The Painless Guide to Implementing Security Service Edge

The plan for migrating to SSE quickly and easily

Forcepoint

CDW.com/forcepoint

Table of Contents

Preface

Organizations across the world must provide critical resources to employees anywhere, anytime in a highly secure environment—often without the luxury of abundant headcount and funding to tackle the task.

To keep resources available without exposing networks to risks, CIOs and CISOs have been layering complexity on top of complexity with more security applications and fewer IT professionals to manage them.

Now, many are turning to converged cloud security platforms to help harden networks and minimize the administrative overhead needed for tasks like maintaining version upgrades, supporting systems on-site and migrating applications and data to the cloud.

Gartner® refers to this converged approach as Security Service Edge (SSE), the security component of a Secure Access Service Edge (SASE) architecture. SSE can ease the stress of security management by providing consistent visibility, control and protection over your organization, your users, and how they interact with resources.

Gartner® predicts that, **"By 2025, 80% of organizations seeking to procure SSE-related security services will purchase a consolidated SSE solution, rather than stand-alone cloud access security broker, secure web gateway and ZTNA offerings, up from 15% in 2021."***

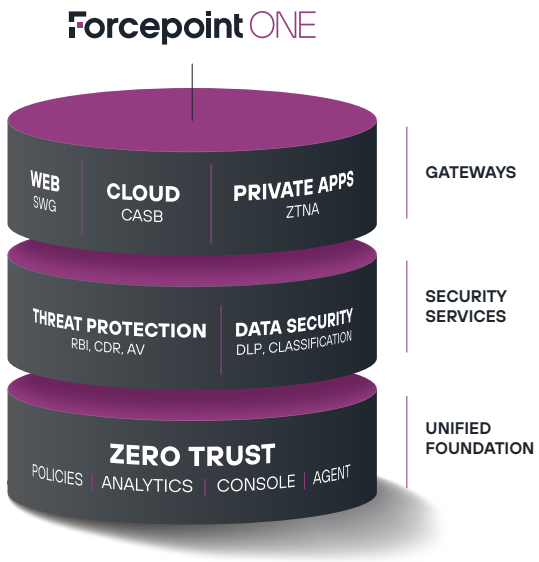

Figure 1: The Forcepoint ONE cloud-native SSE platform

Forcepoint ONE, the SSE solution from Forcepoint, is an all-in-one, cloud-native security platform that makes it easy to adopt Zero Trust. Forcepoint ONE brings together essential security capabilities, including three secure access gateways (CASB, SWG, and ZTNA) and a variety of shared threat protection and data security services. This approach to simplifying security enables organizations to manage one set of policies, in one console, communicating through one endpoint agent.

Gartner, Magic Quadrant for Security Service Edge, Lawrence Orans, John Watts, Craig Lawson, Charlie, Winckless, 24 January 2022, Updated 30 March 2022.

Regardless of the benefits of an SSE platform, the question always comes down to migration. Which obstacles might crop up? How can you migrate your disparate security tools and policies to a single platform without interrupting the flow of your business and putting your applications and data at risk? What if you're confident you can replace VPN with ZTNA now, but aren't ready to migrate to CASB or SWG?

This guide will walk you through our seven-stage strategy for migrating to an SSE platform using Forcepoint ONE as the model. We'll show you how to move from your current environment to that future state seamlessly in as little as 45 days, spending 10 hours a week on average, without interrupting your operations. And we'll show how to plan for further enhancements, as you expand or add additional capabilities to your deployment after the initial migration

Forcepoint ONE can do this with no patchwork or surprises. Working with you and your implementation partner, the Forcepoint team will lead or support the migration through a consolidated, proven approach that provides complete visibility every step of the way.

Forcepoint ONE Migration Timeline

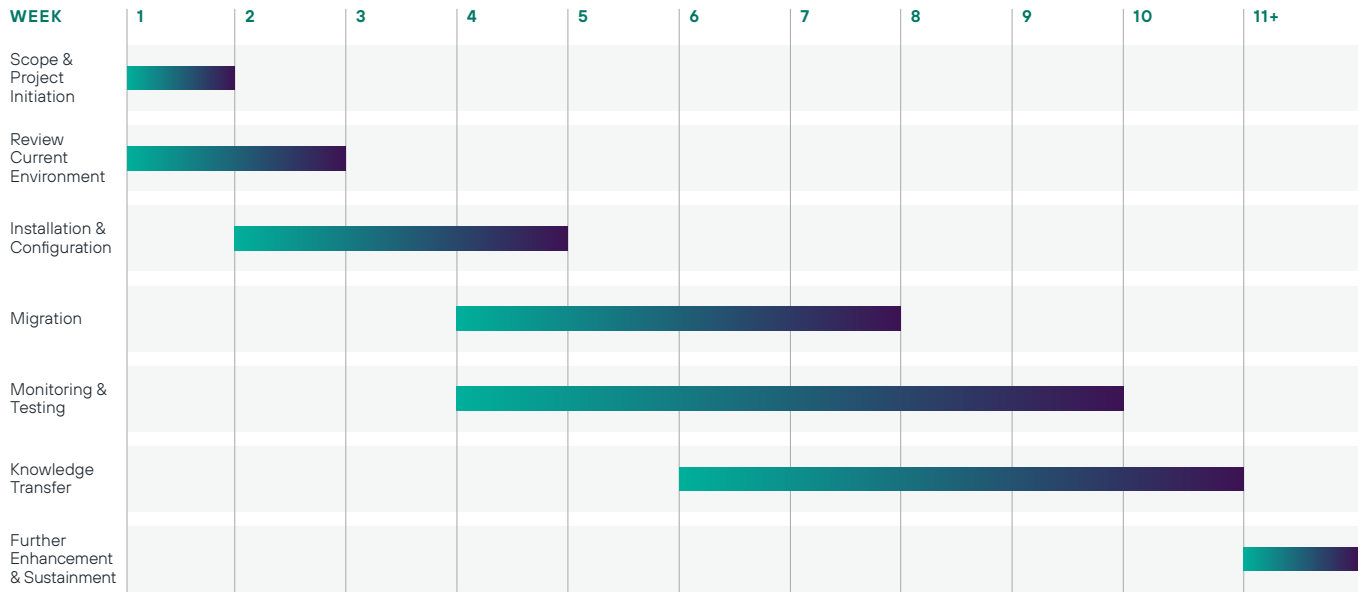

Figure 2: Sample timeline for migrating CASB & SWG services

This is an example of an 11 week migration timeline conducted for a company of over 5,000 employees. In most cases, Forcepoint can complete the entire process between 45 and 90 days. We'll do the heavy lifting for you. Based on experiences with other clients, we'll share best practices and identify potential risks and issues before they occur.

Our 11 week program is focused on getting you up and running with one SSE capability, like SWG or CASB. We'll start with a review of your environment and identify the work to be completed. Next, we move to the installation and configuration of the new platform, followed by migration of policies, monitoring, testing, and tuning. We wrap up with a knowledge transfer, so that you're enabled to expand to securing additional applications or prepared for deploying further SSE services. However, our job doesn't end with the initial migration project, we are here throughout your time as a customer to ensure sustained value with our platform and provide ongoing enhancements and additional capabilities as you require them.

Now, let's look at the first step of creating the scope and starting your migration project.

Step 1 – Scope and Project Initiation

The hardest part of any migration is knowing where to begin. What are your short-term and long-term goals? Think of them in terms of "values" or "wins":

- → What do you want to achieve first to demonstrate success internally to leadership?
- → What are your biggest and most important use cases?
- → What teams need to come together to make the migration a success?

We will help you identify your goals and necessary steps in a way that ensures complete accuracy, visibility, and accountability. With Forcepoint, you'll measure twice and cut once while building your SSE migration.

Based on our experience with hundreds of other client SSE migrations, 90 percent of use cases will focus on securing and controlling web (SWG) and SaaS (CASB) access aligned to business needs. You can begin by migrating one gateway, such as SWG, then leveraging that migration experience to easily deploy CASB to bring visibility to cloud apps or ZTNA for controlling access to private apps without VPNs. While feature acronyms are important, we will focus on what's integral to your business and how to ensure your end-users have fast and safe access to the resources they need, no matter where they are or what devices they're using.

Forcepoint and your migration partner will map out a way of recording wins quickly so your company can see progress, such as safe access to websites, early in the migration.

We'll also align your teams effectively for departments to unite and collaborate on a shared strategy. It's vital to bring together the network and security side of your organization. After all, that's the key to making security simple: merging connectivity and security using a SASE architecture. Whether it involves a security team, DevSecOps team, or network team, we'll work with them to understand their needs and show how everyone in your organization will benefit from the migration.

And then, with all that information in mind, we'll develop and maintain a timeline like the 11-week example in Figure 2, so that everyone knows exactly where things stand during every step of the migration journey.

Step 2 – Review Your Current Environment

With insights into your goals and use cases, Forcepoint and your migration partner can review your current architecture. Whether your security is outdated, recently updated, or includes a variety of products, we take the time to consider all aspects of your architecture to design an implementation plan tailored to your specific needs. This is done to ensure your success using Forcepoint ONE.

It is also a good point in the project to cement and share your goals you identified in the previous step and understand the metrics by which you'll measure success. It's critical that everyone knows what "good" looks like to you. The implementation plan will reveal exactly what's being deployed and configured, and how long it will take to complete.

We will use this time to identify and map your policies. No two policy mappings will look alike. Customers typically have multiple security services and gateways, so we're prepared to map across multiple components. We'll take our time and leverage our experience to establish policies carefully based on industry best practices and your individual needs and use cases.

Similarly, our teams will also review the efficiencies of your architecture. While whiteboarding and mapping out the implementation process, we can identify policies that you no longer need or can improve and make those changes now as you transition to a new, converged architecture.

This step serves as an opportunity to show how the SSE technology works, ensuring it's covering everything appropriately. You'll know what it will look like when it goes live, what to expect, and how to address issues or activities as they occur early in the implementation and workflow.

Forcepoint ONE Implementation Plan.
We tailor the implementation plan based on the organization's specific needs, goals, and timeline, while still mantaining engineering best practices. This approach minimizes risks and achieves the desired outcome.

Forcepoint ONE Trial Environment.
Forcepoint hosts two clouds: Configuration can first be tested in the Trial cloud with test apps and users, before migration to the production cloud with real apps and real users.

Figure 3: Sample Implementation Plan

Step 3 – Connecting and Configuring

Now comes the easy part: connecting and configuring your new SSE platform, Forcepoint ONE. With a firm knowledge of your goals and architecture, we will start with identity provider integrations and then move on to integrations specific to the set of SSE services to be used: cloud apps, private apps and/or web access.

For this step, Forcepoint hosts two clouds. First, we create the trial environment to test application connections and new policies. Then we apply the successful connections and policies to the production environment with production tenants and real users.

We take this time to explore any previous policies that existed along with the new architecture. This is where the expertise of Forcepoint and its partners can really shine through. We work together to identify opportunities to optimize, simplify, and improve policies on access and use of a website or application. For example, we can look into patterns of access to applications and websites, file uploads and downloads, sensitive data being moved across apps or sites, malware detected from websites or user uploads, managed versus unmanaged device access, and all the associated reports and dashboards that may be necessary. You can take user groupings from identity providers and apply granular policies around any of these elements that an organization may need to control.

Often, we can help customers reduce the total number of security policies while also covering more use cases, driving a more efficient and effective way to do security.

For those that may not have been using DLP policies previously, Forcepoint ONE offers a wide range of out-of-the-box policies. The highly effective, pre-defined DLP policies result from our real-world experience with customers and can help you show quick and meaningful ROI to be the next hero or rock star your organization is looking for.

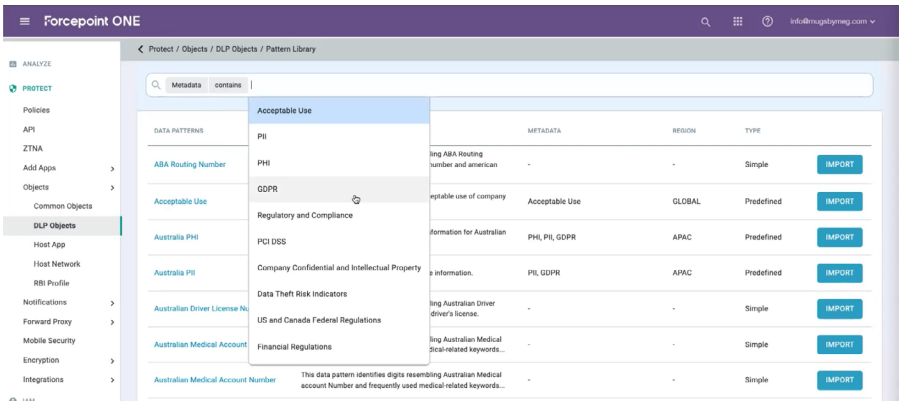

Figure 4: Forcepoint ONE data classifier library has over 190 pre-defined templates

Step 4 – Migration

After connecting and configuring your new Forcepoint ONE environment, we can begin the migration phase, starting with a small pilot group and gradually implementing more robust policies. We work with the endpoint management system you use to roll out the Forcepoint agent to managed devices.

Here, your network team will take over for the security team, which has been leading the process. Network teams play a critical part of the migration, and the earlier collaboration between teams starts, the better things go.

Teams will also set up a small User Acceptance Testing (UAT) group to ensure there aren't any unforeseen conflicts between speed and access, on the one hand, and security policies, on the other. This step is crucial to prevent any surprises for the company later and why it is necessary to have a diverse set of users in the UAT group with varying levels of technical proficiency.

> **Don't just fill the group with IT network and security teams. Include less technical members to help identify communication needs up front, which will make things easier on you in the long run.**

For migration success, we want to ensure that the admins and end-users all understand what types of policies will be implemented so they are comfortable working in the UAT group. We suggest rolling out internal blog or wiki pages to address common issues. That way, team members can focus on doing their jobs as normal and not on determining whether they are being protected.

Step 5 – Monitoring and Testing

Once we connect services and migrate policies, we monitor for efficacy and user experience to fine-tune the policies. We begin testing during the first couple of weeks with at least two business-critical cloud or private applications (CASB or ZTNA) and a couple of external websites (SWG). We want to check in daily on the performance to verify we have the right policies in place.

For example, perhaps we went a bit too far in blocking a particular data set, and we might need to adjust settings. You could select a different option in the policy and confirm the results. This stage is where we're trying to make things work as seamlessly as possible for the admin and the user population. From there, we can begin expanding to more business-critical applications. And then continue to fine-tune as we go.

Even though it looks on the timeline to be the longest phase, it doesn't mean more of your time. The migration team will not be with you 40 hours a week for five or six weeks. Rather, we will check in frequently for five minutes to monitor, test, and adjust where we can. Depending on your comfort, we can begin implementing more aggressive blocking actions, such as stopping the download of a sensitive file from a cloud app to a user's corporate laptop. Or you could prevent someone from sharing a file to another user via Slack. As we go, we can get more granular with individual access rights. Maybe you'll allow logins from a personal device or restrict access from certain regions.

It's important to move at your comfort level, especially if you are building out DLP policies using custom match patterns. Moving from an audit mode to actual blocking can be a hurdle for many organizations. We are here to help you with that transition. We understand how data security works and we want to give you as much help as possible. Once we make the switch to block actions, we won't introduce friction to your organization.

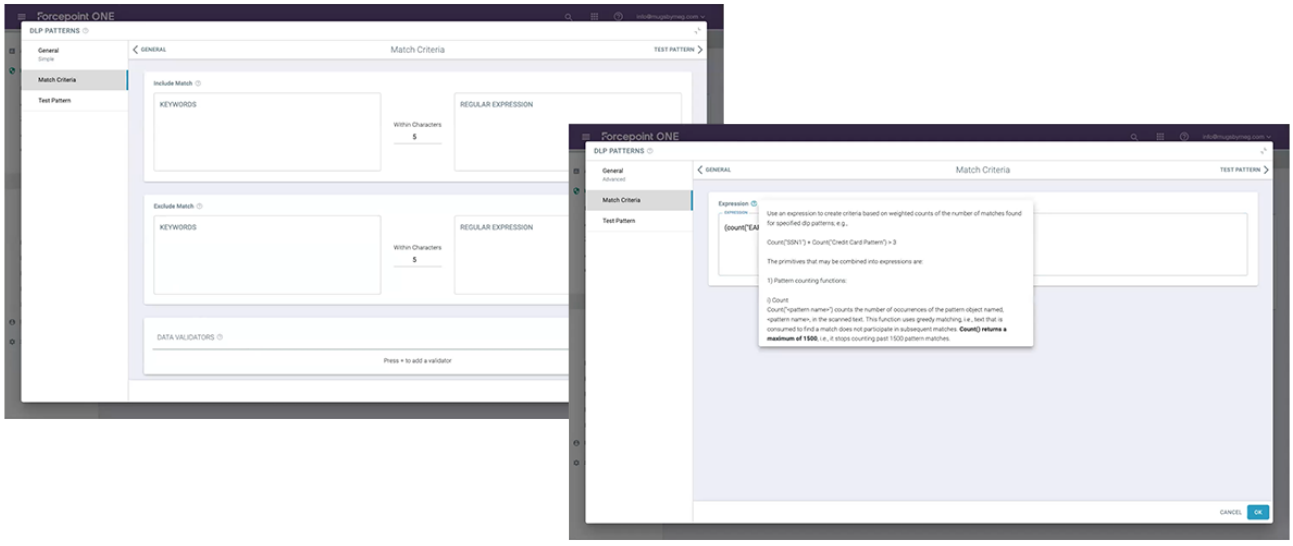

Figure 5: Building DLP policies using custom match patterns in Forcepoint ONE

Step 6 – Knowledge Transfer

Even though knowledge transfer is near the end of the process, we like to think of this as an ongoing informal activity throughout the entire process. We consistently transfer knowledge through multiple approaches so you get the most out of Forcepoint ONE.

Documentation

Part of the knowledge transfer involves the constant availability of implementation documents, knowledge base articles, architecture diagrams, and high-level/low-level design (HLD/LLD) diagrams. These documents and other resources will show how to conduct multiple tasks like opening a support ticket.

Table-Top Exercises

We will conduct table-top exercises to help everyone on your team understand how to respond to issues. An exercise might involve how to respond to a help ticket in under ten minutes. Or it might involve how to support a new use case. Overall, you and your team will learn how to best triage issues, tackle alerts, and understand roles and responsibilities. Consider it like a fun safety drill without all the stress.

Project Handover

We will work with you to conduct a thorough project handover to your account manager. We want to align everyone and make sure stakeholders understand all aspects, ranging from knowing the short-term and long-term goals, how the environment is configured, and why. This starts around the time of the pilot stage and continues throughout the process. We'll help establish institutional knowledge so that you're prepared to own the solution.

Ongoing Training

The Forcepoint team is available with resources and documentation before, during, and after any migrations to make sure you have the tools you need to train your staff, hire well, and develop the right people to support your implementation. Often, we're part of a de facto residency for months at a time or for further enhancements. We want to ensure you're taking advantage of new services you may add, such as Remote Browser Isolation (RBI) to stop threats from risky websites, and understand any new challenges that arise.

Step 7 – Further Enhancement and Sustainment

Just because the initial migration is over doesn't mean we're finished making your SSE better daily. At any point in your relationship with Forcepoint, you have the option to add or upgrade to additional functionality as we continue to enhance and develop the Forcepoint ONE platform. With Forcepoint ONE, you can easily add new security services that are managed from the same console.

Upgrade Support

Forcepoint ONE licensing allows you to upgrade support for additional dedicated personnel. The first level is Essential, and the next level up provides a Customer Advocate dedicated to a handful of accounts. The top level of Enterprise gives you a dedicated Technical Account Manager (TAM) who works on just a couple of accounts.

Add More Applications

With Forcepoint ONE, you have the option to expand to secure more internal applications. The initial migration might cover three to five applications, such as your CRM, collaboration, and communication tools. Later, you can extend support to other apps like cloud storage, which we can help you execute.

Expand Core Services and Enhance Capabilities

Forcepoint ONE gives you flexibility and choice. Not everyone will want to deploy all the core SSE Gateways at once. If you first implemented CASB for SaaS apps and SWG for websites, afterward you can replace VPN with ZTNA for private apps. Every app, whether protected by CASB or ZTNA, appears on your single sign-on (SSO) page to give your users the best, most consistent experience.

You can also enhance security capabilities. Say you want to go beyond antivirus scanning: you can integrate RBI for zero-trust web browsing or Content Disarm and Reconstruction (CDR) to sanitize files of any threats before the documents get to your network or users' machines. You could further augment malware protection with CrowdStrike Machine Learning. You can do all this easily with Forcepoint ONE.

Refine Your Data Security

Along with expanding across the applications you want to protect, you can refine your data security. You might, for example, have identity-based access control but want to go deeper on data security. You could also change access permissions and control what's seen inside and outside of your organization. Forcepoint resources help you easily do all of that. You can add Forcepoint Classification which uses machine learning-based AI to facilitate data classification tagging.

If you want to simplify connectivity and control of your branch offices or remote sites, you could combine Secure SD-WAN to SSE for a complete, Data-first SASE solution from Forcepoint.

For more SASE insight, download the new Gartner® report: 2022 Strategic Roadmap for SASE Convergence.

Deciding When to Migrate to SSE

Industry analysts like Gartner® agree on recommending SSE and SASE as the way forward for security and business leaders. Your SSE journey really should start with the most critical business needs. This holds true whether you want to adopt all SSE capabilities initially or one at a time.

With the right partner, you can migrate in phases from the starting point that matters most to you. For some security professionals, cloud applications might be critical. For others, it could be access to proprietary applications. No matter what, you can keep using your current investments until you're ready to make a clean break to SSE.

A perfect time for migration might be when an existing security investment is up for renewal. Even if that point is six or 12 months down the road, we can take the first few steps at your pace, as slow or fast as you need. When it's all said and done, migrating to the Forcepoint ONE SSE platform is the fastest path toward simplifying security—it will help you lower risk, reduce cost, and unlock efficiencies at a scale that you can't achieve with point products.

Ready to Simplify Security?

Visit our solution Forcepoint ONE solution page for more information, or to schedule a demo with one of our SSE experts. To find out more about migrating to SSE, watch the supporting migration guide webinar: A Seven Stage Strategy to Migrating Security Service Edge.

Forcepoint

CDW.com/forcepoint

About Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, Twitter and LinkedIn.

[FP-Whitepaper-The Painless Guide to Implementing Security Service Edge-US-EN-CDW] 05Dec2022