

The Painless Guide to Security Service Edge (SSE)

Why SSE matters, how it works, and what it does for you.



Zapraszamy do kontaktu!
Więcej informacji: www.kreski.pl

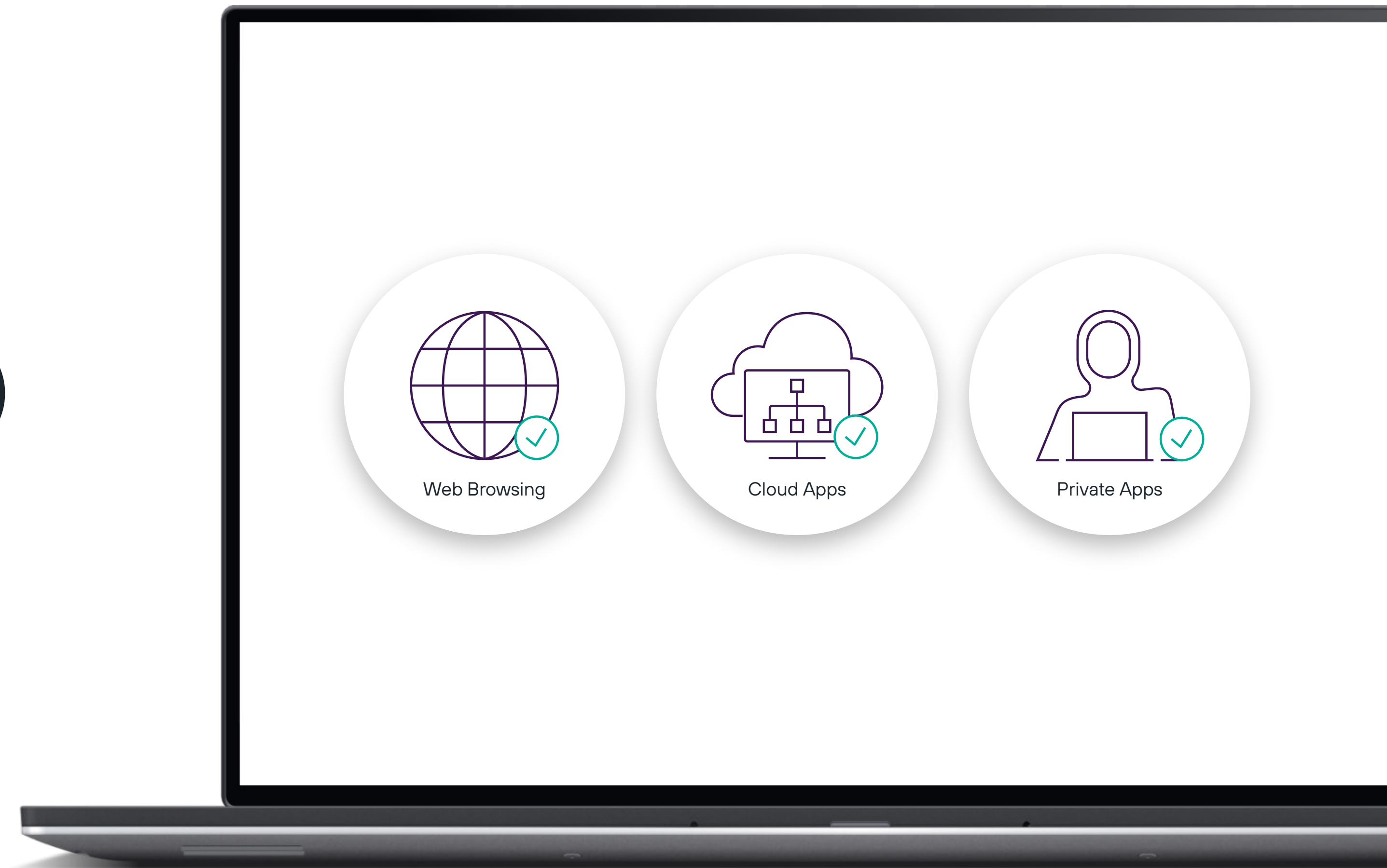


Table of Contents

“By 2025, 80% of enterprises will have adopted a strategy to unify web, cloud services and private application access from a single vendor’s SSE platform.”

PREDICTS 2022: CONSOLIDATED SECURITY PLATFORMS ARE THE FUTURE, GARTNER®

03

Complexity is the enemy.

Convergence is the key to executing a zero trust strategy.

06

Under the SSE Hood.

Exploring the core services.

08

How SSE Works: A Day in the Life of Kris.

Three scenarios of data risk.

12

Forcepoint ONE: Converged Security that Fits your Needs.

Deployment options & additional capabilities.

13

Drive Immediate Value from SSE.

See the benefits of migrating.

Gartner, Predicts 2022: Consolidated Security Platforms are the Future, Charlie Winckless, Joerg Fritsch, Peter Firstbrook, Neil MacDonald, Brian Lowans, 1 December 2021

Complexity is the Enemy

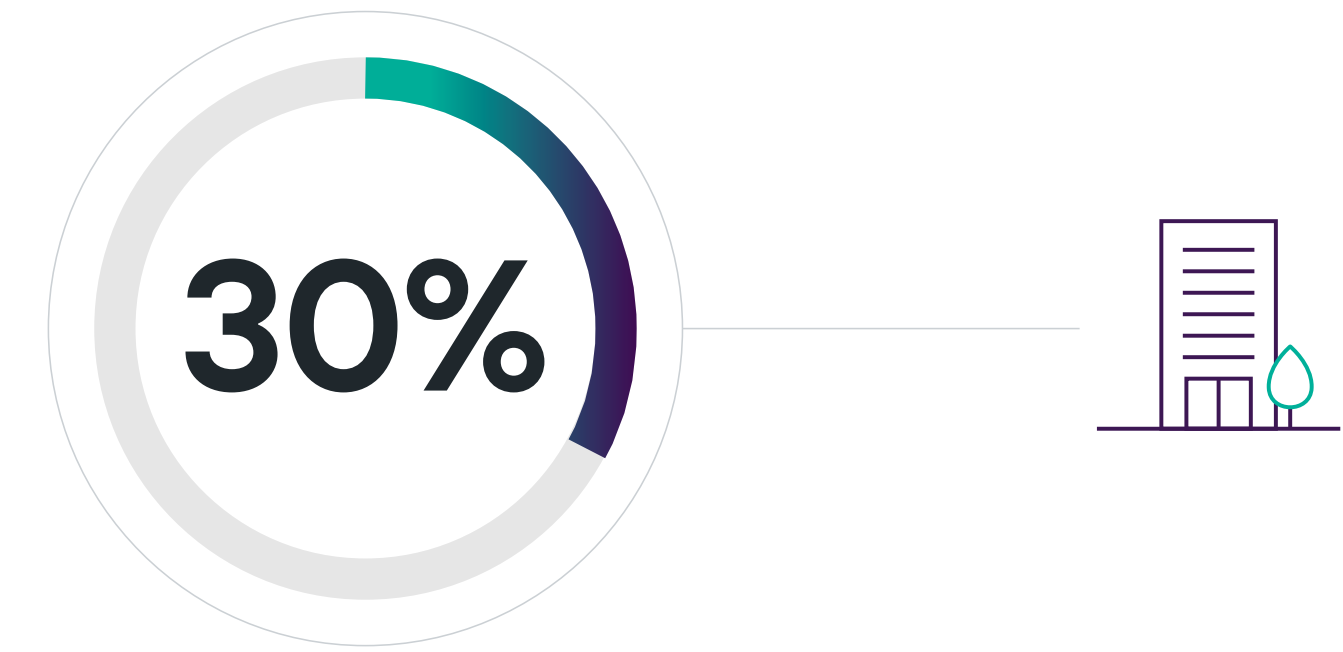
Look around. Your business or mission is now digital-first, and your apps and data can't get to the cloud fast enough.

It'd be awesome if security could transform, too. After all, the cyber crooks are getting smarter, raking in more money than most countries' economies. Your employees are working remotely wherever the internet is available, with both company-issued and personal devices at hand.

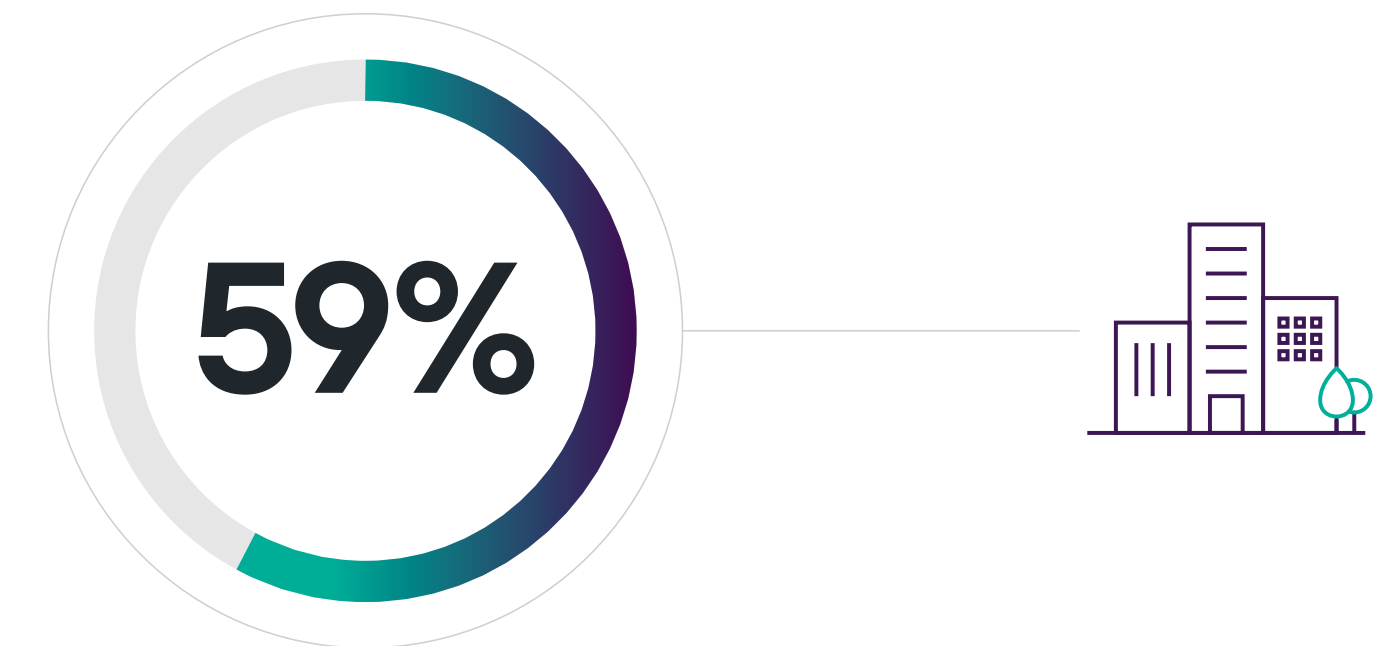
Where to look first? You're already managing more tools than ever. Each has a proprietary console, generating their own set of alerts and false positives, which introduces yet more risk and requires the implementation of orchestration tools, incident response, and [SIEMs](#).

The resulting complexity and costs are making enterprises less safe year after year. SOCS are under increasing pressure and the ongoing talent shortage of security professionals doesn't help. Things are complicated, and you probably don't feel they are getting any easier.

It's time to simplify security.



of enterprises deploy more than 50 security products



of enterprises deploy more than 30 security products

Cyber Resilient Organization Study 2021 from IBM Security

<https://www.ibm.com/resources/guides/cyber-resilient-organization-study/from IBM Security>

Zero Trust Leads the Way

The simplified security model of the future must embrace zero trust. Why is that? NIST* tells us...

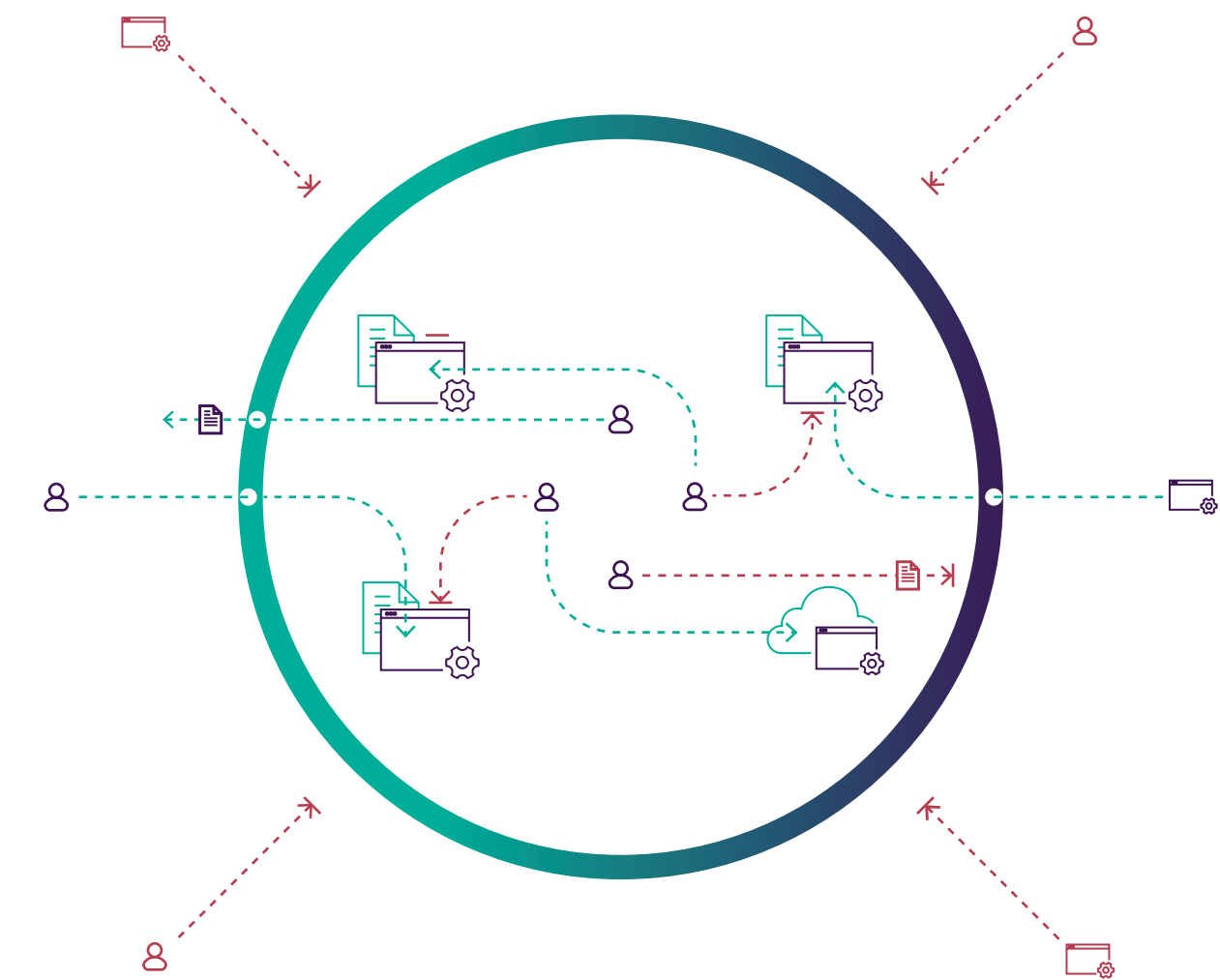
"Zero trust focuses on protecting resources (assets, services, workflows, network accounts, etc.), not network segments, as the network location is no longer seen as the prime component to the security posture of the resource."

The network perimeter as we know it, has vanished. The new edge is wherever your people and data are; who is accessing what and how are they doing it?

Now, security policies must focus on identities and explicit permission of a given identity to access a given resource at a given point in time.

Why should we treat the web, cloud, and internal apps as separate things that security teams must manage? The name of the game is to control access, without getting in the way of everyone's day jobs. Zero trust is also about making security transparent, not an Olympic obstacle course for users.

Trying to implement zero trust across your organization may seem too much of a burden, but it doesn't have to be.



> 100% believe the Zero Trust architecture is 'somewhat' to 'critically' important to reducing their enterprise's cyber risk.

> Only 59% have so far adopted Zero Trust as a foundational model across their enterprise.

ISMG ZERO TRUST STRATEGIES REPORT

*Zero Trust Architecture, NIST Special Publication 800-207 <https://csrc.nist.gov/publications/detail/sp/800-207/final>

Converged Security for Less Complexity

“Driven by the need to reduce complexity, leverage commonalities and minimize management overhead, security technology convergence is accelerating across multiple disciplines.”

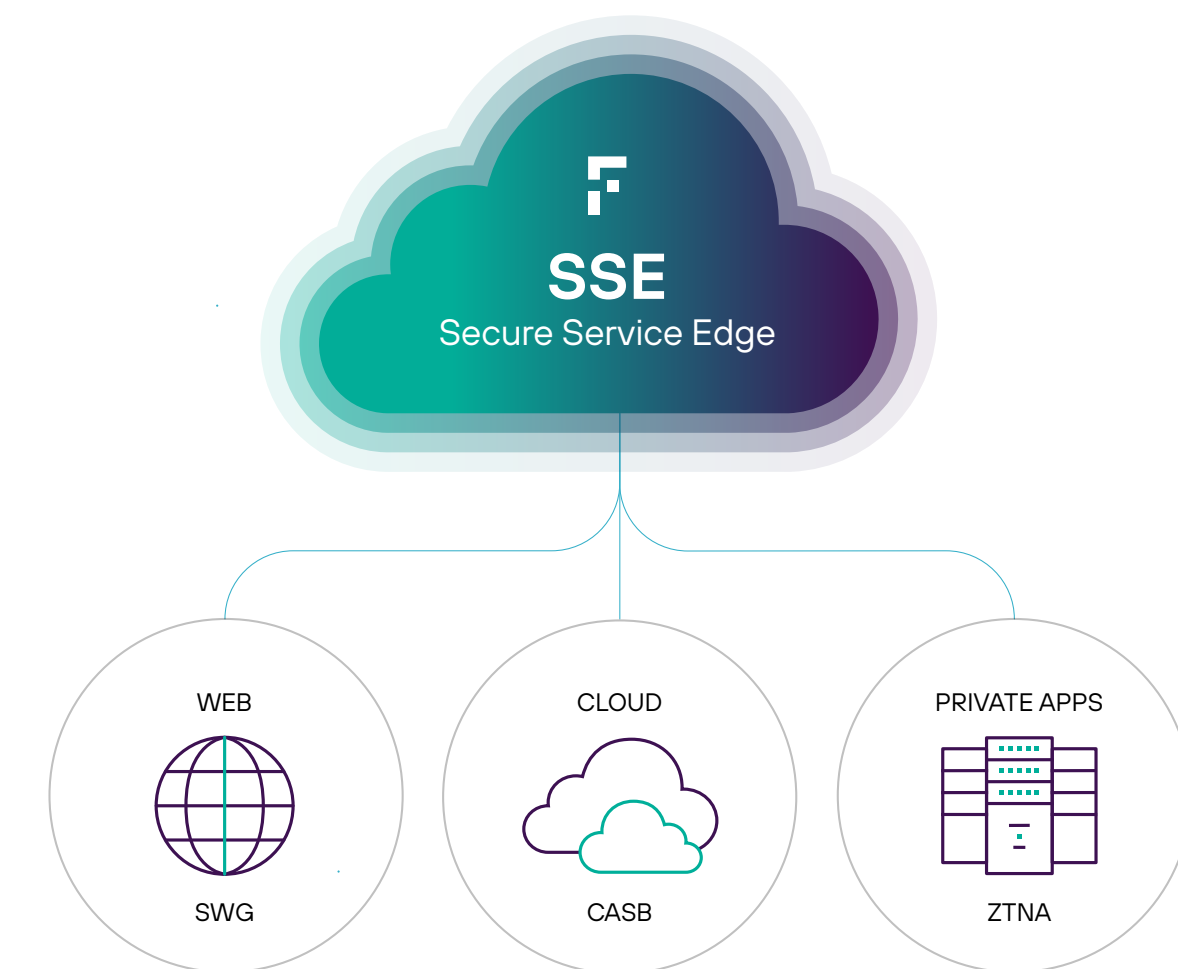
GARTNER®, PREDICTS 2022: CONSOLIDATED SECURITY PLATFORMS ARE THE FUTURE

Convergence is the key to executing a zero trust strategy. Think of SSE as a consolidation of technologies that includes Secure Web Gateway ([SWG](#)), Cloud Access Security Broker ([CASB](#)), and Zero Trust Network Access ([ZTNA](#)) as the cornerstone. Many security vendors have taken this too literally and pushed portfolios of disjointed, on-premises technologies up into the cloud and called it SSE. Those who did missed the point—resulting in the same patchwork of fragmented products that organizations have been wrestling with for years.

SSE relies on a unified platform that manages policies for using business resources in one place, from one console, with access and enforcement provided through one endpoint agent rather than many.

This all-in-one approach makes it safer for people to work anywhere—at home, in an office, or anywhere in between—because they can get to and use all the business resources they need through the internet, securely.

Gartner, Predicts 2022: Consolidated Security Platforms are the Future, Charlie Winckless, Joerg Fritsch, Peter Firstbrook, Nel MacDonald, Brian Lowans, 1 December 2021



“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.”

GARTNER®: MAGIC QUADRANT™ FOR SECURITY SERVICE EDGE

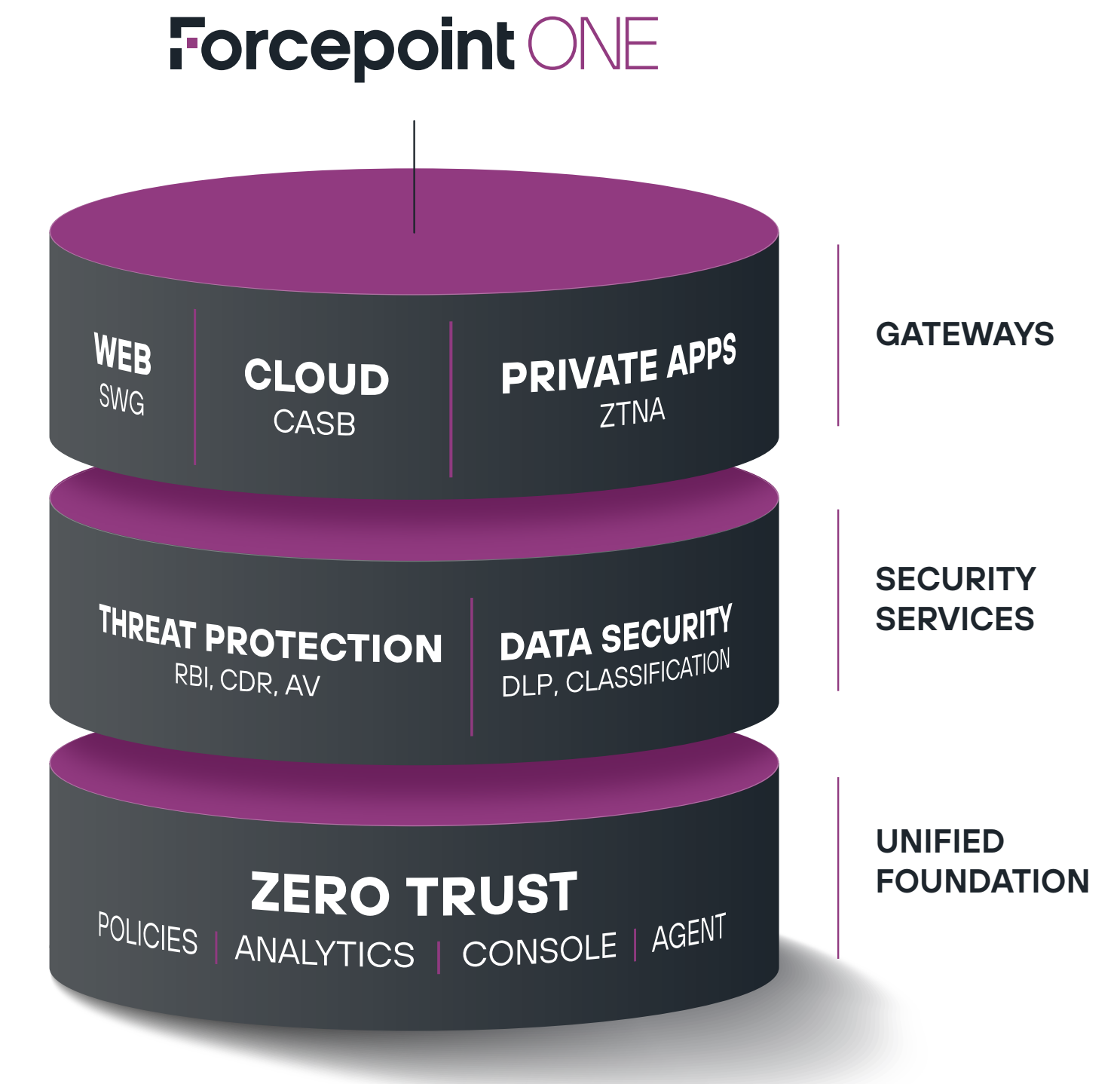
Gartner, Magic Quadrant for Security Service Edge, Lawrence Orans, John Watts, Craig Lawson, Charlie, Winckless, 24 January 2022, Updated 30 March 2022,

GARTNER and MAGIC QUADRANT are registered trademarks and service marks of Gartner, Inc. and/or its affiliates in the U.S. and internationally and are used herein with permission. All rights reserved.

Under the SSE Hood

Let's illustrate with the Forcepoint SSE solution, Forcepoint ONE. Forcepoint ONE unifies modular services in a cloud-delivered platform:

- **CASB** enables identity-based access controls for cloud apps so users on managed or unmanaged devices can easily and safely use cloud apps no matter how they need to connect. The unique reverse proxy technology makes it easy to connect for traditionally difficult use cases, such as personal devices, consultants, contractors, and auditors; and even provides for inline malware scanning and data loss prevention. This serves more types of users, with consistent control to prevent malware and stop sensitive data from walking out the door.
- **SWG** monitors and safeguards interactions with any website. This includes blocking access to websites based on category, blocking downloads of malware, blocking uploads of confidential or sensitive data to personal file sharing accounts, and detecting shadow IT. And, together with CASB, gives you control and visibility over shadow IT activity.
- **ZTNA** allows you to ditch the VPN for users. ZTNA gives you infinitely greater control with the confidence to allow people to use the devices that work best for them, even unmanaged devices and BYOD. Further, ZTNA & CASB together lets security teams deliver identity-based access controls for internal apps and cloud apps seamlessly using a Single Sign On (SSO) page to simplify the user experience.
- **DLP** consistently protects sensitive data across the cloud, the web, and private applications, even agentlessly, all from one console.

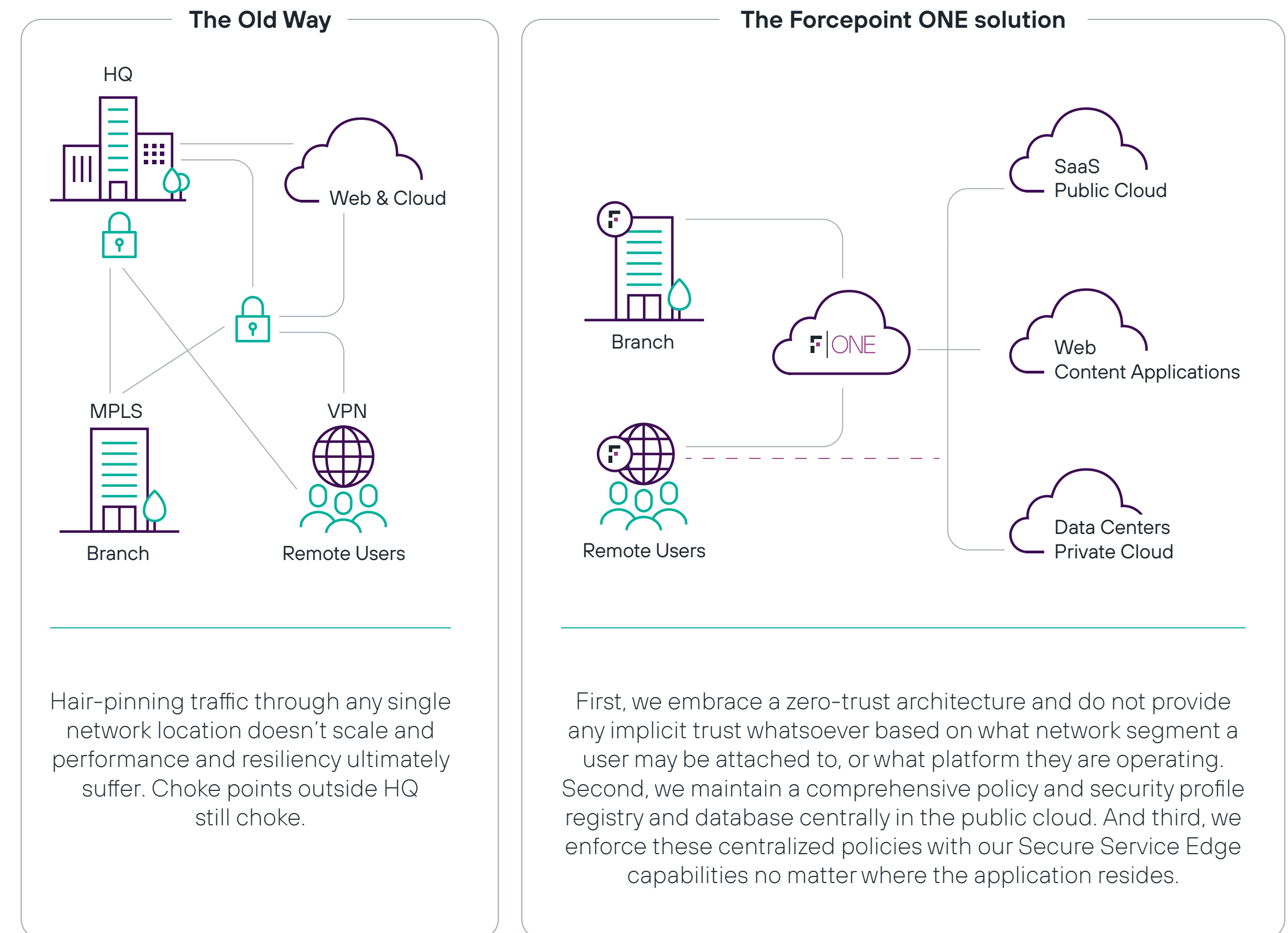


ONE Platform | ONE Console | ONE Agent

It's Time For a Better Approach to Connectivity

The innovation within the Forcepoint SSE platform integrates connectivity with identity and analytics, unifying modular security services in a distributed, high-performance environment.

Forcepoint ONE runs on a distributed AWS architecture with hundreds of on-ramps located around the world. That means no performance choke points. You can add security services whenever you need them. And you can control them all through one endpoint agent that feeds information to a central management console, which lets you configure one set of security policies for all the channels that your average remote or in-office employee uses nowadays, including web, cloud apps (SaaS), private apps.



Zapraszamy do kontaktu!
Więcej informacji: www.kreski.pl

How SSE Works: A Day in the Life of Kris

Security should allow people to be productive from anywhere, no matter how they need to work. We want to say “yes” as often as possible and only step in when either colleagues or the data they are interacting with presents risk. Controlling a single set of security policies from one place makes everything simpler.

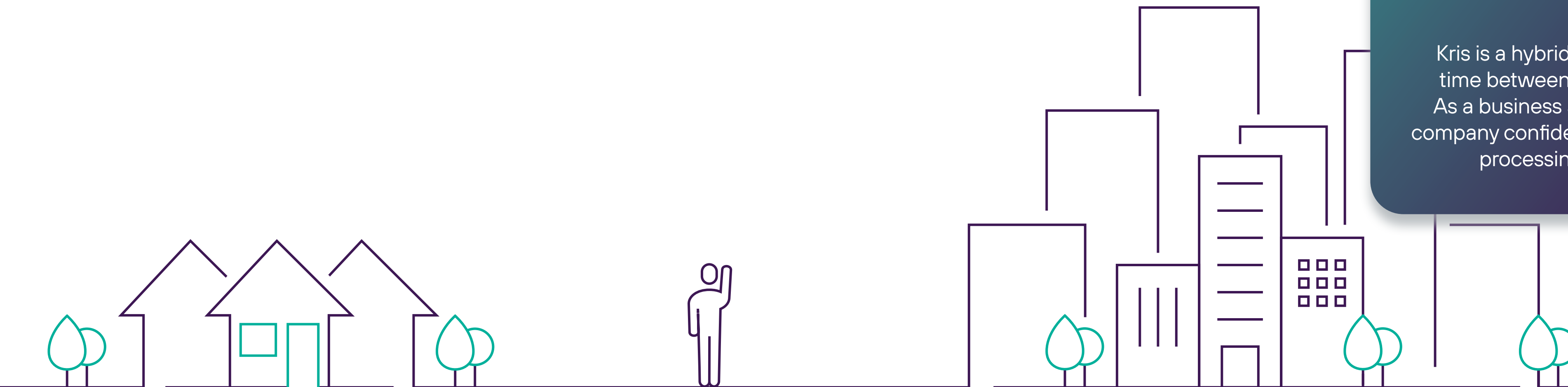
Let’s explore three scenarios of data risk as Kris, a business analyst, goes about their workday.

Employee Example



Kris Holdsworth
Business Analyst

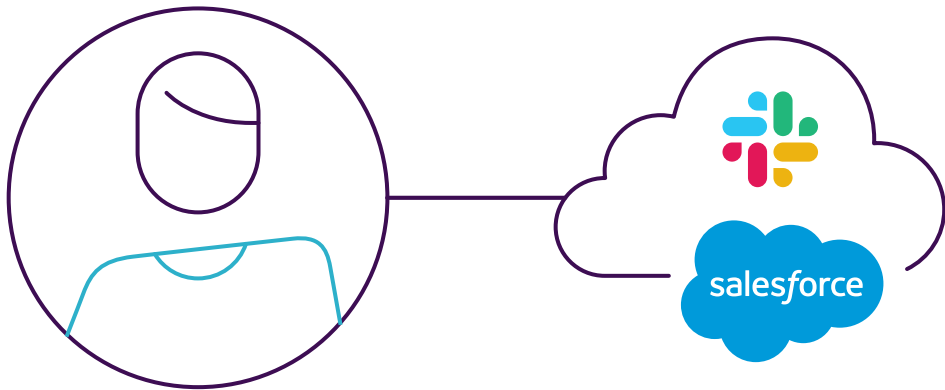
Kris is a hybrid worker who splits his time between home and the office. As a business analyst, he works with company confidential information as well processing customer data.








Accessing Cloud Apps

With a remote and hybrid workforce, it’s important your workers have access to the business apps they need to do their job, from wherever they are — and sometimes even from their personal devices.

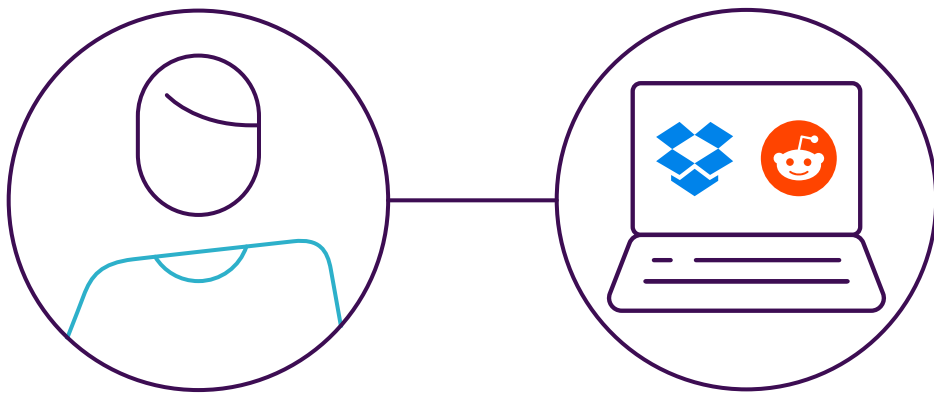
Kris is starting his day at home and wants to check something on Salesforce before heading into the office. Let’s follow Kris’ actions and observe how Forcepoint ONE responds behind the scenes...



	From home, Kris browses directly to salesforce.com or through a corporate application portal.	The session redirects through CASB, which analyses whether the device is managed, its location, and its security posture. Based on pre-defined security policies, CASB confirms Kris’ identity through multifactor authentication apps.
	Kris logs into their Salesforce account on their corporate-issued laptop.	CASB manages connections to business apps, allowing users to log on seamlessly and safely.
	Kris is granted managed app access.	The admin policies also control direct access to the app, controlled access, or no access at all. This happens in milliseconds without impacting employee productivity. All traffic from Kris’ device and the app passes through CASB.
	Kris decides to download a revenue forecast from Salesforce.	CASB scans any downloaded file for malware and sensitive data. As Kris’ company is balancing a large remote workforce and implementing zero trust they allow downloads of sensitive data only to managed devices, whereas unmanaged devices are still given access but cannot move sensitive data outside of company control. Since Kris is using a company managed laptop the download is allowed.
	Kris attempts to transfer a sensitive file contaminated with malware via their corporate Slack and upload the data to personal cloud storage.	CASB can check files being uploaded into cloud apps and can automatically block uploads containing malware. Together with SWG, CASB can also block uploading of files to unsanctioned apps using the SWG on-device unified agent.

Accessing Websites

Having safe web access is a necessity for today’s workforce, but it’s not as simple as dividing them into good and bad; Safe sites can become compromised, “recreational” sites may need to be accessed for work related purposes... and sometimes you need to visit the unknown or uncategorized.



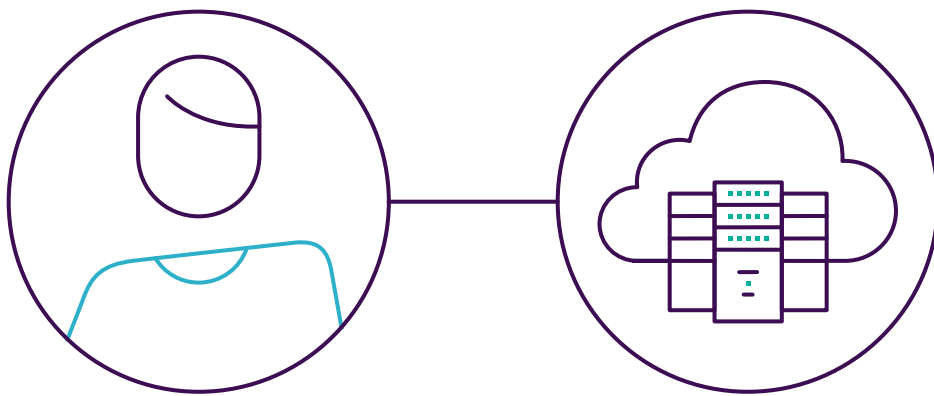
Kris has now arrived at the office and needs to browse a social website for work related research...

	<p>In the corporate office, Kris browses reddit.com for company-related research.</p>	<p>Kris visits reddit.com/r/technology to research recent posts on malware. The SWG content policies allow granularity to the directory level; this subreddit is considered work-related so Kris can access it.</p>
	<p>Within the r/technology subreddit, Kris accidentally clicks a link to an inappropriate subreddit page.</p>	<p>Kris’ Forcepoint ONE administrator has created SWG content policies that allow access to acceptable subreddit pages, but block access to inappropriate subreddits and other inappropriate pages. SWG prevents Kris’ error and blocks the new subreddit page.</p>
	<p>Kris starts a confidential spreadsheet on their company laptop that includes customer PII and wants to continue working on their personal laptop at home. From home, they try to upload the file to personal cloud storage and download it to their personal laptop.</p>	<p>To prevent business data loss, the company’s Forcepoint ONE administrator created a SWG content policy that blocks upload of sensitive customer information (PII) to any personal file sharing website. When Kris attempts the upload, it is blocked, and a message pops up to explain why the upload was blocked.</p>

Accessing Private Apps

Private Apps are typically the most critical of business applications and often handle the most sensitive data. This presents IT with the dual headache of keeping a firm grasp of who has access to data, and what they are doing with it, whilst not impeding people from doing their job.

Kris is now on vacation, but a work issue has come up that requires an immediate response...



	<p>From their personal device, Kris browses to the corporate single sign-on portal(SSO) and clicks on an internal application.</p>	<p>Access to any application managed by Forcepoint ONE — cloud or private — requires proper authentication. This controlled access for unmanaged devices is useful for many atypical users, such as contract workers, consultants, and auditors.</p>
	<p>Kris gets one-click access to the company's internal applications, such as SAP and Sharepoint, from the same SSO page that they use for access to all business applications.</p>	<p>Kris' browser displays the SSO page, showing tiles for each web app Kris and their partners can access. (If Kris' company uses CASB, Kris' managed SaaS apps are accessible from the same user portal for a consistent experience.)</p>
	<p>Kris is granted managed app access.</p>	<p>The admin policies also control direct access to the app, controlled access, or no access at all. This happens in milliseconds without impacting productivity. All traffic from Kris' device and the app passes through ZTNA.</p>
	<p>Kris uploads a vendor contract as an attachment.</p>	<p>Just like for CASB and SWG, the ZTNA service scans all uploads and downloads for sensitive data and malware. If the file is malware-free the upload is allowed. If it is infected, the ZTNA gateway blocks the upload, alerts Kris, and logs and reports the blocked event.</p>

Forcepoint ONE: Converged Security that Fits your Needs

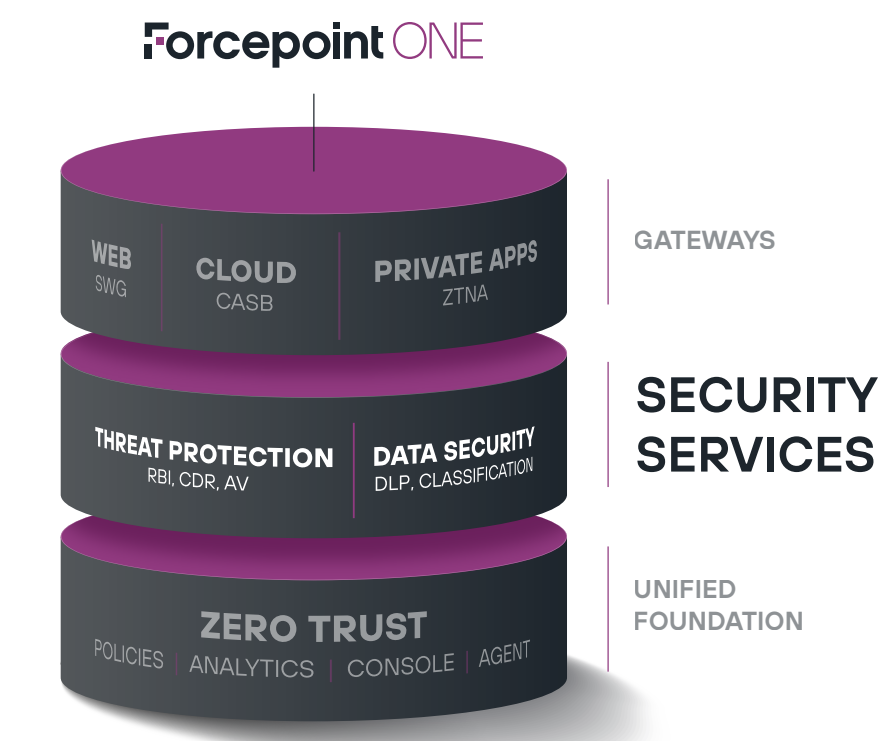
The simplicity and flexibility of the Forcepoint ONE cloud-native SSE platform allows you to start quickly and configure the security services you need. Choose Cloud Edition for all-in-one SSE that lets you control access to cloud apps, websites, and private apps for both managed and unmanaged devices. Or, pick the services you need and add more as you go.

1. **Cloud Edition** is the full Forcepoint ONE platform, with CASB, SWG, and ZTNA driving synergy for security teams. There is one console to create and manage a single set of security policies, and one agent to enforce them. All security services fit together seamlessly.
2. **CASB Edition** represents the evolution of the multiple-award winning cloud app security solution from Forcepoint, with built-in best-in-class data loss prevention and advanced threat protection for unmanaged devices.
3. **Web Edition** makes browsing even risky or un reputable websites simple to control and prevents upload or download of malware or confidential data.
4. **ZTNA Edition** lets organizations ditch VPNs to connect remote workers with private web and non-web apps. Set up controls for zero trust access, stop data loss, and implement malware scanning in minutes.

Enhancing the Security Services

Forcepoint ONE provides a clear and simple path to the security model of the future.

- **Add Forcepoint Remote Browser Isolation (RBI)** for a zero trust approach to web browsing with Content Disarm and Reconstruction (CDR) to provide automatic file sanitization of files.
- **Add CrowdStrike Machine Learning malware protection**
- **Add Forcepoint Classification powered by Getvisibility** that incorporates true artificial intelligence (AI) and machine learning (ML) to automatically categorize both structured and unstructured data.



Drive Immediate Value from SSE

It may typically take months or even years for your vision of security to fall into place. This isn't the case with SSE. Going cloud-native gets you off the starting blocks fast and makes it much easier to adopt zero trust so you can:

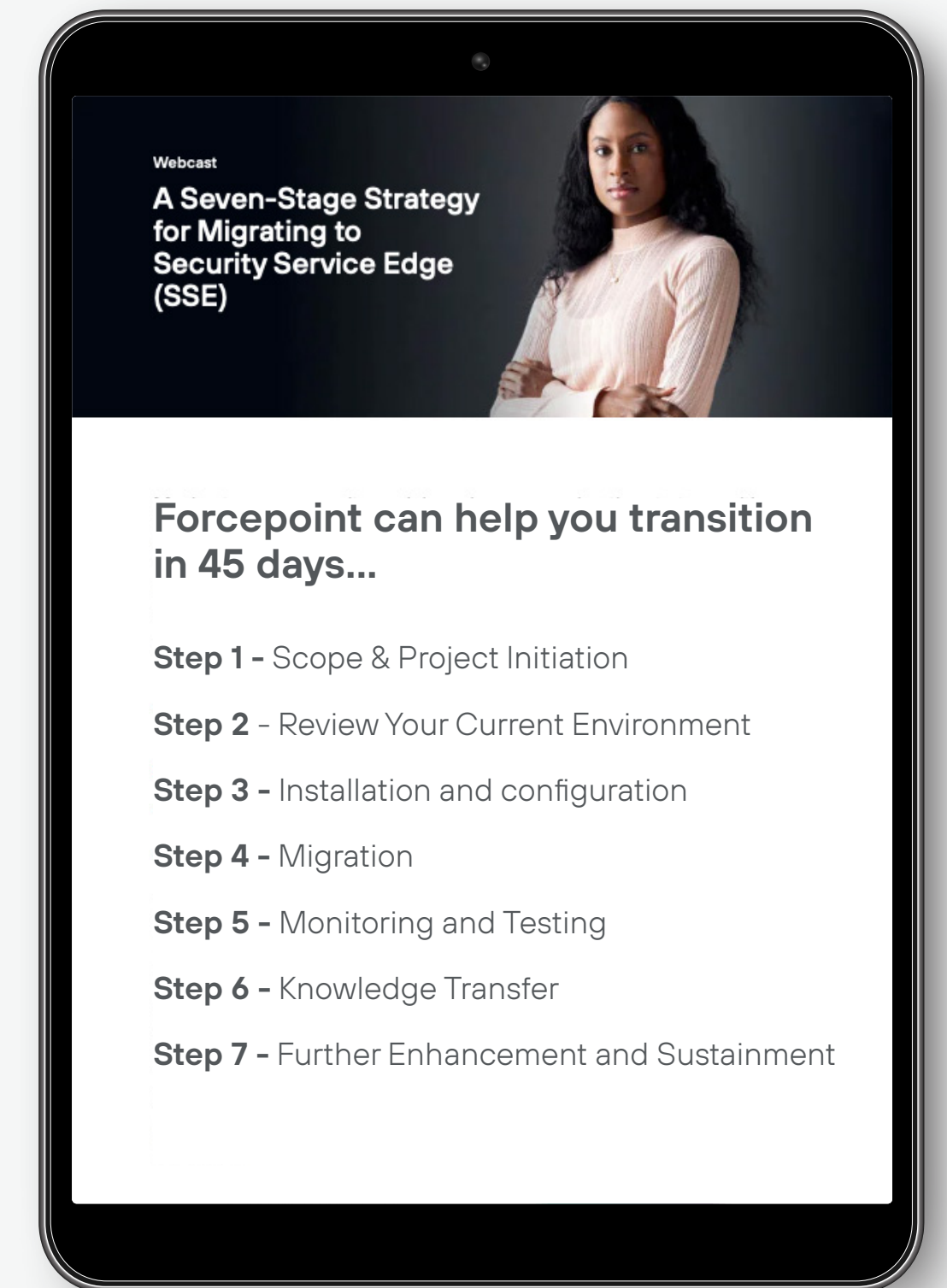
- 1. Increase productivity:** Truly enable teams to work from anywhere and embrace emerging cloud and IoT technologies, hassle-free.
- 2. Reduce risk:** Adopt zero trust and reducing complexity many traditional threats disappear. Native DLP capabilities help prevent accidental and malicious insider data losses.
- 3. Reduce cost:** Consolidate disparate solutions and reduce other expensive technologies (VPN, NDR, IPDS, etc.). Also, simplify management via a single console with reduced false positives and alerts to give IT more time to focus on more strategic priorities.
- 4. Streamline compliance:** Meet the demands of the board of directors and auditors requiring verifiable compliance with emerging regulations; Forcepoint ONE delivers enforcement managed from a centralized portal and provides detailed forensics.

For typical implementations, you could achieve time to value in 45 to 90 days. With simpler deployments, you could see ROI in as little as 21 days.

IT Leader Viewpoint:

"We were able to get Forcepoint ONE up and running seamlessly, very quickly, and with no disruption to our users."

DAVID LEVINE
CISO, RICOH USA



For more information, see our Seven-Stage Strategy webinar for Migrating to Security Service Edge

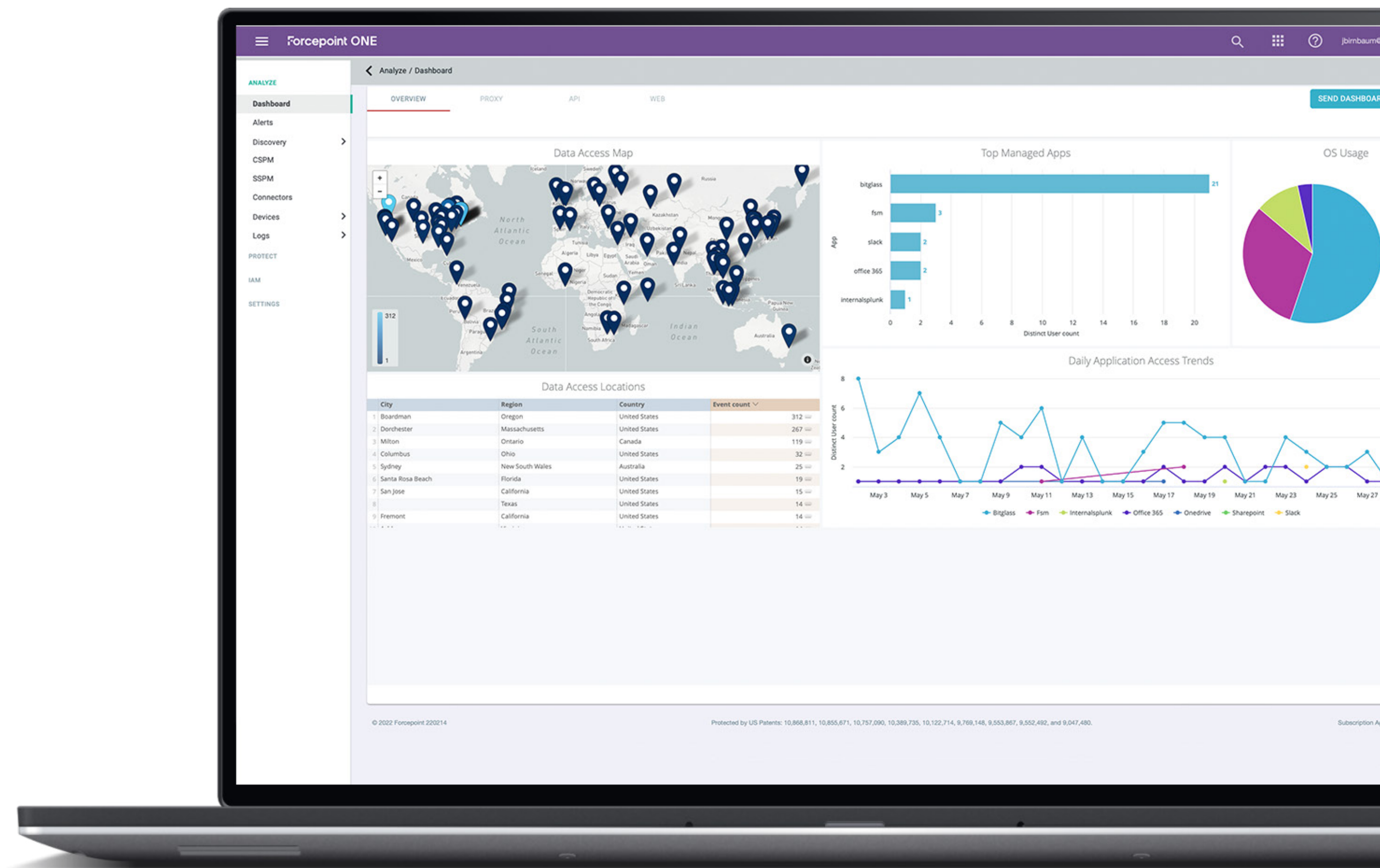
Making Security Simple

It's time for IT to become the hero again – get control of the chaos, maintain control of data and enable your people to keep doing the work that drives the business forward.

In the end, moving to a unified cloud platform improves compatibility, reduces disconnects, closes gaps, and improves efficacy by bringing services to the edge, where people are working today. You can dramatically improve the efficiency of security with fewer disparate products and vendors to manage.

For security pros on the front line, a single console with unified policies makes management a game-changer. With efficacy comes accuracy, allowing teams to cut through alert noise and minimize investigation time. Security leaders can get a handle on data risk and simultaneously say “yes” to the board more often. But most importantly, it makes the lives of people easier by safely allowing them to do more, the way they want to work. That's simplifying security.

Visit www.forcepoint.com/ONE for more information on Forcepoint's SSE solution.





Forcepoint

forcepoint.com/contact

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](#).

© 2022 Forcepoint. Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint. All other trademarks used in this document are the property of their respective owners. [FP-The Painless Guide to SSE-Ebook] 06Sept2022