Forcepoint ONE

A Unique, Data-First SASE Platform

Forcepoint

Whitepaper

Table of Contents

Disruption creates opportunities to accelerate transformation

For years, "digital transformation" has been all the rage. Before 2020, applications were slowly moving out of corporate data centers into the cloud. A small percentage of people were occasionally working remotely, often using mobile devices like phones and tablets to augment corporate laptops. Then the pandemic hit, and everything changed.

Overnight, most employees started working from home. With productivity at stake, many organizations adapted by accelerating their migration to cloud-based apps, which users could get to much more easily than wrestling with VPNs to connect to traditional data center applications. While this made access easier, it also reduced the visibility and control that IT organizations had over sensitive data.

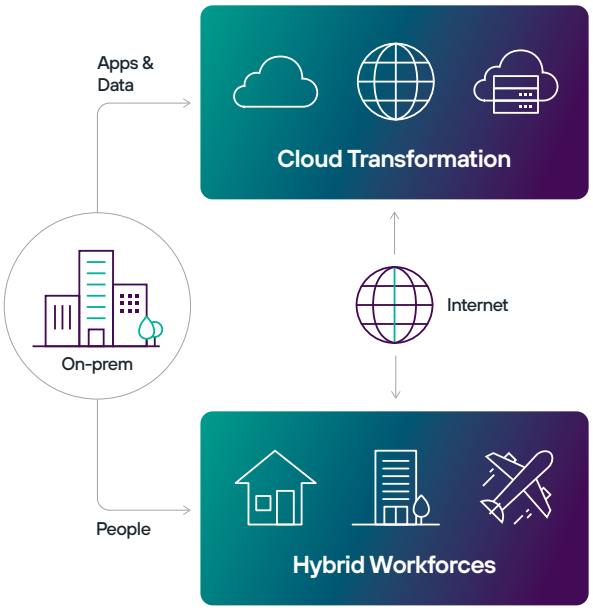
Unfortunately, data thieves quickly adapted as well, attacking cloud apps from all over the globe. As people juggled their personal and professional lives in the physical and digital worlds, "bad guys" took advantage of the huge number of people who weren't accustomed to working in a hostile digital world. Simple actions, such as using a smartphone to access work data or browsing websites from a work laptop to make purchases, created opportunities for phishing, drive-by downloads and other forms of compromise.

Working anywhere is changing everything. Again.

As the pandemic eased, people began to go back into offices, but not like they did in 2019. Even now, few organizations have returned to old work patterns. While many businesses and government agencies are trying to encourage people to spend time in the office, it's no longer the default place that work is done. Many people now see the office as a place they visit, in the same way they used to view taking trips to remote sites, partners or customers.

In addition, many employees have become dependent upon phones and tablets (BYOD) for keeping connected when not sitting at a desk. What used to be a convenience for a select few is now the standard way that people stay productive in an increasingly competitive world.

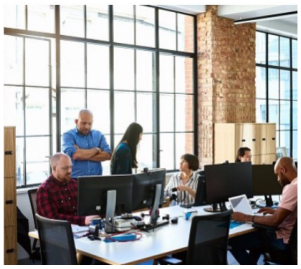
Employees now expect – and are expected – to be able to work **anywhere** with business data located **everywhere**.



Challenge:
Adapting to protect your business

Changing where and how people work is tough enough in the best of times. But recent uncertainties spurred many businesses to focus first on making sure they were prepared to weather any economic storms. Enabling people to use resources in innovative ways – such as safely using generative AIs like ChatGPT and consuming data from BYOD without putting that data at risk – is crucial to driving an organization's financial top line. In addition, with budgets staying tight, finding new efficiencies in both capital and operating expenses is key to protecting the bottom line. Of course, all of this must be done securely, so that sensitive data can be used wherever it is needed without creating more risk or introducing issues with auditors.

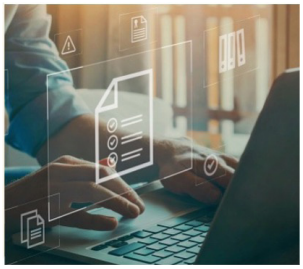
That's where Forcepoint comes in. We believe that the right approach and the right technology can turn these rapid shifts in how people work and how information is managed into an opportunity rather than a burden. That's why we created Forcepoint ONE, our platform for simplifying how you connect and protect your people and data in a modern, cloud-first world. It's all about helping you make them more productive and your business more efficient, safely.



Increase Productivity

Cut Costs

Reduce Risk

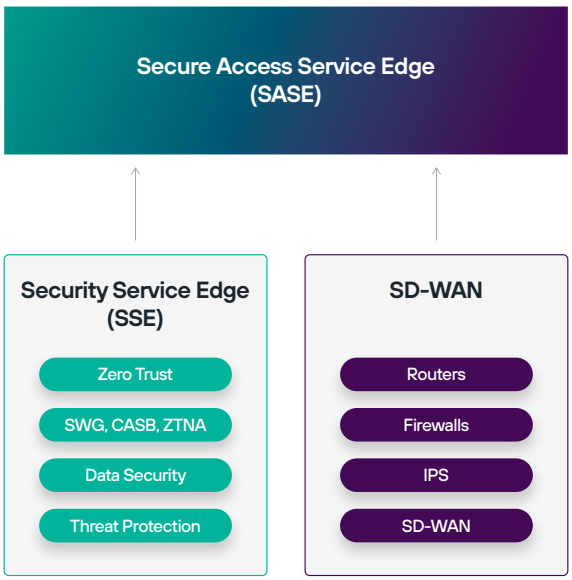


Streamline Compliance

Solution:
Secure Access Service Edge (SASE)

In 2019, Gartner proposed a new IT architecture, Secure Access Service Edge (SASE), bringing security and networking together, managed and often delivered as services from the cloud.

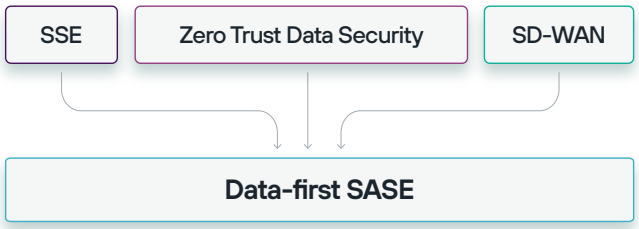
Connectivity products such as firewalls, routers, intrusion prevention systems and application-centric networking have already begun to converge into a new generation of unified SD-WAN solutions. Similarly, SASE architectures make it easier for security gateways to apply policies for Zero Trust-based threat protection and data security consistently across web (SWG), cloud (CASB) and private application (ZTNA) access. Gartner subsequently started referring to this unified approach to security as Security Service Edge (SSE).



Forcepoint ONE: A Data-first SASE platform

Forcepoint was one of the first proponents of the SASE architecture. It represents many of the principles and technologies we helped pioneer for connecting and protecting distributed businesses and government agencies. When the pandemic forced all organizations to become highly distributed, SASE became the right way at the right time to deliver the productivity and efficiency our customers were asking for.

However, we believe that SASE is the starting point for a modern cloud-based architecture, not the finish line. Forcepoint goes beyond just securing access to business resources – we safeguard the ongoing usage of sensitive data everywhere, from the endpoint through the cloud. We call this approach Data-first SASE.



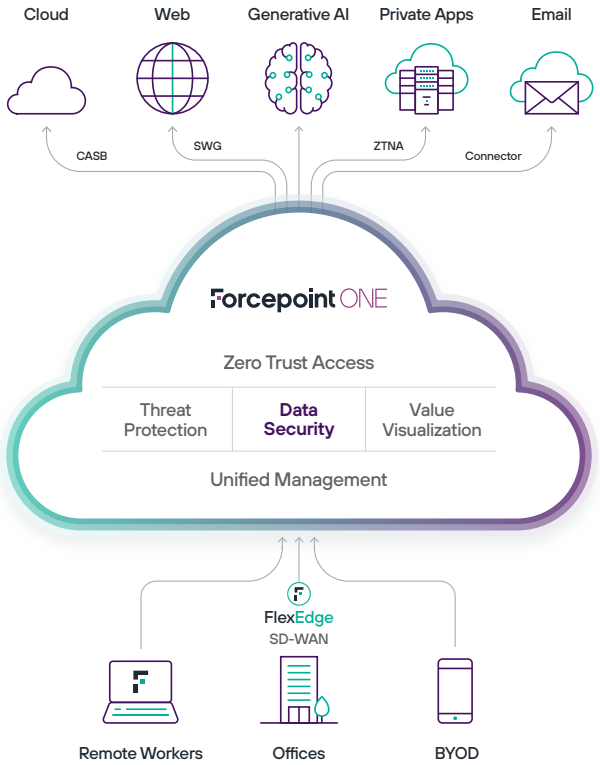
Our Data-first SASE platform, Forcepoint ONE, unites a wide range of technologies in the cloud to make security simple for distributed businesses and government agencies. It gives employees, contractors and other users safe, controlled access to business information in the cloud, on the web and in private applications while keeping attackers out and sensitive data in. As a result, users can be more productive, whether at home or in the office, while businesses are more efficient.

Popular uses of Forcepoint ONE

With Forcepoint ONE, organizations can address current challenges easily and incrementally. This enables IT teams to solve immediate problems quickly and add capabilities as needed in the future. In shorter terms, it's "Security Simplified."

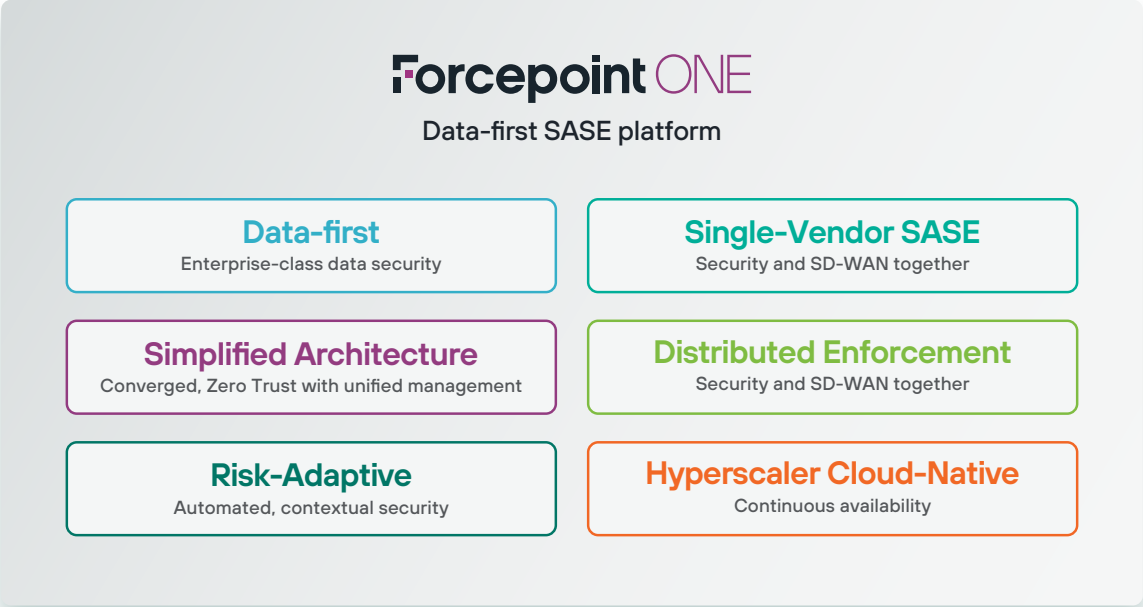
Forcepoint ONE is being used around the world to:

- → **Prevent data loss from cloud apps** (esp. Microsoft 365 and Google Workspace) and on the web.
- → **Safeguard Bring Your Own Device (BYOD)** agentless access to cloud and private apps.
- → **Implement Zero Trust access** to cloud, web and private apps is secured for remote and office users.
- → **Control Shadow IT, including ChatGPT** and other generative AIs, enabling use without the risk of sensitive data being exfiltrated.
- → **Simplify mergers & acquisitions.**
- → **Replace VPNs** for accessing internal apps.
- → **Accelerate cloud app performance** at branch offices.
- → **Enable any website or downloaded document** to be used safely even if contaminated.
- → **Detect misconfigurations** and violations of compliance frameworks.



Six ways that Forcepoint ONE SASE is different

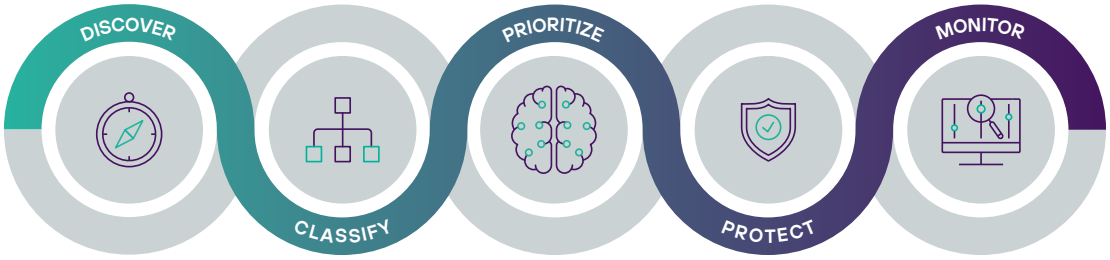
Forcepoint ONE brings together six key elements to deliver the security and networking that organizations need to be successful in today's rapidly changing world:



Data-first: Enterprise-class data security everywhere

Forcepoint has a different point of view from most vendors. We believe that modern cybersecurity is fundamentally about enabling sensitive data everywhere to be used safely anywhere. That's why we build some of the strongest data security technology in the industry into the core of our Forcepoint ONE platform and our SSE gateways – CASB (forward proxy, reverse proxy and API-based), SWG (cloud- and endpoint-based) and ZTNA (agent-based and agentless).

Forcepoint's Data Loss Prevention (DLP) technology is depended upon by thousands of organizations around the world and has been called a "leader" by major industry analysts. It's part of a Zero Trust-based framework called the Data Security Lifecycle that implements best practices for protecting data efficiently and effectively from unauthorized access, theft or accidental loss.



Data Security Lifecycle

We automate each step in this lifecycle. With our solutions, customers can rapidly identify where sensitive data resides, classify structured and unstructured data (in the cloud and on-premises), determine where to focus their efforts, stop data loss across all key channels of exfiltration (endpoint, email, web, network and cloud applications) and continuously monitor what users are doing with sensitive data.

This approach goes far beyond the basic pattern matching that often passes for data security in other SASE solutions. By classifying data and organizing it into different groups, data security policies can be written and enforced that automatically handle new instances and types of sensitive data. To make policy definition simple, especially for complying with region- or industry-specific mandates, we incorporate one of the industry's most comprehensive libraries of policy templates. In addition, our Forcepoint ONE SSE gateways for controlling access to web (SWG), cloud (CASB) and private applications (ZTNA) enable DLP policies to be specified in one place and applied consistently across different channels.

This simplicity isn't limited to a set of pre-defined applications. Forcepoint ONE can apply granular data security controls to any web-based app using the same Field Programmable SASE Logic (FPSL) scripting mechanism that Forcepoint itself uses in its own policies. Administrators can easily build rules that triggers off attributes in an HTTP request (domain, method, URI, query string or cookie) to detect user interactions, log the pages being used and optionally block them. For example, Forcepoint ONE can easily:

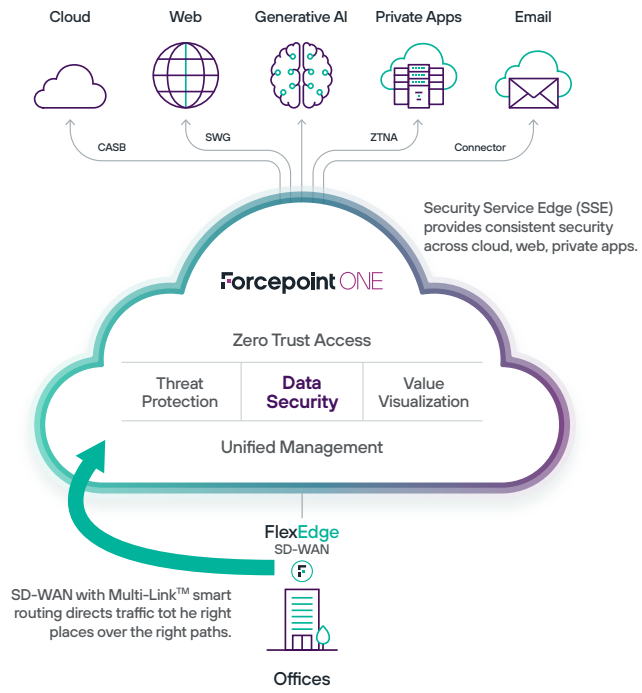
- → Block logins to corporate SaaS applications using a personal email address.
- → Log every file uploaded to personal Google Drive accounts for users in a risky-users group.
- → Block likes in Facebook.
- → Only let members of the marketing group post to LinkedIn.
- → Block sensitive content in a Twitter post.

And, since people in today's workforce often depend upon phones, tablets and endpoints such as Linux workstations or Chromebooks, **Forcepoint ONE makes it possible to safely use cloud and internal private web apps from BYOD and other agentless devices to keep people productive without putting data at risk.**

Single-vendor: Security and SD-WAN in one

Forcepoint is a pioneer in integrating security and networking technologies into a single product, managed from a single console. Forcepoint Secure SD-WAN solutions were among the first to combine SD-WAN routing with high-security firewall and intrusion prevention technologies.

Our patented multi-link, multi-ISP aggregation is used around the world to transform legacy wide area networks built on private circuits such as MPLS into modern, broadband-based SD-WAN. Designed specifically for massive scalability, Forcepoint Secure SD-WAN enables policies for as many as 6,000 sites to be managed from a single console.



With Secure SD-WAN, distributed organizations connect their remote sites and branch offices directly to the internet to provide the highest performance for accessing modern cloud applications. **Advanced capabilities such as application steering, application health monitoring and zero-touch updating enable IT organizations to proactively deliver consistent performance and uptime to keep people productive and infrastructure costs low**.

As a result, our SD-WAN provides a foundation for implementing a converged SASE architecture. Organizations can automatically route traffic for various applications to our Forcepoint ONE Security Service Edge (SSE) gateways running in the cloud. This not only makes it easy to safeguard employees and business data, it enables security policies to also be defined and enforced for unmanaged devices such as guest laptops on Wi-Fi, BYOD phones and tablets, even printers and Internet of Things (IoT) devices.

Simplified Architecture: converged, unified management

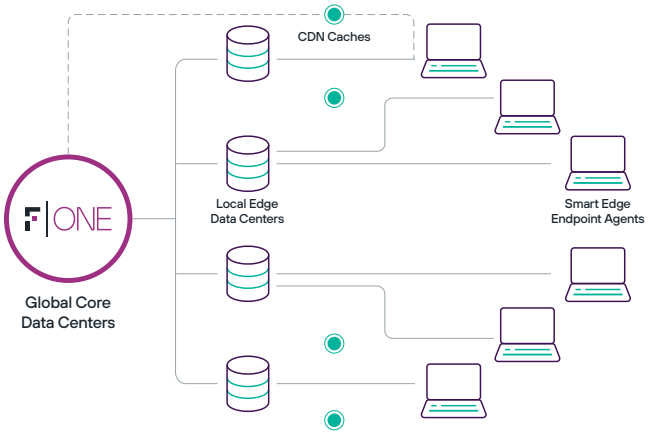
Forcepoint's mission is "Security Simplified." The days of people taking pride in the complexity of security infrastructure are over. With environments constantly changing, IT teams are often stretched to the limit and forced to do more with less. **Reducing complexity is no longer just a good idea – it's the only way to keep businesses productive, cut costs and prevent risk from spiraling out of control**.

To help customers simplify their own enterprise architecture, Forcepoint ONE itself is designed to avoid gaps and redundancies in technologies that used to be fragmented. Gateways for securing access to cloud apps, the web and internal private applications share code and use a common set of underlying security microservices for keeping threats out, sensitive data in and helping business leaders better understand the value of the connectivity and security they are delivering to the organization.

Key elements of the Forcepoint ONE platform include:

- → Zero Trust-based access gateways that control how employees and others use cloud (CASB), web (SWG), and private applications (ZTNA).
- → Advanced threat protection services such as remote browser isolation, automated document sanitizing (known as content disarm and reconstruction), antivirus and malware sandboxing.
- → Leading-edge data security services that prevent theft of sensitive data consistently over each channel (DLP).
- → Secure agentless access from BYOD and unmanaged devices to cloud (CASB) and private web (ZTNA) apps.

- → Interactive dashboards that visually present the key performance indicators and economic value of the services Forcepoint ONE is delivering.
- → A single console for setting policies for controlling how business resources are accessed and used.
- → Patented SAML identity provider integration for working with or supplementing existing IdP systems.



Forcepoint ONE uses a multi-tier architecture. Global core data centers perform the primary functions of the platform such as inspecting data-at-rest in SaaS and IaaS, checking SaaS and IaaS for security misconfigurations and analyzing data from endpoint devices.

Local edge data centers deliver policies and act as Content Delivery Network (CDN) caches for frequently requested information such as threat intelligence categorization. These edge data centers automatically scale up to handle transient loads such as when people converge at a conference.

Additional capabilities that complement the access services delivered from the cloud are provided by endpoint software, called SmartEdge, that runs on managed laptops and other devices. SmartEdge automatically connects remote workers to the right security services and ensures that the right policies are enforced. Forcepoint is currently integrating this technology with telemetry from our other endpoint and network controls to enable IT organizations to deploy and manage a single endpoint application providing the full range of Forcepoint ONE connectivity and security.

Based on Zero Trust principles

Policies for Forcepoint ONE access services are built around a Zero Trust approach of specifying the identity, application, devices and location for which each given action should be applied:

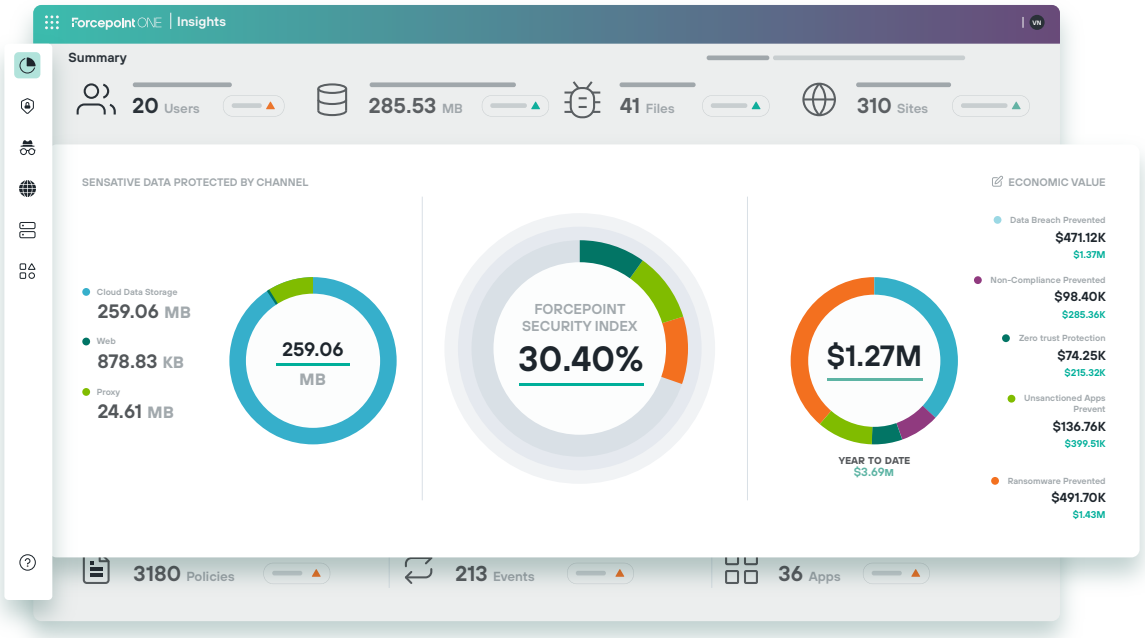
Proxy

ID	Groups	Access Method	Device	Location	Action
7073	Admins	Any	Any	Anonymizers IaaS Provider IPs	Deny
69739	Any	SSO Auth	Managed Win - AV On	Corp Network and VPN	Direct App Access
28475	Any	SSO Auth	Any	Any	Secure App Access DLP Download DLP Upload
188394	Any	Any	Any	NRD-HQ	Secure App Access DLP Download DLP Upload

Data security and threat prevention policies can be specified for all uploads and downloads and then be combined with user notification and coaching to ensure users and data are protected.

Connecting the dots on the economic value of SASE

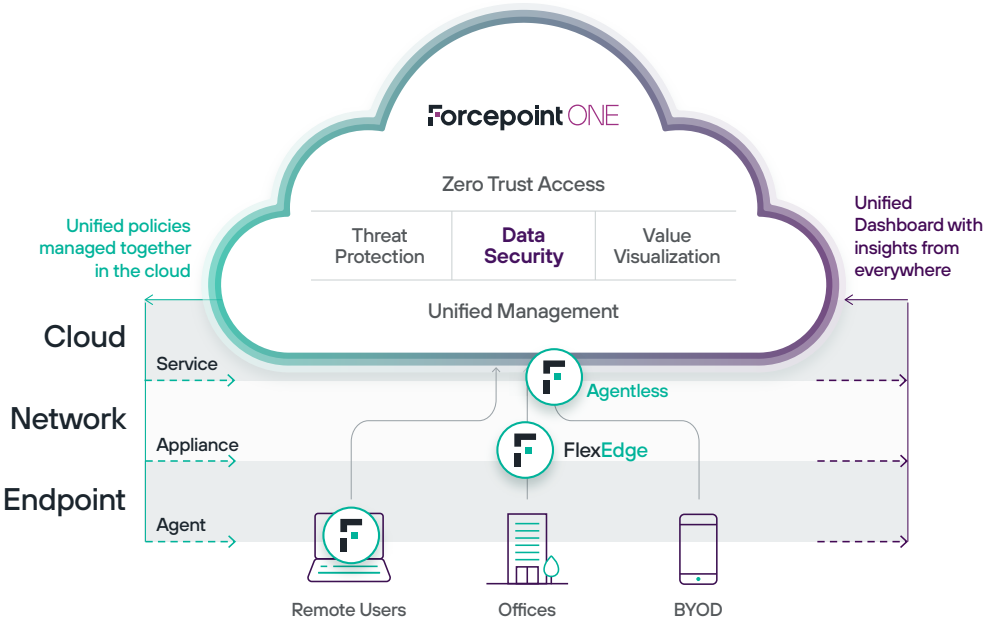
Forcepoint ONE gives administrators full visibility and unified reporting across all their managed and unmanaged devices. Our Insights dashboards provide a consolidated view of what is happening across different security services that illuminates the business value that Forcepoint is delivering.



Multi-tier, Distributed Enforcement across cloud, network edge and endpoint

The cloud has revolutionized how security is managed and delivered, while the internet has supplanted the corporate network as the backbone of IT operations. Together, they enable a consolidated control plane to be easily accessed from anywhere. But the cloud is the beginning, not the end, of a modern approach to security.

While all SASE solutions provide cloud-based enforcement of policies, we go further. **Forcepoint ONE puts enforcement of networking and security policies wherever they are needed: close to the user on the endpoint, close to infrastructure in the network, as well as close to applications in the cloud**.



This distributed approach optimizes the performance of applications, reduces the use of network bandwidth and eliminates problems that can arise when traffic is redirected through chokepoints – whether in old, private data centers or new, multi-tenant cloud services. Forcepoint ONE ensures that the same policies are enforced everywhere, and the same dashboards can be used to monitor the operation of those policies.

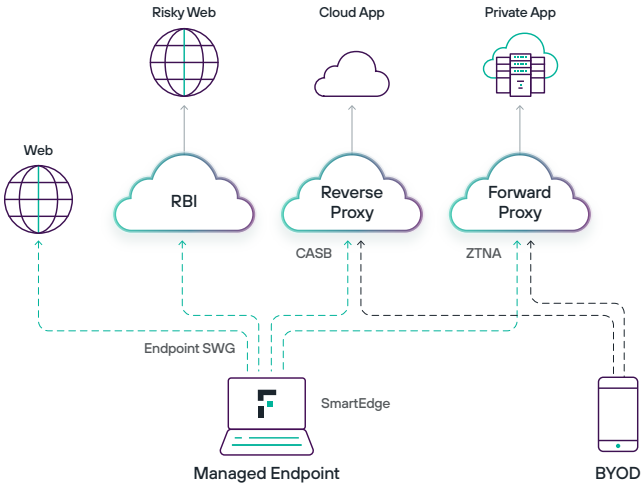
Endpoint-based cloud "onramp" optimizes application performance and user experience

For example, traditional SWG architectures that force all web traffic through a cloud proxy, while simple to deploy, often present challenges in the real world:

- → **Latency –** The extra network hops and processing that is introduced reduce browsing speeds by as much as half. Some cloud applications (including some of the most popular office collaboration suites) are sensitive to these delays and can fail to operate properly.
- → **Bandwidth utilization –** Organizations that equip sites with multiple internet links may be unable to take full advantage of them to optimize cloud application performance and cost (e.g., sending high-priority video conferencing over faster links while lower-priority traffic goes over less-expensive ones).
- → **Location awareness –** Cloud applications that use the internet address of the endpoint to select specific content or functions (such as which language to present a page in) may not function correctly, leading to user confusion and helpdesk burdens.
- → **Compliance –** In some situations, sending sensitive data off a controlled endpoint device and onto the internet (even if it is going straight to the proxy) can trigger breach procedures.

Microsoft specifically recommends that Microsoft 365 users avoid using proxies, forcing organizations to choose between productivity and security. Forcepoint ONE addresses these issues by enabling web security policies (including those for data loss prevention) to be enforced on endpoints running our SmartEdge software.

SmartEdge provides a "cloud onramp" that automatically routes traffic to the appropriate service or application based on what is being accessed. It complements the cloud proxies that Forcepoint ONE offers for securing agentless devices such as BYOD and IoT.



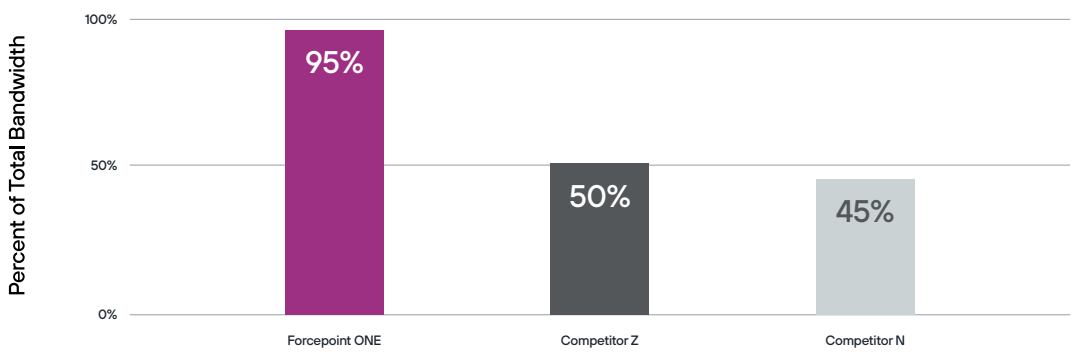
SmartEdge endpoint software steers traffic to right places

SmartEdge is particularly valuable for remote users since it provides the most natural, productive and secure user experience. It works with our cloud platform to ensure policies are properly enforced in all situations, including:

- → **New URL access –** When a user tries to access a URL for the first time, the SmartEdge SWG queries the closest Forcepoint ONE CDN cache to retrieve the appropriate web browsing policy for that combination of user group, device type, URL category, location and URL reputation. If the result of the query is not in the cache node, the request is forwarded to the closest Forcepoint ONE local edge data center. Assuming the website is not blocked, all web traffic is exchanged directly between the device and the website, thus avoiding hairpinning.
- → **SWG risky website protection and isolation –** Risky websites can be specified in Forcepoint ONE based on their URL Site Categorization or URL Reputation Scores. When a user attempts to access a risky website, the SWG isolates the access and redirects it through Forcepoint Remote Browser Isolation (RBI). RBI reduces the attack surface of the endpoint by hiding the IP address and remotely rendering the website in a temporary container that is specific to the user's session.
- → **File movement to/from a secured, unsanctioned web application –** When a user attempts to upload a file to or download a file from an unsanctioned web application with a web browsing policy that enforces secure access, Forcepoint ONE will block attempts to upload or download files based on policy rules for DLP or malware protection in the web browsing policy.

The distributed enforcement approach in Forcepoint ONE delivers up to twice the browsing performance of cloud-only systems with full protection against web-borne threats or inappropriate uploading of sensitive data.

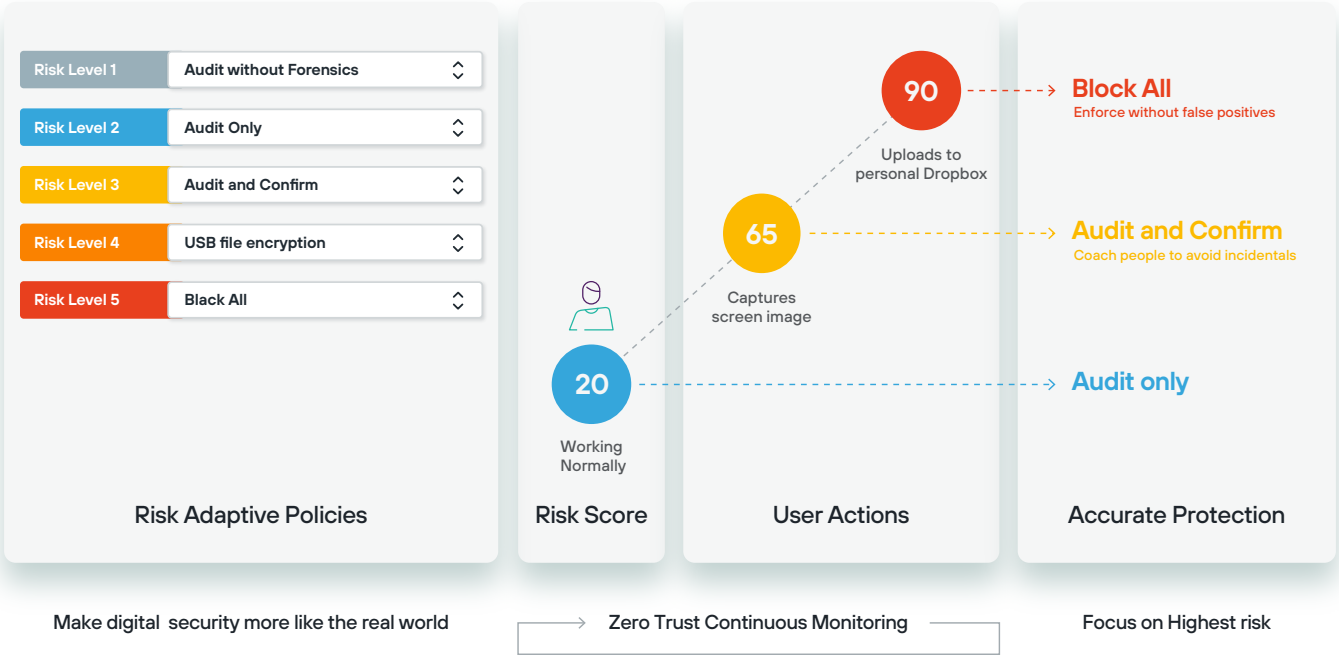
SWG Throughput as a Percent of Total Bandwidth



Risk-adaptive protection for contextual security

Now that people are working anywhere with data that resides everywhere, defining individual policies for every relevant combination of users, devices, locations, applications and other attributes is error-prone and unscalable. Worse yet, such a static approach doesn't match how organizations operate in the real world: They give people who show good judgment the ability to use sensitive data and resources with minimal interference but apply more stringent controls if mistakes or poor choices are made.

Forcepoint is a pioneer in such "risk-adaptive" protection, which dynamically chooses which policies to enforce based on users' own actions, whether their devices are up to date with corporate guidelines, the sensitivity of the data they are trying to use and other factors.



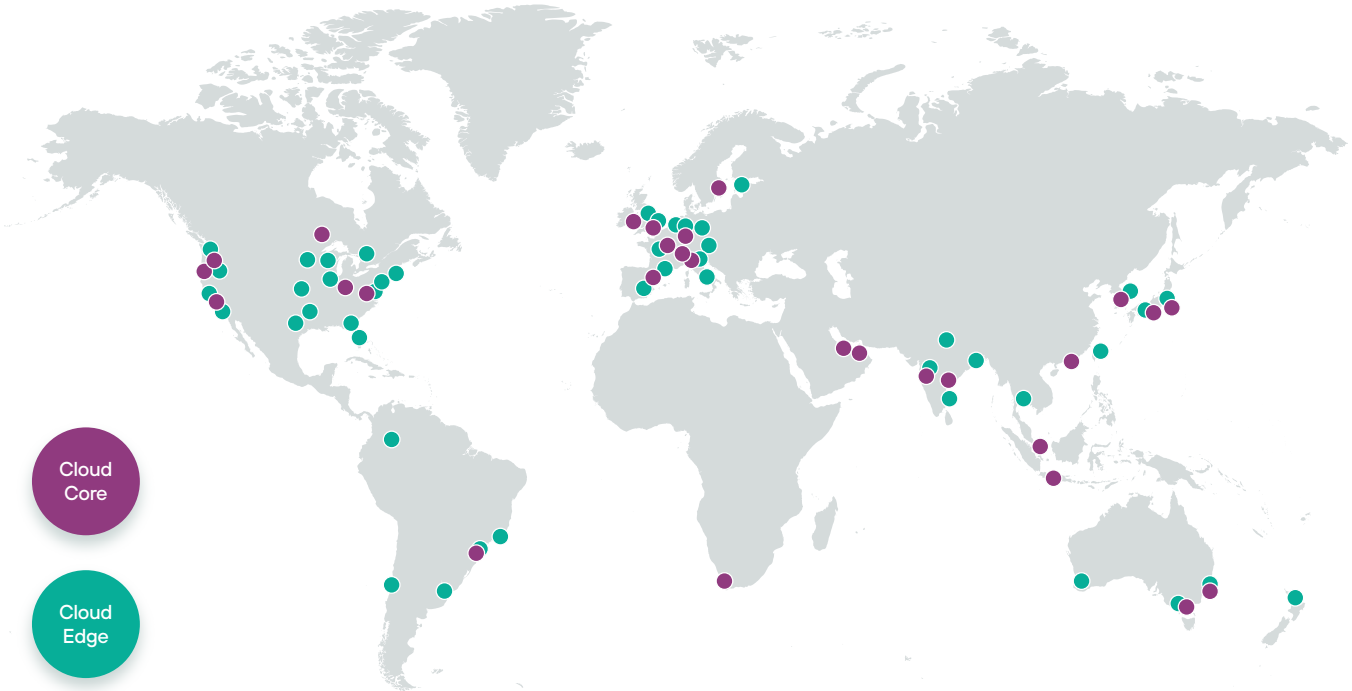
This approach automates and personalizes security, giving people the freedom to use sensitive data in innovative ways while focusing enforcement on the situations where it's needed most. Forcepoint incorporates this technology into our enterprise DLP solutions, which can be used to protect data across a wide range of channels such as on endpoint devices, in networks and in email, as well as in cloud and web applications that are secured with the SSE services in Forcepoint ONE. **The result is better user productivity, lower operating costs (easier policy definition, fewer urgent helpdesk calls about users being blocked) and less risk.**

Hyperscaler cloud-native, continuous availability

Cloud services are typically deployed in one of several ways:

- → **Proprietary data centers –** In the early days of the web, vendors that wanted to offer Software-as-a-Service needed to build and maintain their own data centers. While this provides the greatest level of control, and initially was often the only option, now the cost it requires makes it very uncommon.
- → **Colocation facilities –** Today, when vendors talk about "their" data centers, they usually are referring to colocation facilities owned and operated by others. This takes less effort than building a proprietary data center, but still requires a significant amount of complexity and cost to operate.
- → **Hyperscaler public clouds –** Increasingly, when organizations go to put applications in the cloud, the fastest way is to use public cloud environments such as Amazon (AWS), Microsoft (Azure), Google (GCP), Oracle (OCI) and others. Known as "hyperscalers" due to their focus on providing massively scalable environments, these systems also provide a range of services that application vendors can use to simplify their own development. In addition, hyperscalers are often already available in most of the geographies the vendors wish to serve and are built with some of the highest levels of physical security.

Forcepoint ONE was designed from the start to run on hyperscalers. Built on AWS, it provides a regional presence on every continent except Antarctica:



Its elastic scalability enables services to be scaled up or down dynamically. For example, if a large number of users come together in a single location, Forcepoint ONE can spin up additional capacity without requiring the deployment of physical hardware. In addition, with so many applications now hosted on hyperscalers (50% of the Top 10k websites, 40% of the Top 100k websites, 23% of the Top 1 Million websites are in AWS), having Forcepoint ONE based there also keeps security close to apps and their data.

The Forcepoint ONE platform is designed to provide continuous availability with no need for planned maintenance downtime. **It uses a "blue/green" deployment strategy that enables updates and new capabilities to be pushed live without taking the service offline**.

The result: better productivity and fewer frantic calls to helpdesks.

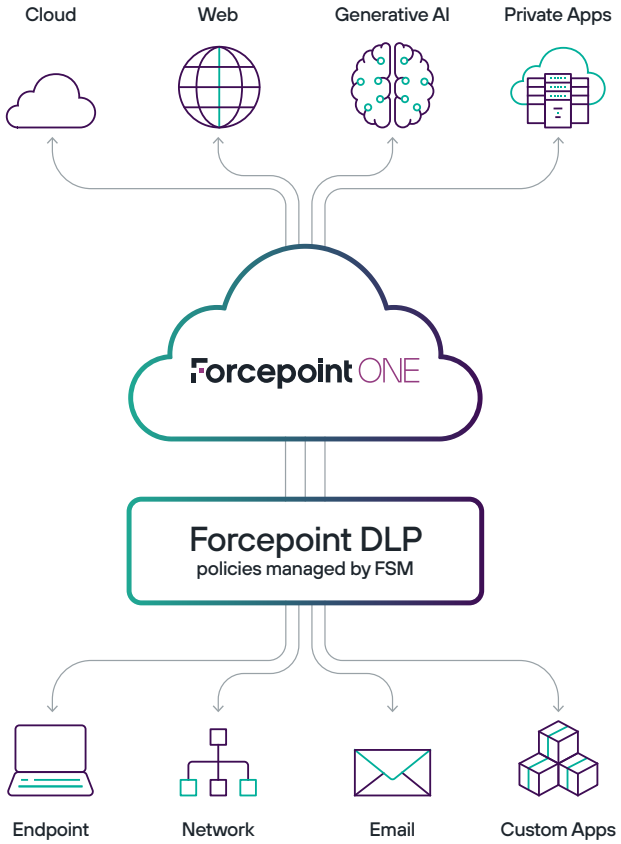
Delivering data security everywhere – even for generative AIs

Forcepoint's solutions work together to enable the same data security policies to be enforced seamlessly from the endpoint to the cloud – and everywhere in between. This enables organizations to manage data security from a single console, with consistent visibility and control. It goes beyond the basic pattern matching of most SSE gateways, providing full enterprise-class security, complete with Forcepoint's pioneering risk-adaptive protection and Zero Trust-based continuous monitoring.

With the rapid emergence of innovations such as ChatGPT and others, strong data security is more important now than ever. Generative AIs are the latest form of "shadow IT": they offer tremendous gains in productivity, but potentially can put sensitive data at great risk.

Forcepoint enables you to take advantage of generative AIs while retaining control of who can use them and how:

- → Limit access to specific groups or individuals who are authorized to test or use AIs.
- → Control file uploads as well as cut-and-paste.
- → Inspect and protect sensitive data against leakage.



Forcepoint ONE: Data-first SASE for the modern world

SASE has quickly gone from being an academic architecture to the most common way organizations plan to connect and protect their modern workforces. Forcepoint ONE brings together more than a decade's worth of experience in each of data-focused security, direct-to-internet networking and cloud services to provide a comprehensive platform for safely giving users fast, efficient access to business resources at every stage of an organization's journey to the cloud.

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.

[FP-Whitepaper-Forcepoint ONE: A Unique, Data-First SASE Platform-EN] 17Aug2023