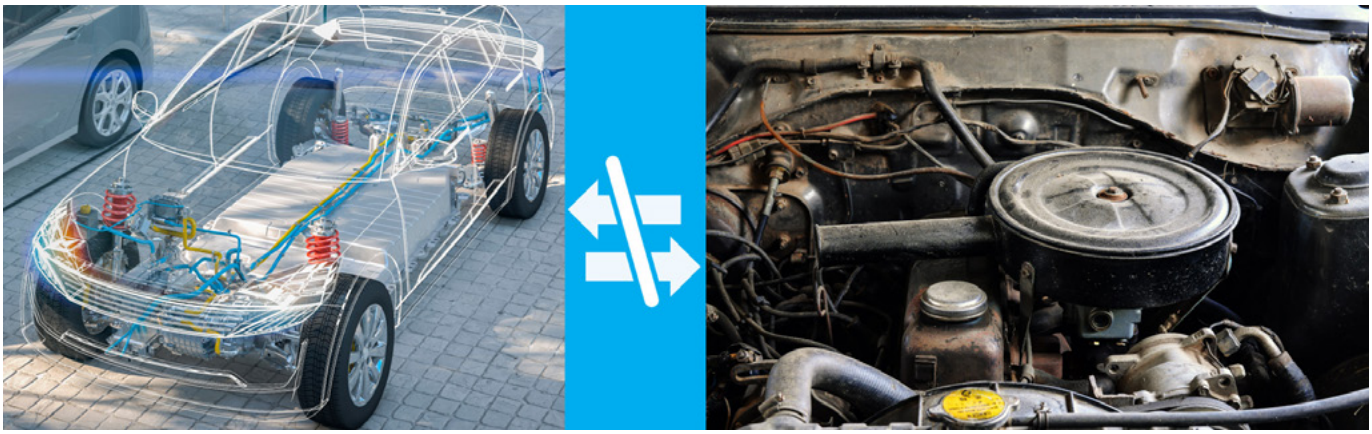
Figure 9: The right SSE vendor provides full SSL/TLS inspection of all traffic using a proxy architecture, similar to a car that is stopped and fully inspected before it is allowed to pass the security checkpost

This threat protection should leverage many industry threat feeds across open source, commercial, and private sources, as well as have frequent security updates.

In addition to blocking threats, inspection at scale enables advanced data loss prevention. **SSE vendors should be evaluated on their data classification capabilities**. These should include regular expressions (regex) as a basic mechanism, but quickly finding and classifying sensitive data across all cloud data channels is a requirement to protect personal, health, and confidential data from loss. This classification requires SSL/TLS inspection and enables advanced capabilities like:

- **Exact data matching**. The SSE uses index templates to identify a record from a structured data source that matches predefined criteria.
- **Document fingerprinting**. The SSE uses a document repository to identify completely or partially matching documents when evaluating outbound traffic.
- **OCR (optical character recognition)**. The SSE detects sensitive data within an image file, embedded images, screenshots, and handwritten texts and closes all cloud-based data exfiltration channels.
- **Machine learning.** Pretrained algorithms make decisions about the sensitivity of the data.

Figure 10: Just like the way an internal combustion engine cannot be retrofitted to function like an electric vehicle, be wary of vendors who tack on capabilities like SSL/TLS inspection to legacy architectures



SSE includes cloud access security broker (CASB) functionality to monitor and enforce policies between cloud service users and apps, and being able to inspect the encrypted traffic in-line has a number of advantages in this context. Inspection can be "out-of-band," which means scanning the APIs of SaaS providers to protect data at rest, or "in-line," the scanning of data in motion. Pay special attention to the latter, as in-line inspection prevents data from being uploaded to unsanctioned apps, data from being downloaded to unauthorized devices, and malicious content from being downloaded or uploaded. The SSE vendor should also allow granular access control based on a rich set of cloud app definitions, file type controls, and risk attributes.

With the adoption of hundreds and thousands of cloud applications, organizations' sensitive data is widely distributed today. The top two data exfiltration channels are cloud desktop and personal email applications. A good SSE vendor should deliver complete contextual visibility and enforcement when rogue users upload sensitive data to their personal Box, Dropbox, and other cloud desktops. They should also stop data exfiltration on personal and unsanctioned webmail services such as Gmail and Hotmail.

Where the differentiation between SSE vendors becomes apparent is how well their ability to decrypt and inspect SSL/TLS traffic elastically scales upon traffic demands, and that this level of inspection be delivered without concern for performance—all of which can only be accomplished with a proxy-based SSE solution built with scale in mind from the start (see Figure 10).

It is important to dig into how the SSE vendor accomplishes this. To maintain minimal latency for each packet inspection, the vendor should employ a single pass architecture where the packet is placed into memory once and the inspection services, each with dedicated CPU resources, are able to perform their scans simultaneously. Vendors who service chain these inspections with serialized physical and virtual applications incur a processing penalty at each hop, and run the risk of excess latency applied to each packet.

These architectural advantages must be applied to newer standards like TLS 1.3, where a true proxy architecture has the advantage of being in-line with two separate connections to the client and server. Since this allows for the entire object to be reassembled and scanned, advanced threat protection, DLP, and sandboxing can be applied. Ensure that TLS versions and cipher upgrades are handled seamlessly by the vendor within their cloud—certain hardware-based vendors may force appliance refreshes to handle the additional load for new cipher support.

Certificate management should also be considered, given the potential complexity that can be introduced. SSE vendors should allow the ability to use their certificates or to bring your own, and permit rotation between the two via API. Certificates should be automatically replicated among the various service edges.

Be wary of SSE vendors that may tack SSL/TLS inspection capabilities onto existing NGFWs, which have inherent scale challenges. This affects even those vendors that lift-and-shift NGFWs with inspection capabilities into virtual instances on CSP compute nodes

⚠ What should I be aware of?

When evaluating an SSE vendor's ability to inspect SSL/TLS, be sure to validate that the latency incurred is acceptable. Unfortunately, non-cloud-native architectures can induce significant performance drops, especially when using TLS 1.2 or earlier versions. **Data privacy can also be a concern, so understand the regulatory constraints and how the vendor handles them**. SSE vendors should allow for the easy exclusion of certain data types to stay within privacy constraints. SSE vendors should never store user data in the cloud.

Be wary of SSE vendors that may tack SSL/TLS inspection capabilities onto existing NGFWs, which have inherent scale challenges. This affects even those vendors that lift-and-shift NGFWs with inspection capabilities into virtual instances on CSP compute nodes. Also, be careful with vendors who combine out-of-band CASB capabilities with limited in-line traffic inspection. Securing data at rest and data in motion is critical.

Evaluate how the SSE vendor manages certificates, and be aware that certificate pinning may be an issue.

Implementing SSL/TLS inspection has been historically challenging to the business for various reasons. **The SSE vendor should be the foremost trusted expert and should provide guidance, understanding, and implementation when enabling SSL/TLS inspection. SSL/TLS inspection** is non-negotiable in the SSE world, as there should be no sacrifice in speed over security.

Outcomes:

SSL/TLS inspection at scale with minimal latency significantly increases the ability to block threats by leveraging the power of the cloud to identify and secure sensitive data. Only SSE vendors with the right cloud-native architecture will deliver:

- SSL/TLS inspection of all traffic at production scale with minimal impact on performance for the most in-depth threat and data protection.
- A single memory scan architecture for unique scalability advantages for decryption at scale.
- The experience to guide customers through the steps and challenges to achieving SSL/TLS inspection..

#4 Pitfall

Choosing an SSE solution that is "one-size-fits-all" and doesn't support flexible, scalable, and diverse deployment and management options

Instead, consider SSE solution(s) that:

- Offer flexible deployment models for protecting users and applications wherever the application is hosted, including the data center, public cloud, private cloud, edge compute node, and on-premises.
- Deliver protection for users accessing applications on both managed and unmanaged end user devices or things.
- Extend those same cyber threats and data protections to protect all other workload-to-workload communications within the same or across multiple clouds.

How the right SSE vendors make this work:

SSE solution evaluators must assess the readiness of their environment to understand how best to apply SSE protections. To support the variety of deployment scenarios, SSE vendors must allow for both public service edges and private service edges.

How the right SSE vendors make this work:

SSE solution evaluators must assess the readiness of their environment to understand how best to apply SSE protections. To support the variety of deployment scenarios, SSE vendors must allow for both public service edges and private service edges.

Most users will connect to the SSE via a vendor's public service edge. These are full-featured, secure Internet gateways and private application brokers that provide integrated security. They inspect all traffic bi-directionally for malware and enforce security, compliance, and firewall policies and need to handle hundreds of thousands of concurrent users with millions of concurrent sessions. Because of this, regardless of where your users are, they can access from any device:

- The Internet with the public service edges protecting traffic and applying your corporate policies.
- Internal applications with enforced access and re-authentication policies based on your organization's corporate best practices.

Figure 11: An SSE vendor must offer both public and private service edge options, which must also work in harmony with each other with a centralized management

It is important to ensure that these public service edges have significant fault tolerance capabilities and are deployed in active-active mode to ensure availability and redundancy. The vendor should monitor and maintain its public service edges to ensure continuous availability. To ensure data privacy, customer traffic must not be passed to any other component within the infrastructure and no data should ever be stored to disk.

However, situations may arise where the public service edge may not meet requirements and therefore the SSE vendor must offer private service edge options (see Figure 11). This option extends the public service edge architecture and capabilities to an organization's premises or private location and leverages the same centrally controlled policy as the public service edges.

For secure access to the Internet, private service edges can be installed in an organization's data center and are dedicated to its traffic, but should be managed and maintained by the SSE vendor, with a near-zero touch from the organization. This deployment mode typically benefits organizations that have certain geopolitical requirements or use applications that require that organization's IP address as the source IP address.

For internal application access, the private service edge provides similar management of connections between the user and application and applies the same policies as the public service edge, with the service hosted either on-site or in the public cloud, but again managed by the SSE vendor. This deployment model allows zero trust within the four walls, as it is useful to reduce application latency when an app and user are in the same location (and going to the public service edge would add extra latency). This option also provides a layer of survivability if a connection to the Internet is lost. The SSE vendor should distribute images for deployment in enterprise data centers and local private cloud environments.

To provide zero trust protection for internal applications, SSE vendors must offer a way to create a secure, authenticated interface between your application servers and both public and private service edges in order to protect internal applications. **This mechanism should be available in several form factors**: a standard virtual machine (VM) image or containerized deployment in enterprise data centers, local private cloud environments such as VMware, or public cloud environments such as Amazon Web Services (AWS) EC2, and packages that can be installed on supported Linux distributions.

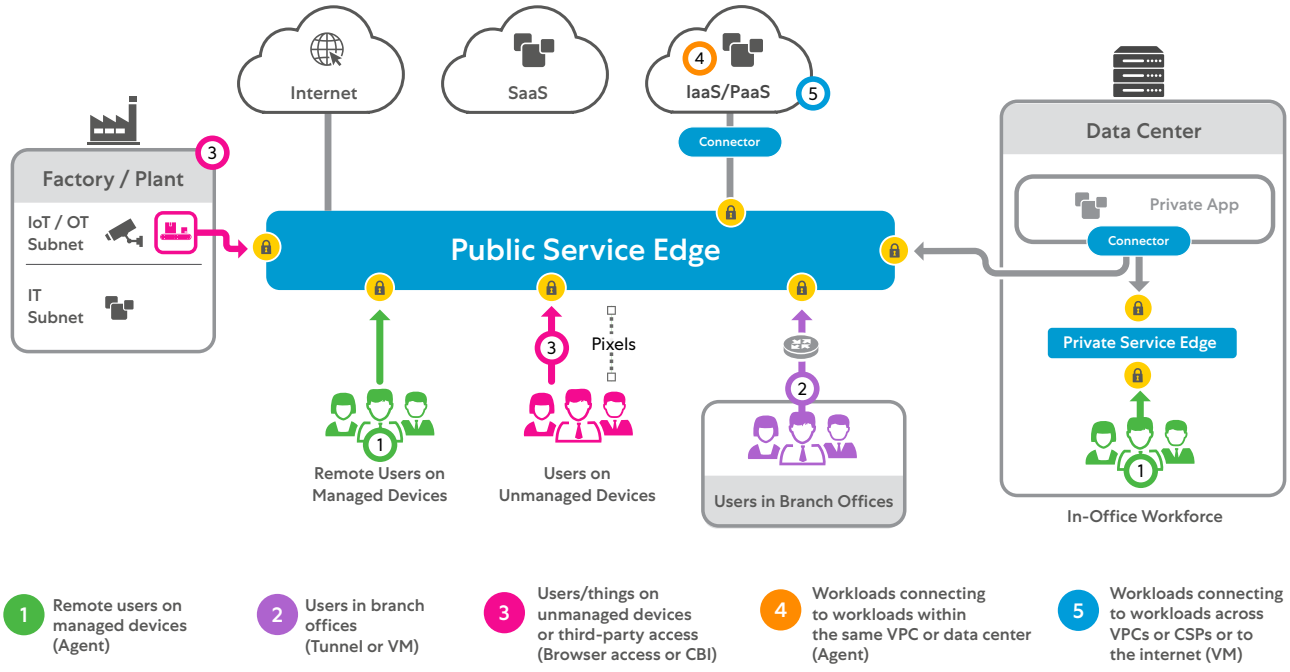


Figure 12: The SSE vendor should support a number of deployment and management modes, accounting for remote users, users in branches, users in HQ, workloads communicating with workloads, etc., via agents and VMs.

Once it is established from where the SSE policies will be administered and enforced, then consider how users and workloads will be offered this protection. It is important to consider various scenarios (see Figure 12):

For remote users on managed devices, the SSE vendor must offer a single unified agent that forwards traffic to the service edge for secure Internet access. The agent should also provide granular, policy-based access to internal resources. All of this should be automatic using the intelligence built into the agent. It should also protect your users' mobile traffic on Wi-Fi or cellular networks. The agent forwards user traffic to the SSE service, which enforces your organization's security and access policies wherever users access the Internet and establishes a secure transport for accessing enterprise apps and services. Ensure that this agent can detect when a user connects to a trusted network and, if a trusted network is detected, whether the agent must disable its service, as determined by policy. Ensure that these agents support a wide range of operating systems, including Windows, MacOS, Linux, iOS, and Android.

For users in a branch office, a common method for forwarding traffic to the service edge is via a GRE or IPSec tunnel. However, the SSE vendor should offer an alternative approach. A virtual machine installed in the branch can simplify the complexity and ongoing administration of these tunnels and eliminate lateral threat movement by removing the customer-managed routable network. The deployment should be automated and include flexible traffic steering policies to the service edge with built-in SLA monitoring and failover. This option works well for medium and large branches and those that offer local services.

The previous option of treating every user like a remote user should be considered for smaller branches where no local services are offered (think about a coffee shop model). Given how recent events have changed the importance of the branch office, this option is desirable, as it allows no one on the corporate network and prevents the chance of lateral movement.

For users/things on unmanaged devices or third-party access to internal web applications, SSE vendors should provide similar SSE protection without the need to install an agent. Such users should leverage a web browser for user authentication that then provides zero trust protection by publishing an application-specific CNAME in your DNS zone so the web browser can automatically redirect those requests. Alternatively, the SSE vendor must also have an integrated cloud browser isolation (CBI) capability for agentless security for any unmanaged device anywhere. As a side benefit, this completely circumvents the need for a fragile reverse proxy.

With CBI, admins would configure a sanctioned cloud resource's SSO setting to redirect to the SSE vendor. After that, when users attempt to access said cloud resource from a personal or third-party endpoint, their traffic is sent to CBI automatically and without any software installations. It renders content into pixels sent to user devices, preventing downloading, copying, pasting, and printing. In this way, users can perform their work duties from unmanaged endpoints without the risk of data leakage and malware uploads, all while respecting compliance requirements.

For workloads connecting to workloads within the same VPC or data center, traditional network segmentation was the answer. While this made sense on paper, achieving network segmentation in practice was challenging. As such, SSE vendors must extend their user-to-application protections to workload-to-workload communications. With an agent installation on the workload itself, the SSE provider should determine risk and apply identity-based protection to your workloads, without any changes to the network, and should have policies that automatically adapt to environmental changes.

For workloads connecting to workloads across VPCs or CSPs or to the Internet, SSE vendors must again extend similar SSE protection offered for users to these workloads. As such, SSE vendors should offer a mechanism, typically via virtual machine (available in public clouds or on-prem hypervisors), that simplifies traffic forwarding to the service edge. The result is cyber threat and data protection to workloads reaching out to the Internet, as well as zero trust protection for workloads in one cloud accessing workloads in another cloud. With this approach, SSE vendors can consolidate multiple products (e.g., web proxies, firewalls, NAT gateways, URL filtering, etc.) into a single solution.

For securing data at rest in IaaS and SaaS environments, the SSE vendor must also provide solutions in the CASB, cloud infrastructure entitlements management (CIEM), and cloud security posture management (CSPM) space, so that API-based scanning with popular SaaS and IaaS applications can occur. Doing so allows for the identifying and remediation of misconfigurations and improper permissions within cloud environments, coupled with audit and scans of SaaS and IaaS platforms for data and threat protection. An SSE vendor should offer these out-of-band capabilities in tight alignment with their in-line capabilities to apply consistent policies to data at rest and data in motion.

The benefit of a single SSE vendor providing this broad blanket of protection is that it can be managed from a central control plane with corporate policies applied evenly and dynamically across all users/thing-to-application and workload-to-workload communications

⚠ What should I be aware of?

Deployment of SSE technology is highly dependent on the complexity of the organization's environment. **Therefore, gaining an understanding of user location, behavior, and access requirements, as well as application requirements is very important**. Also, certain countries like China present unique challenges with performance due to Internet controls that even flexible deployment models can't overcome. The SSE vendor should offer innovative solutions to deal with these challenges.

Outcomes:

Deployed correctly, these flexible, diverse, and scalable options will provide your organization with all the benefits of the Security Service Edge, regardless of where the user or thing may be, or where the application is hosted, and will even extend such protection within the application itself:

- The benefit of a single SSE vendor providing this broad blanket of protection is that it can be managed from a central control plane with corporate policies applied evenly and dynamically across all users/thing-to-application and workload-to-workload communications.
- Extending the same protection for managed devices to unmanaged BYOD and third-party access allows greater flexibility for contractors and employees.
- Workload-to-workload security affords DevOps and CloudOps engineers the same zero trust protections for their applications accessing other workloads, other clouds, or the Internet.

#5 Pitfall

Choosing an SSE solution that provides a mediocre user experience by not optimizing application connectivity or diagnosing UX degradations

Instead, consider SSE vendors that:

- Are transparent, easy to authenticate, and always on, ensuring that end users on their SSE platform are having a great user experience using objective measures.
- Correlate poor end user experience to its underlying causes, be it the endpoint, network, application, or security stack.
- Leverage partnerships with popular SaaS vendors like Microsoft 365 to minimize the latency between the public service edge and application provider's network

How the right SSE vendors make this work:

The SSE vendor's points of presence across the globe and Internet peering exchange relationships with providers and application vendors provide a powerful alternative to the backhauling and hairpinning required by legacy security stacks.

Beyond these architectural benefits, SSE vendors are uniquely positioned to measure and diagnose end user experience based on their presence on user endpoints and in the application data path. These advantages allow SSE vendors to understand user experience from the perspective of the user's endpoint and provide deeper diagnostics and scale by leveraging the public service edge infrastructure.

Focus on SSE vendors that have integrated a monitoring solution (commonly called **Digital Experience Monitoring** or DEM) into their existing agents and cloud infrastructure. Those vendors offering solutions that require additional agents or are loosely integrated acquisitions will not provide the same level of visibility and diagnostics.

The DEM solution offered by the SSE vendors needs to be broad—providing end-to-end visibility and troubleshooting of end user performance issues for any user or application, regardless of location. In addition, it should enable continuous monitoring for network, security, desktop, and help desk teams with insight into the end user device, network, and application performance issues. Finally, it should enable both reactive workflows helping to close employee-reported trouble tickets and proactive workflows helping to identify macro-issues (like regional ISP outages or global application downtime) before users ever notice. **This needs to be enabled with machine learning-based scoring algorithms, tracking normal vs. abnormal user experience by user, application, office, or geolocation**.

This monitoring should be at multiple levels, including layer 7 to provide insight into web application response times and layer 3 to understand network behavior, including hop-by-hop insight into path, latency, and packet loss. This analysis should also include self-diagnosis of the SSE vendor's cloud to identify if and when the SSE hop is inducing anomalous delay. Finally, the solution should provide insight into the user's endpoint device health and identify device events contributing to scoring drops **(see Figure 13)**.

SSE vendors are uniquely positioned to measure and diagnose end user experience based on their presence on user endpoints and in the application data path.

Microsoft Teams and Zoom Quality Performance Monitoring and Troubleshooting

With Teams and Zoom becoming the primary collaboration and communication platform for many organizations, measuring and diagnosing audio/video quality issues becomes even more pressing. DEM solutions provided by the SSE vendor should be able to interface with popular UCaaS applications like Zoom and Microsoft Teams to ingest audio and video quality metrics and marry them with deep, hop-by-hop network analysis and endpoint device analytics. By combining these data sets, the DEM solution should identify those having quality issues as well as provide a root cause for the problem.

Additionally, the DEM should leverage the scale of the SSE vendor's cloud, using it to proxy and cache telemetry tests, so that granular data can be collected from every end user, every few minutes, with minimal impact on the applications.

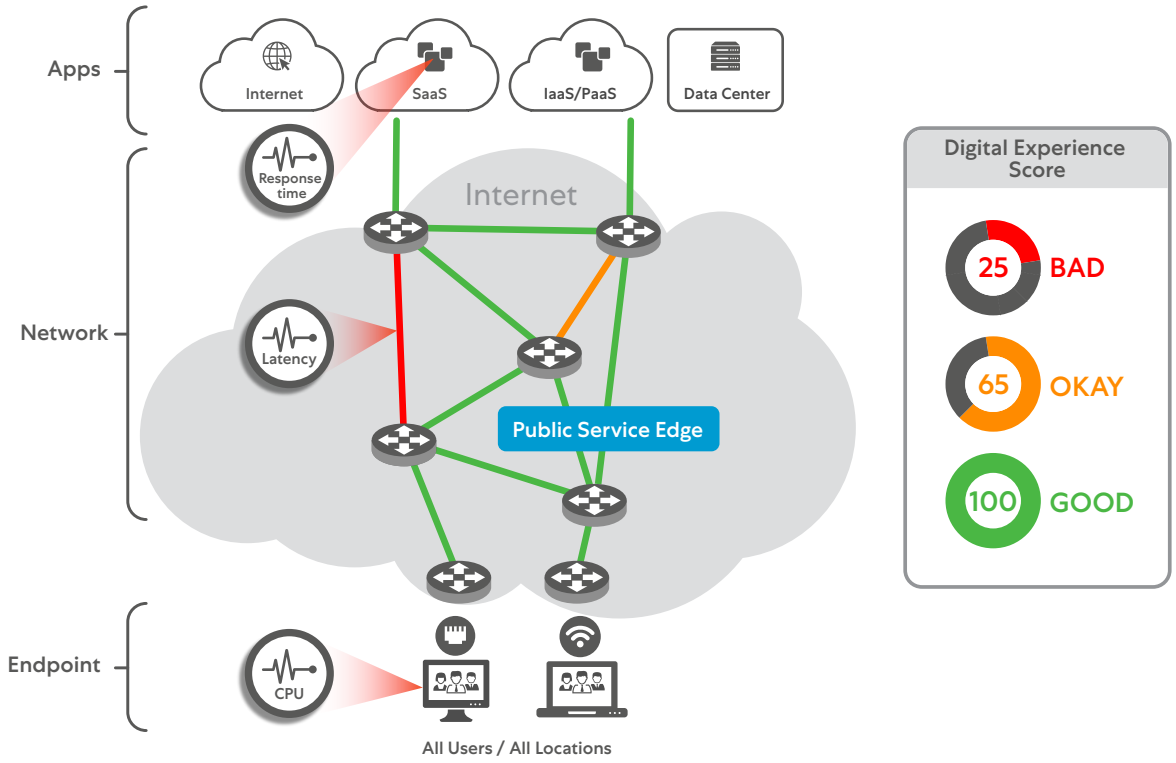


Figure 13: A DEM solution embedded as part of the SSE platform should provide unique visibility into the quality of the user experience from the perspective of the end user, shedding light on endpoint, network, and application issues

Be wary of legacy monitoring tools that take a data center-centric approach to monitoring and collecting metrics from fixed locations rather than directly from the user device. This approach does not provide a unified view of performance based on the user device, network path, or application, and offers little visibility when users and applications are not in the data center or on the corporate network. These tools create information silos and do not share any context, leading to fragmented visibility into the user experience and extended troubleshooting time. Point monitoring tools optimized for data centers leave visibility gaps for detecting, troubleshooting, and diagnosing end user performance issues across the Internet, whereas a modern DEM solution built into an SSE platform provides the widest range of data for root cause analysis (see Figure 14).

The DEM solution should identify those having quality issues as well as provide a root cause for the problem

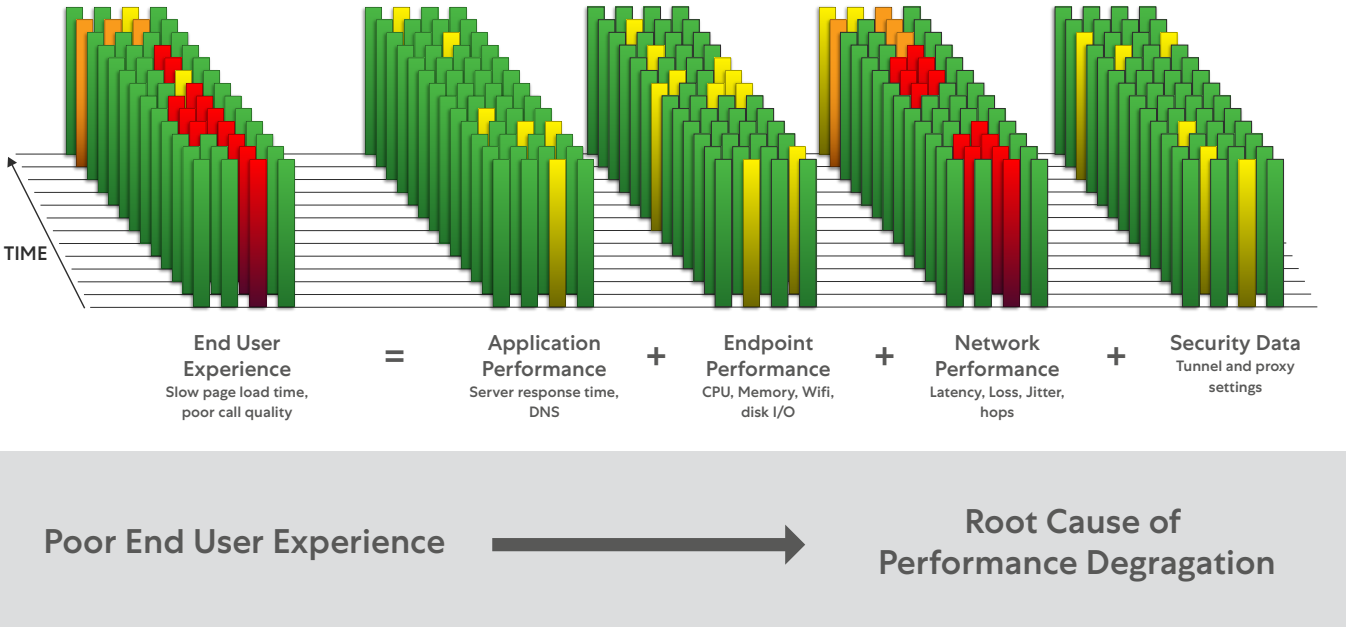


Figure 14: A DEM solution embedded as part of the SSE platform should provide unique visibility into the quality of the user experience from the perspective of the end user, shedding light on endpoint, network, and application issues

Optimizing M365 User Experience

A comprehensive SSE can go beyond measuring and diagnosing end user experience to optimize the performance of popular SaaS applications like Microsoft 365. The challenge is many companies centrally route traffic through hub-and-spoke networks and ExpressRoute. In addition, user traffic from M365 increases network utilization by 40% and most companies' Internet egress infrastructures just aren't up to the task and user experience suffers. Microsoft recommends direct Internet connections and SSE vendor architecture allowing for local Internet breakouts to provide optimal performance and cost.

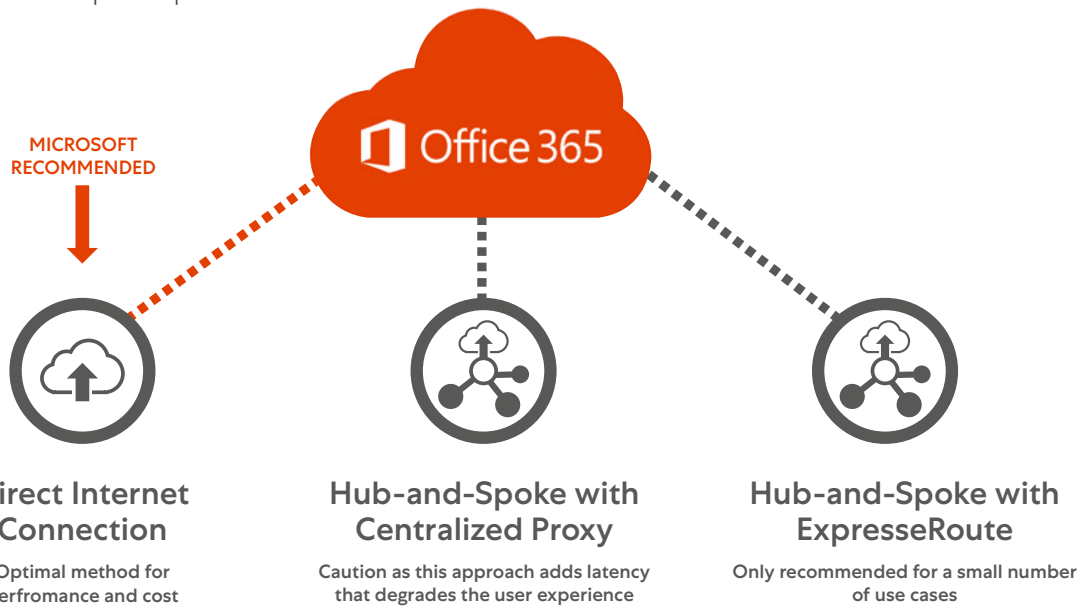


Figure 15: Microsoft recommends a direct Internet connection as the optimal method for performance and cost, aligning with the tenets of SSE (source: microsoft.com).

But architecture matters. The SSE vendor's points of presence across the globe and peering relationships with providers and application vendors need to bring the edge closer to the users for fast connectivity and low latency access. Look for SSE vendors that peer with direct fiber to Microsoft 365 in most major exchanges to reduce latency to approximately 1-2 ms round trip time, scale to handle the high number of long-lived connections, allow for rapid file downloads, and provide fast DNS resolution with fewer hops. (see Figure 15).

M365 transactions are especially important to secure with your SSE solution, as the inspection of applications like OneDrive and SharePoint is advantageous for the prevention of sensitive data loss. This also provides a full audit trail of every communication to and from the M365 applications. However, be aware that certain M365 applications like Teams may not need to be inspected, given that much of this traffic is voice/video via UDP.

⚠ What should I be aware of?

Given our work-from-anywhere (WFA) world, there are many weak links along the chain of delivering good application performance across the global mesh of wired and wireless networks. Optimizing user experience is difficult even with superior architecture and dedicated toolsets measuring and diagnosing UX issues. It is essential to establish reasonable expectations with end users about what constitutes an acceptable user experience of critical applications. It is then vital to use these expectations to build baselines to monitor and manage.

Diagnosing user experience issues is more of an art than a science. It requires excellent tools and architecture, but it is also dependent on having the right skill sets to interpret and act on the data. While DEM tools offered by SSE vendors will highlight most causes of issues (Wi-Fi, ISP, backbone, endpoint, or DNS problems), a subset will require escalation and additional data sets. For example, logs and packet traces may be required to get to the root cause. And there will also be a subset of issues that don't get solved at all, which is absolutely normal.

Beware of vendors that hairpin traffic. An SSE vendor's data centers should all be compute and inspect capable, allowing a faster and better user experience. The cloud-native architecture should not hairpin traffic to a few centralized locations for traffic inspection. For example, if a user pops up in Melbourne, their traffic inspection should happen locally with threat prevention and data protection services and not be backhauled to other regions such as Sydney or Singapore. SSE vendors that run their cloud on hyperscalers often end up hairpinning the user traffic. A hyperscaler may have 120 edge points but 80 percent of them are likely to be on-ramps to take traffic to a smaller number of hyperscaler data centers where SSE policy control can be enforced. It is important to understand how many data centers are on-ramps and how many data centers can actually enforce policy.

Outcomes:

The success of any transformation, be it digital, network, or security, is driven by how the end user experiences it. The ultimate goal of any SSE project is to improve the end user experience while reducing threat exposure and protecting sensitive data. Therefore, the ideal outcome is that an SSE vendor's ability to improve UX can be measured with the DEM capability—this should be an easy task, as moving away from hairpinning to a data center or away from VPNs are well-accepted ways to improve the user experience:

- The SSE solution should modernize the user experience and update the help desk experience. By leveraging a proactive approach to user experience, the help desk can react before users complain.
- The SSE solution should provide insight into real-time audio and video performance for collaboration platforms like Teams and Zoom.
- The SSE solution should collect metrics from the application, endpoint, and network layers to find anomalies and provide root cause determination.
- The SSE vendor must provide minimal hops between their cloud and popular destinations like Microsoft 365.

#6 Pitfall

Choosing an SSE solution with limited integration and orchestration with an ecosystem of third-party vendors

Instead, consider SSE vendors that:

- Integrate via robust APIs with other best-of-breed ecosystem players (like CSPs, SD-WAN, IAM, SOAR/SIEM, EDR, etc.) to ensure optimal protection and user experience.
- Leverage these integrations to enable automation and orchestration and reduce operational complexity and overhead.
- Don't add to technical debt by cobbling together a solution portfolio with limited integration both within the portfolio and with third parties

How the right SSE vendors make this work:

Most organizations struggling with technical debt realize that much of it is due to the procurement of vendor technologies over the years that fail to interoperate.

Worse is the so-called "platform" offered by a single vendor that is not really integrated, but a collection of acquired point products that have no real integration beyond a dashboard. Often these vendor technologies require specialized skills to operate and maintain a fragile coexistence with accompanying technologies. SSE can eliminate much of this technical debt with a unified security platform in the cloud supplied by a single vendor. Given this vision, SSE still lives among an ecosystem of complementary technologies, and vendors must regard interoperability with this ecosystem as a primary objective **(see Figure 16)**. This ecosystem consists broadly of other security, network, and cloud solutions.

Figure 16: Don't be in the desert with a vendor that doesn't have a rich ecosystem of third-party integrations, as this leads to technical debt, limited interoperability and a fragile (not agile) security stack.

To ensure fast, easy, and secure deployment and integration, the SSE vendor must provide integrations with leaders in:

- Cloud service providers (CSPs), both IaaS/PaaS and SaaS
- Endpoint detection and response (EDR)
- SD-WAN
- Identity and access management (IAM)
- Security information and event management (SIEM)/security orchestration, automation, and response (SOAR)
- Orchestration tools

These integrations must allow for orchestration between the SSE vendor and adjacent vendors to reduce complexity, TCO, and improve security posture (see Figure 17).

Cloud Service Providers (IaaS/PaaS and SaaS)

For internal applications shifting to the cloud or being built natively in the cloud, the SSE vendor must integrate leading IaaS/PaaS providers like AWS, GCP, and Azure to provide zero trust secure remote access connectivity to those applications. Doing so ensures that these applications are never exposed to the Internet, making them completely invisible to unauthorized users, connecting via inside-out, policy-based connectivity versus extending the network to them.

This approach ensures direct-to-cloud access without connecting through a remote access VPN, with the ability to leverage the scale advantages of the cloud provider without adding any network segmentation complexity. It doesn't rely on any virtual or physical appliances, and brings the advantages of zero trust to eliminate the attack surface.

For popular SaaS applications, SSE vendors should provide one-click integrations. In the case of Microsoft 365, the SSE vendor's integration should map all Microsoft IP ranges and domains for listed M365 apps, enabling transparent forwarding of end user traffic to their cloud. In addition, peering with Microsoft 365 reduces round trip time, improves scale, and allows for faster file downloads and DNS resolution.

SSE integration with other SaaS vendors like ServiceNow can improve data protection. By scanning new and existing ServiceNow data, the SSE vendor should identify sensitive data based on DLP policies and block outbound upload of sensitive data files. Integration with ServiceNow Security Incident Response can orchestrate response actions, including updating custom blocklists. Risky IPs, domains, and URLs can be blocked without manual intervention, while cloud misconfigurations can be closed to help reduce the risk of a breach.

Endpoint Detection and Response

The SSE vendor should integrate with various endpoint security partners to share telemetry, enhance mutual visibility, and orchestrate responses. Such integration allows for defense-in-depth to implement zero trust effectively and efficiently.

This integration should provide the ability to assess the user's identity, location, and device posture to implement appropriate conditional access policies automatically. In addition, cross-platform correlation and workflow can accelerate investigation and response. This entails:

- Assessing device health and automatically implementing appropriate access policies.
- Identifying zero-day threats, and correlating with endpoint telemetry to identify impacted devices to enact rapid responses with a cross-platform quarantine workflow.
- Investigating threats with endpoint and network context for effective detection and decision making.

SD-WAN

The SSE vendor should integrate with SD-WAN vendors to simplify traffic routing from the branch and make it easy to establish secure local Internet breakouts.

A joint SSE/SD-WAN solution can enable secure, policy-based access to the Internet and business-critical applications, and provide identical protection for all users, wherever and whenever they connect to cloud applications and the open Internet. SD-WAN solutions can be integrated with SSE through API integration. With this combined solution, enterprise branch offices can manage the surge of cloud and Internet traffic without backhauling to the centralized DMZ in the data center, using a hybrid WAN architecture for network transformation along with robust security.

It should be noted that any SSE vendor should be network-agnostic, and not exclusively tied with any network underlay solution. In fact, many of the benefits of SD-WAN are from its "software-defined" capabilities, but not necessarily the WAN, which inherently extends the corporate network and allows for lateral movement of threats. SSE decision makers should evaluate carefully the reasons for continuing to extend the corporate network to the branch and consider alternate approaches (like Internet-only) that are more secure.

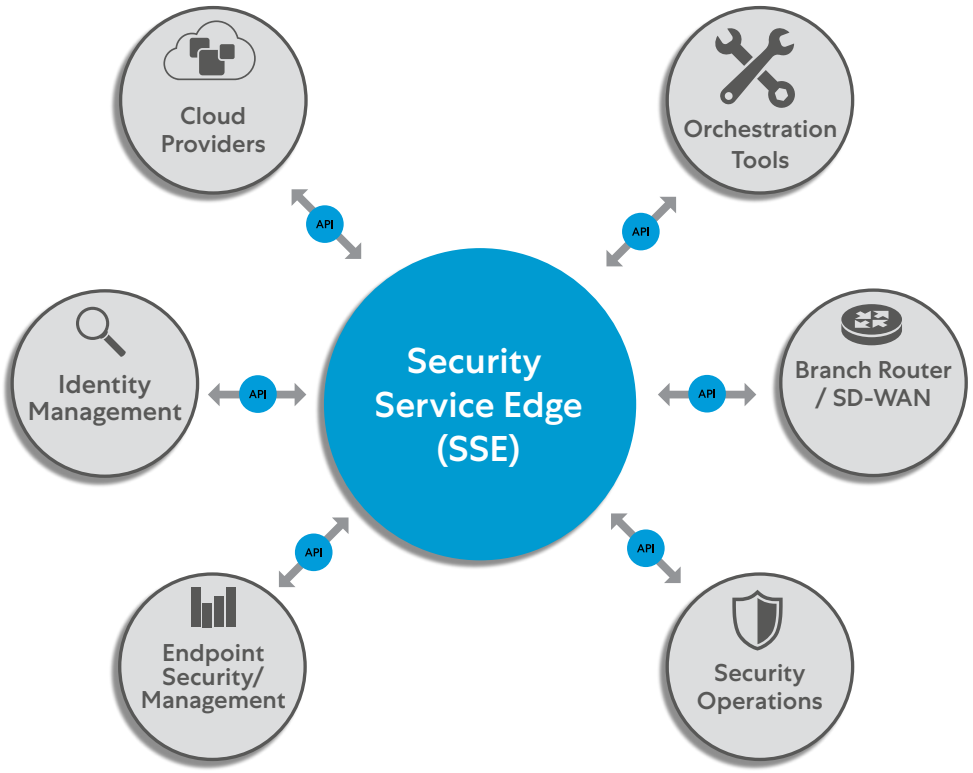


Figure 17: SSE vendors should integrate with best-of-breed players across various functions.

Identity and Access Management

SSE vendors should provide integrations with IAMs to enforce device posture-driven zero trust access and more effective enterprise-wide threat protection.

Using standards like Security Assertion Markup Language (SAML), deploying the integration should be easy. Users should be able to authenticate and secure Internet and internal application access. The IAM manages the end user access to applications through a combination of SSO and MFA while the SSE vendor secures the connection. Support for the System for Cross-domain Identity Management (SCIM) protocol enables all user information to be kept in sync between the two systems, including user group or job role changes and account deletions for instances of users moving on from the company.

SIEM and SOAR

SSE vendors should include integrations with SIEM and SOAR vendors in order to enable efficient and effective risk and compliance management with information enrichment and automation.

SSE vendors must have the ability to send log data in near real time to both on-prem and cloud-based SIEM/SOAR solutions to facilitate log correlation from multiple sources, thus allowing organizations to analyze traffic patterns across their entire networks. Additionally, organizations must be able to leverage log data in the SIEM to conduct extended historical analyses (> 6 months). Doing this ensures compliance with regulatory mandates through local log archival.

Orchestration Tools

As infrastructure as code (IaC) and DevSecOps forces security teams to "Shift-left," SSE vendors must provide the APIs for orchestration. Here, the focus is on internal applications where the instantiation of zero trust access is part of the application delivery lifecycle, enabled by orchestration scripts (such as Ansible or Terraform), particularly for user-to-application or workload-to-workload segmentation settings. Such orchestration allows zero trust capabilities to align with agile methods used by software developers.

As infrastructure as code (IaC) and DevSecOps forces security teams to "Shift-left," SSE vendors must provide the APIs for orchestration

⚠ What should I be aware of?

SSE decision makers must evaluate the depth of API integrations, the update frequency, and monitor shifts in the market that may impede future integrations (i.e., an acquired vendor becoming a competitor). Be cognizant of skills scarcity in your organization, as implementing these integrations—especially with legacy tools—will require specialized abilities

Outcomes:

SSE vendors offering rich, API-based third-party integrations provide operational efficiencies stemming from the ability to orchestrate best-of-breed solutions and reduce chances of vendor lock-in:

- SSE vendors that integrate with leading ecosystem players (like CSPs, SD-WAN, IAM, SOAR/SIEM, EDR, etc.) future-proof their technology and reduce technical debt.
- An orchestrated ecosystem of integrated vendors reduces operational complexity, overhead, and can decrease operator errors.
- SSE vendors that cobble together a solution portfolio through acquisition tend to fall behind in product innovation and often lack interoperability with third parties.

#7 Pitfall

Choosing an SSE solution that can't easily show value in a production environment pilot

Instead, consider SSE vendors that:

- Seamlessly pilot their solution with a single unified agent, access to a global set of service edges (close to the user), with a centralized and easy-to-use UI.
- Pilot the many aspects of the SSE platform with minimal additional deployment requirements.
- Provide the confidence that their solution will work as intended upon full deployment with minimal post-sales effort.

Figure 18: Ensure the SSE vendor test drive is with the real thing and not a toy replica. Only a pilot run in a production environment can prove the value of the SSE vendor's solution.

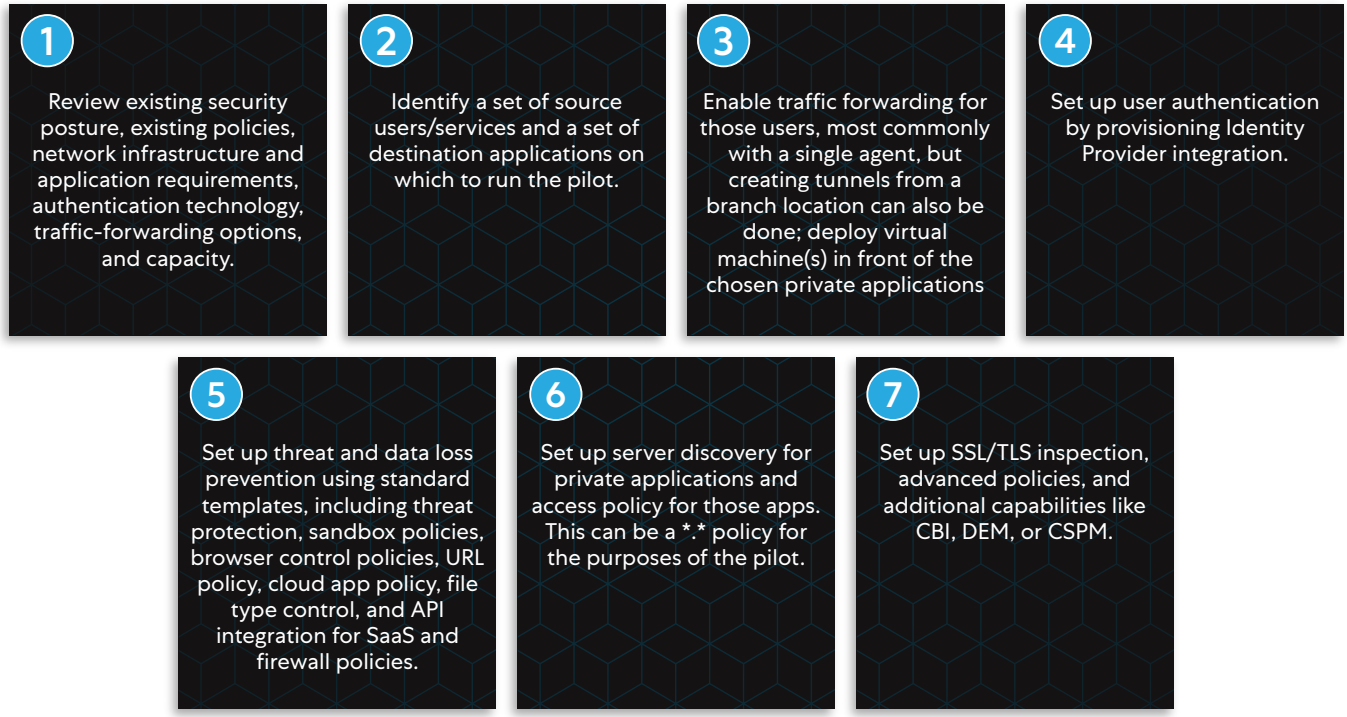
How the right SSE vendors make this work:

Adopting an SSE platform requires rethinking your security architecture, and so choosing an SSE vendor should not be taken lightly. The ability to understand the SSE vendor's true ability to work in your production environment is therefore critical. The ease by which this is done is representative of the architecture of the platform.

When considering SSE vendors, understand the steps required to run a pilot. For the right SSE vendors, the process should be finding a way to forward traffic to the SSE service edge, and then the SSE vendor's own cloud takes over. There should be minimal steps for the SSE admin to take, other than establishing a forwarding mechanism, configuring basic policies, authentication, and reporting. Of course, advanced policy configurations will take more time.

The pilot should address a set of business outcomes and involve members of various teams, including security, network, and desktop (for the installation of the endpoint agents, for example). However, the active involvement of these teams should be minimal—they are, after all, looking to acquire a SaaS solution. SSE vendors that require deep involvement, particularly from networking teams to handle complex routing scenarios in a pilot, should be a red flag.

Take a sequential approach that reflects your business goals when planning for a comprehensive SSE solution pilot:



All of the steps above should be straightforward and achievable by the SSE vendor in a short amount of time (most likely days) and without any major routing or configuration overhauls. While actual full deployment will require further steps, advanced policy settings, dealing with various types of applications and endpoints, and integrations and co-existence with other agents/technologies, the SSE vendor should be able to show the value of the platform through a straightforward yet well-executed pilot.

During the pilot, the SSE vendor must be able to prove the following, aligning with the six previous practices detailed in this document:

- **Global cloud infrastructure with minimal latency to the end user that operates with high availability and performance.** The vendor should demonstrate their ability to operate this cloud at scale and demonstrate the effect of failover.
- **Zero trust for every user session**, from protecting private applications, public applications, and even work-load-to-workload communications (if the pilot calls for this).
- **Advanced threat protection and advanced DLP by peering into encrypted traffic**. Certificate management may require some additional steps in the pilot, but proving the vendor's ability to do SSL/TLS inspection with minimal latency added is an excellent way to differentiate one SSE vendor from another.
- **Flexible deployment option**s. While this may not be part of the pilot, the SSE vendor must provide a plan to protect all users, regardless of location or application. It may require an understanding of deploying private service edges or CBI for contractors. The key point to verify is that the SSE vendor can meet the requirements of a distributed workforce and applications with their deployment models.

- **Optimal user experience**. This metric ranges from ease of use (how does the end user interface with their agent, for example), to the general user experience of accessing both public and private applications over their SSE platform. The vendor should be able to measure and diagnose a broad set of end user performance issues (Wi-Fi, ISP, CPU, etc.). This ability to measure/diagnose should be built directly into the SSE platform without the need to deploy any new agents.
- **Third-party vendor integration**. While this also may not be part of the pilot, the vendor must supply methods to integrate log data into an external SIEM tool or integration with an EDR tool in place. The SSE vendor should analyze the tool ecosystem in place and provide recommendations to integrate once the actual deployment begins.

Give preference to SSE vendors that require the least amount of overhead, given the skill and personnel shortage faced in the industry.

The benefit of going to a SaaS security vendor is to entrust the SSE vendor to handle duties typically handled by internal staff—the pilot should provide a clear indication how much effort deploying, managing, and updating the SSE solution will take.

⚠ What should I be aware of?

- Pilots cannot test every possibility, and unforeseeable issues could arise during an actual deployment.
- Verify that the SSE vendor is customer-centric and shows the desire to overcome any deployment issues that arise.
- Remember that you likely won't see scale in a pilot and may not see things break. SSE vendors may avoid ugly networking issues or routing issues during the pilot that may only be exposed during deployment. The right SSE vendor should be the one that doesn't rely on any network routes to function.
- Factor in the management overhead required—what will you own vs. what will the SSE vendor own? Figure out the effort required for a production deployment, plus for the ongoing maintenance of the solution.
- Some SSE vendors may not be true SaaS. Ensure that managing the SSE solution has the lowest total cost of ownership, especially important given the skills shortages faced by most IT organizations.

Outcomes:

A worthwhile pilot will prove the SSE solution is easy to deploy, performs in your production environment, and achieves your objectives

- SSE vendors that can seamlessly pilot their solution bode well for full deployments. With the goal of low TCO, a single unified agent, access to a global set of service edges, and a centralized and easy-to-use UI all make the ongoing maintenance of the solution straightforward. Any large-scale deployment will require time and effort, but the goal should be to work with the vendor that minimizes it.
- An SSE's architecture and design should make it easy to add on features with minimal additional deployment requirements (like additional agents or VMs). This way, buyers can take a phased approach to SSE, knowing that moving between phases will not require heavy lifts.
- Ultimately, the goal is to have confidence that the SSE vendor will deploy smoothly in a production environment and be by your side during unavoidable hiccups. Customer-focused vendors with proven architecture are your best clues that your security and network transformation investment will succeed.

Don't take our word for it

"Big bang" moments that allow enterprises to sharply invest in a new path are very rare. As such, enterprises must consider a measured approach to delivering SSE. The scope for enterprise SSE (as shared publicly through https://trust.zscaler.com), addressing all possible users, servers, devices, etc., is outlined in Pitfall #2. Below is how your contemporaries have addressed the adoption of SSE:

Reference A:

Customer deployed the Zscaler SSE platform for Zero Trust control of:

- End user granular access to private services
- End user Internet security, including in-line inspection and data protection
- Network transformation with users completely removed from network
- Protection of workloads, Internet, and private access
- Limited third-party access control

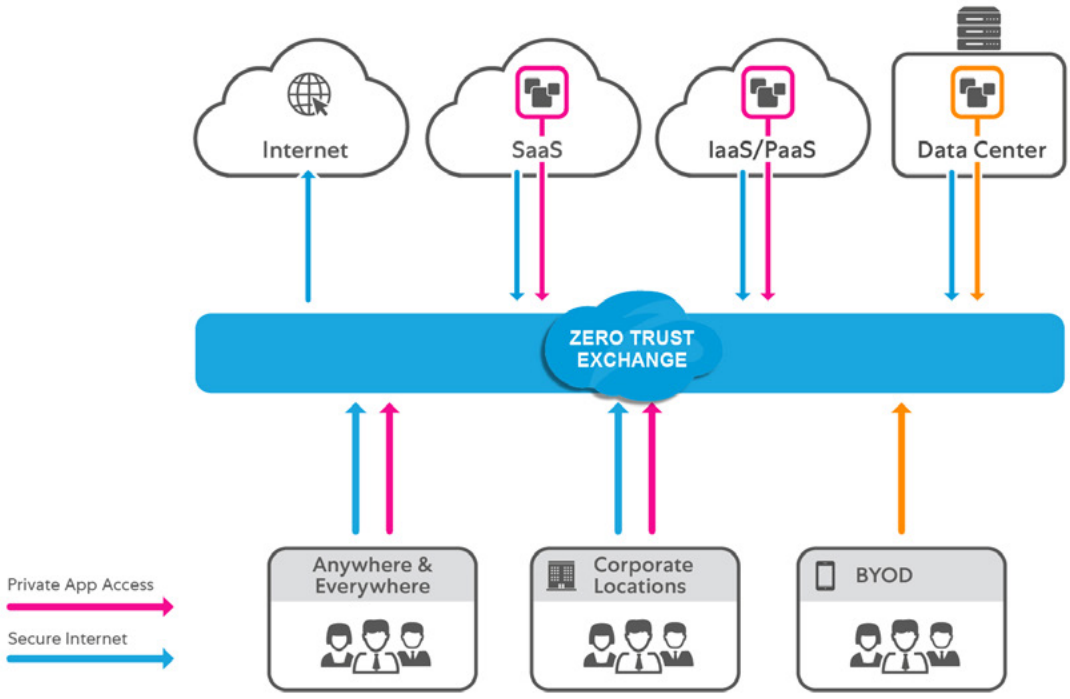


Figure 19: High level representation of enterprise-deployed connectivity with Zscaler

"In less than five days, we smoothly, safely, and cost-effectively transitioned 20,000 employees to WFA by replacing VPNs with Zscaler's zero trust network access solution."

Michael Alvmarken, Service Manager for Cybersecurity and Technology, Sandvik Group

"Leveraging the Zscaler cloud infrastructure and native integrations with ZIA and ZPA gave us the best data insights into our end users"

John Dawes, Director Enterprise Architecture, Reckitt Benckiser

"By not backhauling our traffic, but directly using the Internet, we expect we can drive down costs by 70%."

Frederik Janssen, VP Global IT Infrastructure Portfolio, Siemens

Reference B:

- Customer deployed the Zscaler SSE platform for:
- Complete visibility of access to all Internet services (cloud and beyond)
- Full in-line control to restrict corporate intellectual property loss
- Digital experience monitoring of user access during work from home

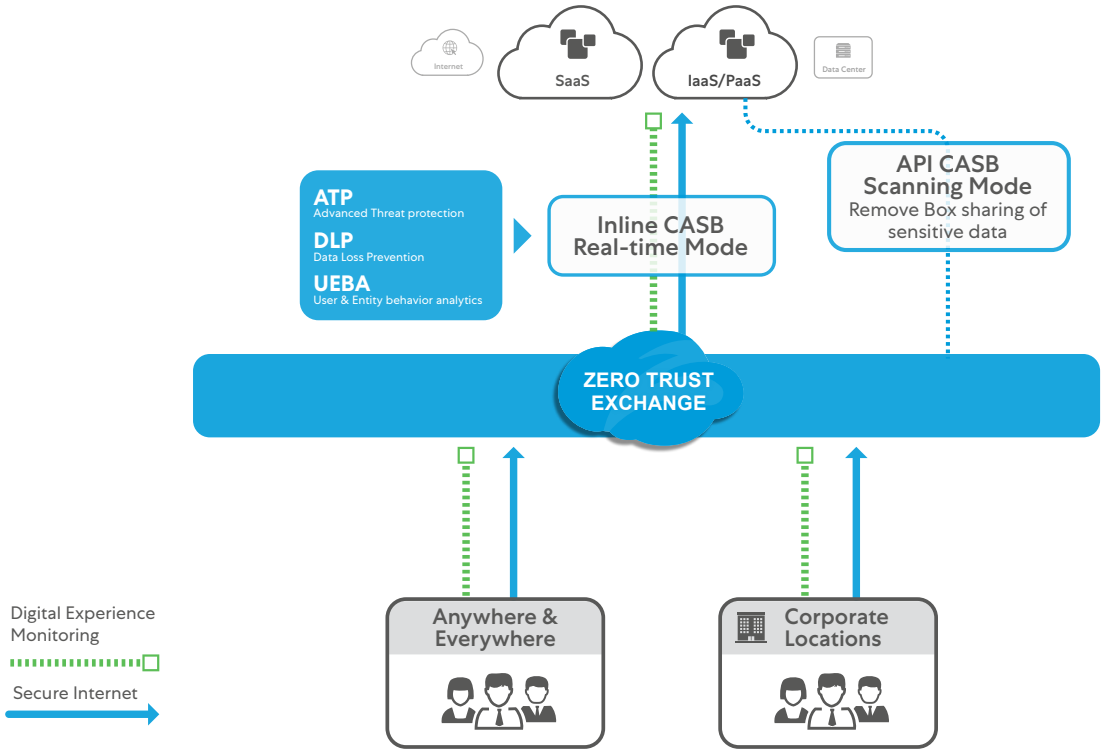


Figure 20: Example of in-line inspection and experience monitoring with Zscaler.

ciena

"We view Zscaler Digital Experience as a critical service in enabling a productive work-from-anywhere experience. We were lucky to solve 25% of user issues in the past. Now ZDX is the starting point resolving all of our user experience issues, and we can pinpoint the root cause 95% of the time."

Ed DeGrange, Principal Security Architect, Ciena

SIEMENS

"Whether it's a commerce or a fraud issue, something on the website, or internal fraud, everything has a financial impact, and that's why security has to be part of it."

Frederik Janssen, VP Global IT Infrastructure Portfolio, Siemens

BOMBARDIER

"With the Zscaler Advanced Cloud Sandbox, there's no heavy lifting for IT, which is critical as today's talent market is so tight that hiring is extremely challenging."

Mark Ferguson, CISO, Bombardier

Reference C:

Customer delivered granular protection of non-IT services using the Zscaler platform:

- Zero Trust to Operation Technology (OT), both employee and third party
- OT to Workload
- Cloud to Workload

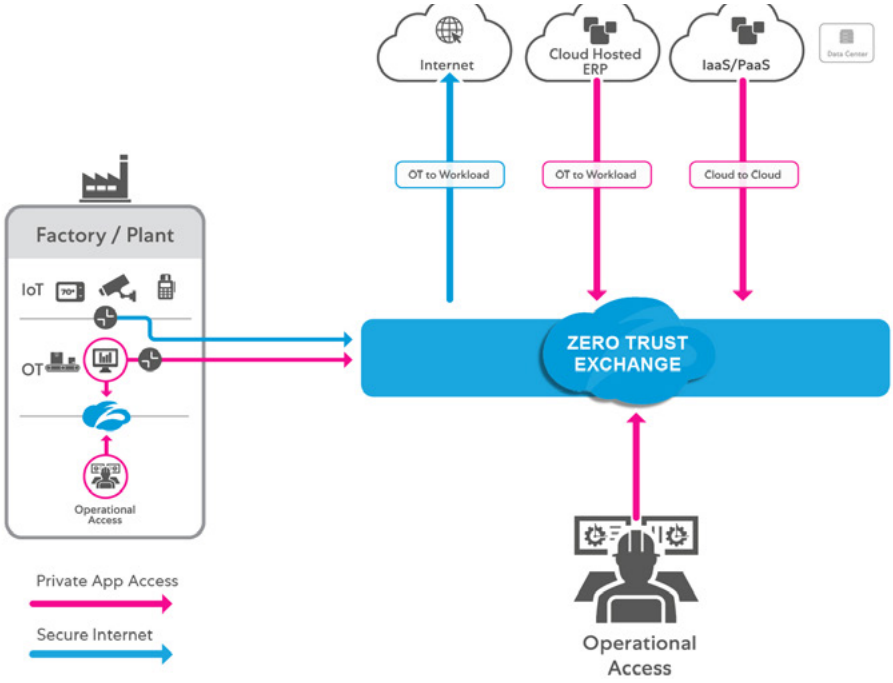


Figure 20: Example of in-line inspection and experience monitoring with Zscaler

Key Takeaways

- ☐ The SSE vendor must offer a documented SLA based on the loss of or degradation of service.
- ☐ The SSE solution must offer enforcement at all sites—in-line, globally, and within carrier-neutral peering points, ensuring the most effective path to customers.
- ☐ The SSE vendor must deliver zero trust controls for all authorized enterprise users, workloads, and devices through any protocol.
- ☐ The SSE solution must deliver a service agnostically over any network.
- ☐ The SSE vendor must provide its in-line inspection through a proxy cloud architecture ensuring minimal latency and enabling full visibility of all web traffic (up to and including TLS 1.3).
- ☐ The SSE solution must provide multiple security controls through a single memory scan architecture for unique scalability advantages for decryption at scale.
- ☐ The SSE vendor must provide its solution as managed centrally and deployable in multiple forms to address customer location, region, locality, and function customization.
- ☐ The SSE solution must be extended to provide protection for unmanaged BYOD, third-party, and partner access with the same level of granular control as employees.
- ☐ The SSE vendor must optimize the user experience by monitoring and diagnosing performance issues for enterprise services (Teams, Zoom, etc.).
- ☐ The SSE solution must collect metrics from application paths, endpoints, and network layers to identify anomalies and provide insight to support teams.
- ☐ The SSE vendor must integrate with best-in-class ecosystem players (like CSPs, SD-WAN, IAM, SOAR/SIEM, EDR, etc.), bringing complete in-depth control and security to the entire enterprise landscape.
- ☐ The SSE solution must be integrated with these vendors to provide orchestration to minimize operational overhead.
- ☐ SSE vendors must be able to seamlessly pilot the functions and locations needed by the enterprise in production.
- ☐ The SSE solution must be simply extensible without the need for additional hardware or agents, allowing enterprises to grow their SSE use through a phased approach.

For more on SSE please visit Zscaler SSE 2022

About the Authors

Sanjit Ganguli (VP, Transformation Strategy / Field CTO) and Nathan Howe (VP, Emerging Technology & 5G) with careers spanning the globe and companies such as Gartner, Nestle, Riverbed, and Verizon, bring a leadership and innovative view on cloud, security, transformation, and emerging technologies.