Forcepoint ONE Top Unique Technologies

Forcepoint

Brochure

Forcepoint ONE Top Unique Technologies

There are many unique technologies used in the Forcepoint ONE security platform. These technologies set Forcepoint ONE apart from other solutions and ensure Forcepoint ONE has maximum visibility and control of access and data movement while maximizing performance and ease of use.

Auto-Scaling, Distributed Architecture on AWS

It is not enough to simply build infrastructure on a public cloud. It must also be architected in a manner that unlocks the underlying reliability, scalability, and performance of the cloud. Forcepoint ONE addresses these concerns with its distributed architecture on AWS and proprietary auto-scaling.

Distributed Architecture on AWS

In order to address the requirements of an ever-growing customer base, Forcepoint ONE is hosted in over 300 data centers on AWS worldwide, including data centers on AWS GovCloud. Forcepoint ONE data centers are specialized into three categories as explained below.

1. **Global Core Data Centers.** These are multi-homed redundant data centers built with the ability to support all Forcepoint ONE functionality. They uniquely include the ability to perform data analysis function such as:
   - → Scanning data at rest in SaaS and IaaS for sensitive data and malware
   - → Scanning SaaS and IaaS security configurations for risky settings
   - → Ingesting and analyzing event logs from Forcepoint ONE on-device agents and third-party systems such as routers and firewalls
2. **Local Edge Data Centers.** Forcepoint ONE is hosted on over 200 local edge data centers across population centers worldwide. The primary function of these data centers is granular access control with malware and sensitive data scanning of data-in-motion between users and the web, the cloud, and private web applications. Placing these data centers in major population centers lets Forcepoint ONE minimize latency and optimize user experience.
3. **CDN Caches.** CDN caches store repeatedly requested assets close to the end user to improve performance. An example would be caching query results for web browsing policies requested by the on-device SWG.

With over 300 points of presence in major population centers, Forcepoint ONE minimizes latency and optimizes user experience.

With auto-scaling, Forcepoint ONE accommodates surges in user traffic and large data-at-rest scanning jobs while maintaining 99.99% uptime.

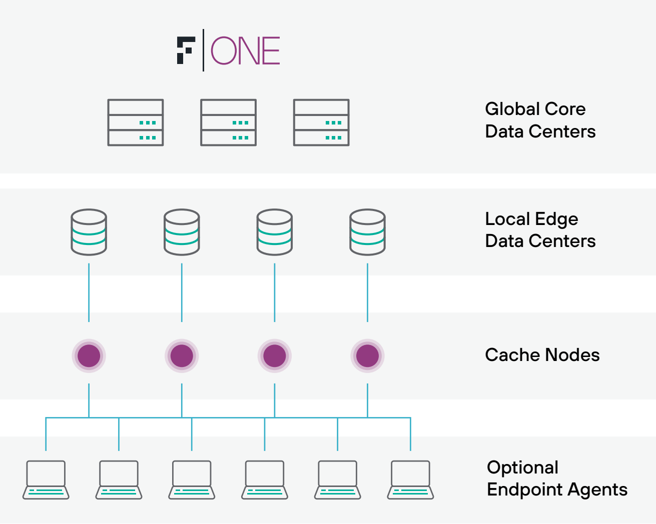


Figure 1: Forcepoint ONE SASE Fabric

Auto-Scaling

Forcepoint ONE uses a proprietary method to ensure that each data center scales up as load increases and scales down when load is reduced. Each data center starts with a baseline configuration of components including databases, Elasticsearch nodes, Hadoop nodes, DLP scanning nodes, and malware engines. If the load on any node crosses a threshold for a sustained period, the node automatically clones itself and becomes part of the same load balanced application tier. Similarly, when the load decreases, nodes can be removed from the tier and deleted. This ensures high service levels are maintained without having to overprovision infrastructure.

The value of this scaling is made apparent in these two use cases.

1. When many Forcepoint ONE users from many customers converge on a popular industry trade show, like RSA, the Forcepoint ONE local edge data center closest to the convention venue will automatically scale up to handle the load and minimize impact on user experience.
2. When a customer uses Forcepoint ONE to scan Google Drive files of all of its users for sensitive data or malware, the task can be completed in minutes compared to many hours if using another vendor's data-at-rest scanning technology.

The combination of a distributed architecture and auto-scaling results in Forcepoint ONE having verified uptime of 99.99% since 2015.

Agentless reverse proxy with AJAX-VM for accessing any web application from any device

The Forcepoint ONE reverse proxy is software running in our global and local data centers, while the AJAX-VM is complementary software running inside the end user browser. Both work together to ensure that Forcepoint ONE can manage traffic between any device and any managed web application, without the need for agent software running on the device. This makes Forcepoint ONE an ideal solution for controlling access to managed SaaS and private web applications from any device, including employee BYOD and contractor devices.

Reverse Proxy

The Forcepoint ONE reverse proxy is a key component of our Cloud Access Security Broker (CASB) and Zero Trust Network Access (ZTNA) solutions. It applies granular access control to ensure only certain users, from allowed devices and locations, can access managed web applications. It also enforces policies that scan data in motion for sensitive data or malware. To perform these functions, the reverse proxy must be in line between all web requests from the browser and all responses from the target web server. This can be ensured by configuring your tenant account in your managed web application to forward corporate email address login attempts to Forcepoint ONE or a third-party IdP integrated with Forcepoint ONE. (See section on SAML integration below for details). With that integration in place, the user browser session is redirected to the Forcepoint ONE reverse proxy which creates a second complementary session between the reverse proxy and the actual target website as shown in the figure below.

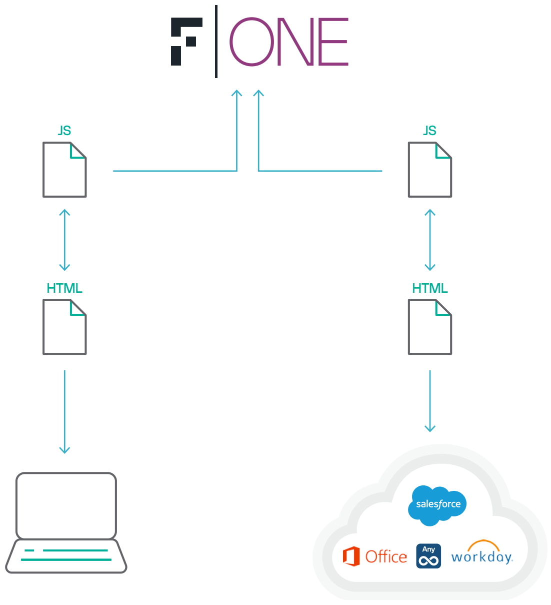


Figure 2: Forcepoint ONE Reverse Proxy Dual Browser Sessions

On the left is the session between the user browser and software in the reverse proxy that looks like the target web server to the browser. On the right is the session between the target web server and software in the reverse proxy that looks like a client browser to the web server. Managing these two tightly coupled sessions means the reverse proxy needs to maintain separate cookies for each session and perform rewrites of URLs to ensure traffic between the browser and the website always passes through the reverse proxy.

AJAX-VM

Modern web applications use JavaScript to support dynamic, real-time interactions between the browser and website. In particular, AJAX calls, which stand for Asynchronous JavaScript And XML, are becoming more popular as web applications look to bring in additional content dynamically. The dynamic nature of AJAX calls means that associated HTTP requests may be created where URLs and cookies need to be rewritten on the fly in the browser in order to be properly received and processed by the reverse proxy server. Failure to do this results in sections of a web page being blank or displaying an error message. To address this problem, Forcepoint ONE has created an abstraction layer within the browser code called AJAX-VM.

The code to support the AJAX-VM is JavaScript added into every web page received from the target web site by the reverse proxy before sending that page down to the end user browser. When an AJAX call is about to be executed, the AJAX-VM JavaScript code intercepts that AJAX call and performs any necessary preprocessing and post-processing to ensure the AJAX call uses the correct URLs and cookies before the corresponding HTTP requests are issued by the browser. The effect is to create an abstraction layer that can handle all types of JavaScript functions while maintaining web page functionality. The result is the Forcepoint ONE reverse proxy is able to work with any web application without special modifications even when the website is modified.

The Forcepoint ONE Reverse Proxy provides contextual access control and scanning of data-in-motion for sensitive data or malware between any managed SaaS application and any user on any device.

The AJAX-VM browser abstraction layer ensures the Forcepoint ONE reverse proxy is able to work with any web application without special modifications even when the website is modified.

Patented SAML IdP integration with denial of service protection

A key function of security is authentication. Forcepoint ONE offers three modes for authentication:

1. SAML relay with a third-party IdP
2. SAML relay with Forcepoint ONE built-in IdP
3. SAML ACS proxy with a third-party IdP

SAML Relay with a Third-Party IdP

SAML relay is the most common method to integrate Forcepoint ONE with a third-party IdP. With SAML relay, Forcepoint ONE is configured as the IdP for your tenant in the SaaS application, but in addition, the third-party IdP is configured as the IdP for Forcepoint ONE as a service provider. In this mode, Forcepoint ONE sees both successful and failed authentications, and can therefore provide better anomaly detection and Denial of Service (DoS) protection.

With SAML relay, if a user attempts to login to the SaaS application directly with their company email address, the following steps occur:

1. The SaaS application recognizes that Forcepoint ONE is the IdP for the domain name of the user and sends a redirect message to the user browser that redirects the user to Forcepoint ONE. This message includes a SAML authentication request to Forcepoint ONE in the message body.
2. Forcepoint ONE reads the authentication request in the message body. Since Forcepoint ONE knows that the IdP for this application tenant is the third-party IdP, Forcepoint ONE sends a new redirect message to the user browser that redirects the user to the third-party IdP. This message includes a SAML authentication request to the third-party IdP in the message body.
3. The third-party IdP reads the authentication request in the message body and checks if the entity that needs to be authenticated is known to the third-party IdP. If yes, and assuming the user is not already logged in to the third-party IdP, the user is redirected to the third-party IdP login page where the user enters their credentials for authentication.
4. Once the third-party IdP authenticates the user, it sends a POST request message to the user browser which redirects the user back to Forcepoint ONE. This message includes a SAML authentication response from the third-party IdP to Forcepoint ONE in the message body.
5. Forcepoint ONE first validates the authenticity of the SAML response. Then, assuming the user is not already logged in to Forcepoint ONE, if enabled, Forcepoint ONE will query the device for the existence of a self-signed or third-party certificate to determine if the user is logging in from a managed device. Depending on the login policy for that connection, the user may then be redirected to an MFA solution to complete the login process.
6. Once the MFA challenge is correctly answered and the user is logged into Forcepoint ONE, Forcepoint ONE sends a POST request to the user browser, with the SAML authentication response from Forcepoint ONE to the SaaS application in the message body.

   → If the Forcepoint ONE proxy policy associated with this connection allows direct access to the SaaS application, the POST request redirects the user directly to the SaaS application URL, bypassing the reverse proxy.

   → If, however, the proxy policy associated with this connection requires secure access to the SaaS application, the POST request redirects the user to a URL on the reverse proxy that is used for proxying this application, and the reverse proxy creates the complementary connection between it and the SaaS application (as described in the Reverse Proxy section above), completing the end-to-end connection. The reverse proxy can now enforce DLP and malware protection per the proxy policy.

   In either case, the user is logged in to their SaaS application account once the application has validated the authenticity of the SAML response.

These steps are summarized in the figure below.

SAML Relay — Authentication Flow

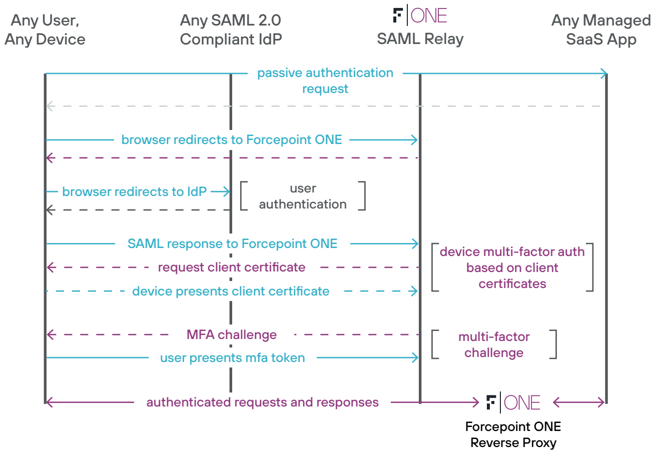

Any User,
Any Device
Any SAML 2.0
Compliant IdP
ONE
SAML Relay
Any Managed
SaaS App
passive authentication request
browser redirects to Forcepoint ONE
browser redirects to IdP
user authentication
SAML response to Forcepoint ONE
request client certificate
device presents client certificate
device multi-factor auth based on client certificates
MFA challenge
user presents mfa token
multi-factor challenge
authenticated requests and responses
ONE
Forcepoint ONE
Reverse Proxy

Figure 3: Traffic flow for SAML Relay mode

SAML Relay with the Forcepoint ONE Built-in IdP

Forcepoint ONE uniquely offers customers complete SAML-based authentication without relying on a third-party IdP by using its built-in IdP, which is Microsoft Active Directory Federation Services (ADFS). This mode is functionally equivalent to SAML relay with a third-party IdP. Simply replace “third party IdP” with “Forcepoint ONE built-in IdP” in the steps for SAML relay with a third-party IdP for a description of this mode. In this mode, Forcepoint ONE sees both successful and failed authentications, and can therefore provide better anomaly detection (UEBA) and Denial of Service (DoS) protection.

SAML ACS Proxy with a Third-Party IdP

With SAML Assertion Consumer Service (ACS) Proxy, the third-party IdP is specified as the IdP for the SaaS tenant, and Forcepoint ONE is specified as the IdP for the third-party IdP for that SaaS application. In this mode, Forcepoint ONE may not see failed authentication attempts from the user, and therefore cannot effectively detect anomalies to deliver denial of service protection.

In ACS Proxy mode, if a user attempts to login to the SaaS application directly with their company email address, the following steps occur.

1. The SaaS application recognizes that the third-party IdP is the IdP for the domain name of the user and sends a redirect message to the user browser that redirects the user to the third-party IdP. This message includes a SAML authentication request to the third party IdP in the message body.
2. The third-party IdP reads the authentication request in the message body and checks if the entity that needs to be authenticated is known to the third party IdP. If yes, and assuming the user is not already logged in to the third-party IdP, the user is redirected to the third-party IdP login page where the user enters their credentials for authentication.
3. Once the third-party IdP authenticates the user, it sends a POST request message to the user browser which redirects the user to Forcepoint ONE. This message includes a SAML authentication response from the third-party IdP in the message body, which Forcepoint ONE saves for step 5, below.
4. Forcepoint ONE first validates the authenticity of the SAML response and saves the response for use in the next step, below. Then, assuming the user is not already logged in to Forcepoint ONE, Forcepoint ONE may optionally query the device for the existence of a self-signed or third party certificate to determine if the user is logging in from a managed device. Depending on the login policy for that connection, the user may then be redirected to an MFA solution to complete the login process.
5. Once the MFA challenge is correctly answered and the user is logged into Forcepoint ONE, Forcepoint ONE sends a POST request to the user browser, with the SAML authentication response from Forcepoint ONE to the SaaS application in the message body.

   → If the Forcepoint ONE proxy policy associated with this connection allows direct access to the SaaS application, the POST request redirects the user to the SaaS application URL, bypassing the reverse proxy.

   → If, however, the proxy policy associated with this connection requires secure access to the SaaS application, the POST request redirects the user to a URL on the reverse proxy that is used for proxying this application, and the reverse proxy creates the complementary connection between it and the SaaS application URL (as described in the Reverse Proxy section above), completing the end-to-end connection. The reverse proxy can now enforce DLP and malware protection per the proxy policy.

In either case, the user is logged in to their SaaS application account once the application has validated the authenticity of the SAML response.

These steps are summarized in the figure below.

ACS Proxy — Authentication Flow

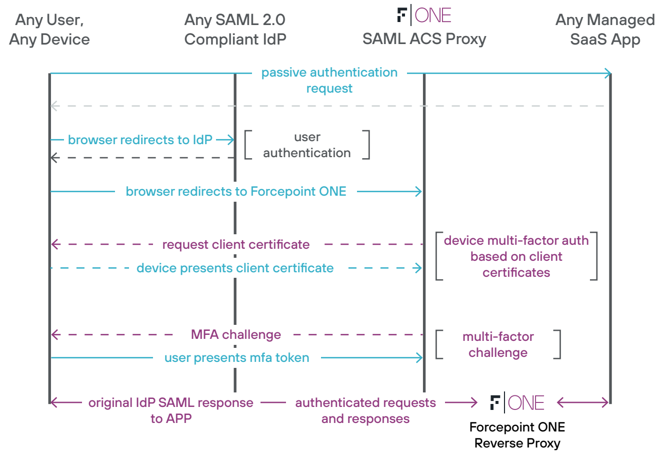

Any User,
Any Device
Any SAML 2.0
Compliant IdP
ONE
SAML ACS Proxy
Any Managed
SaaS App
passive authentication request
browser redirects to IdP
user authentication
browser redirects to Forcepoint ONE
request client certificate
device presents client certificate
device multi-factor auth based on client certificates
MFA challenge
user presents mfa token
multi-factor challenge
original IdP SAML response to APP
authenticated requests and responses
ONE
Forcepoint ONE
Reverse Proxy

Figure 4: Traffic flow for ACS Proxy mode

Forcepoint ONE is designed to integrate with any SAML 2.0 IdP, but it also can be used with its own built-in IdP service.

When integrating Forcepoint ONE with an IdP in SAML relay mode, Forcepoint ONE can provide a level of denial of service protection by rejecting repeated brute-force login attempts.

Unified Agent with Auto-Generated Key and Certificate

Forcepoint ONE uses a single unified agent for Windows or macOS for all of the following functions:

→ Forward proxy CASB function for non-browser applications such as the Outlook for Windows client.

→ On-device SWG (see below), and

→ ZTNA for non-web applications such as those using SSH and RDP.

With most cloud security vendors, to allow encrypted communication between the user's end device and the vendor's cloud infrastructure, the customer's security team must store private keys and associated certificates on the vendor's hosted server, with the associated loss of trust. In addition, the customer has to manage client certificates on each endpoint.

Forcepoint ONE eliminates these requirements with our unique, patent-pending technology. Here, Forcepoint ONE uses self-managed keys and certificates on our hosted servers. There is no need to place institutional keys and certificates in the cloud, mitigating risk. In addition, each on-device agent carries a fully functional crypto engine. Keys and certificates are self-generated periodically on the endpoint agent. Even if a device is stolen or compromised, the keys on the device cannot be used to spoof any other device. In addition to enhancing security, there is no administrative overhead required to manage certificates on the endpoints.

The Forcepoint ONE unified on-device agent is multi-purpose and supports functions for forward proxy CASB, on-device SWG, and ZTNA for non-web applications.

Unique auto-generated keys and certificates eliminate the overhead of customer-proved key management, and a stolen key and certificate from one agent cannot be used to gain access from another device.

On-device Secure Web Gateway (SWG)

A Secure Web Gateway (SWG) is software for controlling access to websites and SaaS not managed by corporate IT. Several vendors claim to have "on-device" SWGs, but the details on how the on-device SWG software interacts with the security provider's infrastructure makes all the difference with respect to performance, security, and ease of management. The Forcepoint ONE on-device SWG architecture uniquely addresses these concerns.

Most SWG architectures take a performance hit because all web traffic must pass through the security provider's infrastructure for inspection before being forwarded to the destination website.

This architecture leads to a phenomenon called hairpinning. Like the shape of a hairpin, the traffic takes a detour before getting to its final destination. This architecture not only adds latency due to propagation delays of the extra network hop, but adds additional latency when the security provider's infrastructure is overloaded due to unexpected peaks in traffic.

Forcepoint ONE addresses this issue by not requiring all web traffic originating on the user device to be sent to our infrastructure on AWS. Instead, our on-device SWG only needs to send traffic to our infrastructure on AWS for two use cases: when the user attempts to access a URL not previously accessed, and when the user tries to upload a file to or download a file from an unsanctioned URL associated with a SWG content.

1. New URL access: when the user tries to reach a URL for the first time, the on-device SWG queries the closest Forcepoint ONE CDN cache node server 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.
2. 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 SWG content 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 SWG content.

For file upload attempts the, following steps occur:

- → A copy of the file to be uploaded is sent to the closest Forcepoint ONE local edge data center on AWS to scan for malware or sensitive data.
- → If a match is found, a message is sent from the Forcepoint ONE data center to the on-device SWG indicating that the upload should be blocked.
- → If no match is found, a message from the Forcepoint ONE data center is sent indicating the file can then be uploaded from the user device directly to the unsanctioned website.

For file download attempts, the following steps occur:

- → The file is downloaded and kept in quarantine on the device while a copy of that file is also sent to the closest Forcepoint ONE local edge data center for malware or sensitive data scanning.
- → If a match is found, the SWG is notified and the quarantined file is deleted.
- → If a match is not found, the SWG is notified and the file is released from quarantine and appears in the user's default download folder.

The difference between the way the Forcepoint ONE on-device SWG handles web traffic compared to other vendors is highlighted in the figure below.

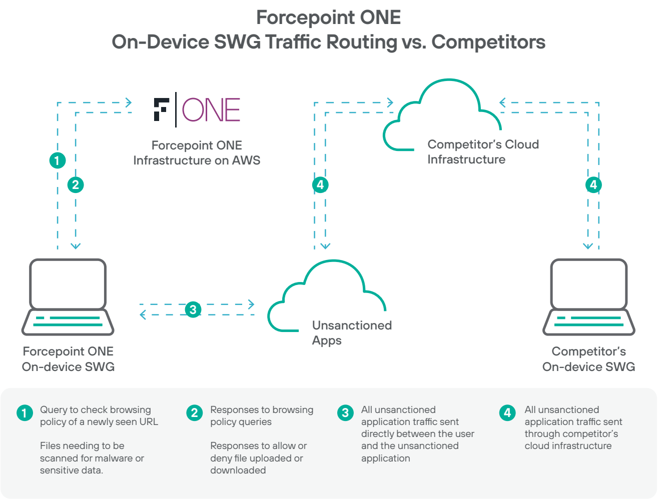

Forcepoint ONE
On-Device SWG Traffic Routing vs. Competitors
F ONE
Forcepoint ONE
Infrastructure on AWS
Competitor's Cloud
Infrastructure
1
2
4
4
3
Unsanctioned
Apps
Forcepoint ONE
On-device SWG
Competitor's
On-device SWG
1 Query to check browsing policy of a newly seen URL
Files needing to be scanned for malware or sensitive data.
2 Responses to browsing policy queries
Responses to allow or deny file uploaded or downloaded
3 All unsanctioned application traffic sent directly between the user and the unsanctioned application
4 All unsanctioned application traffic sent through competitor's cloud infrastructure

Figure 5: Forcepoint ONE on-device SWG traffic flow compared to competitors

By not requiring all HTTP traffic to pass through the Forcepoint ONE infrastructure on AWS, the net effect of the unique on-device SWG architecture is to significantly increase effective throughput. For example, when Forcepoint ONE was competing against two other SWG vendors for a SWG deployment for a Fortune 100 company, in benchmark tests Forcepoint ONE had nearly double the performance compared to the other vendors as shown in the chart below.

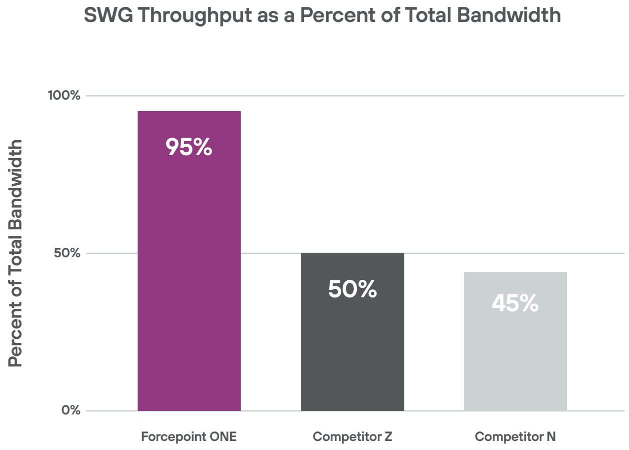


Figure 6: Forcepoint ONE SWG throughput compared to competitors

The unique on-device SWG architecture of Forcepoint ONE, combined with the use of self-managed keys and certificate inherent with the unified Forcepoint ONE agent, provides clear advantages with respect to performance, security, and ease of management.

The Forcepoint ONE on-device SWG's unique traffic flow increases effective throughput up to 90% greater than competitors.

Auto-generated and auto-rotated keys and certificates reduces risk and simplifies management.

Field Programmable SASE Logic (FPSL)

The advanced match patterns of Forcepoint ONE let administrators build complex data patterns with Boolean logic for detecting sensitive data in files and enforcing DLP. Field Programmable SASE Logic (FPSL) extends this string matching capability to any part of any HTTP request. It lets administrators build logic that will detect any user interaction with any web page, log that event, and optionally block it. This powerful capability unlocks a near limitless number of use cases that wouldn't be available out-of-box.

Use cases include:

→ Block logins to corporate SaaS applications using a personal email address

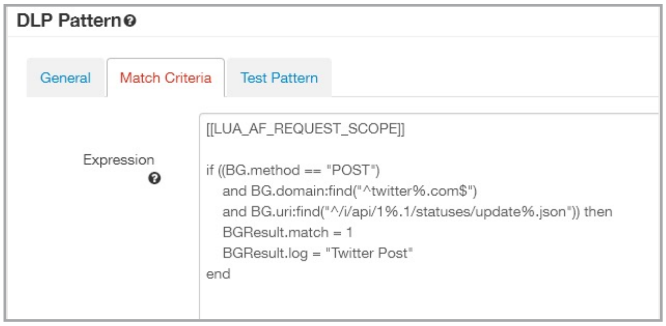
→ Log every file upload to personal Google Drive accounts for users in a risky users group

→ Block likes in Facebook

→ Only let members of the marketing group post to LinkedIn

→ Block sensitive content in a Twitter post

FPSL exposes a scripting language that Forcepoint ONE engineering uses for our own product development: LUA. An example of a script that matches against post requests to Twitter is shown in the figure below.

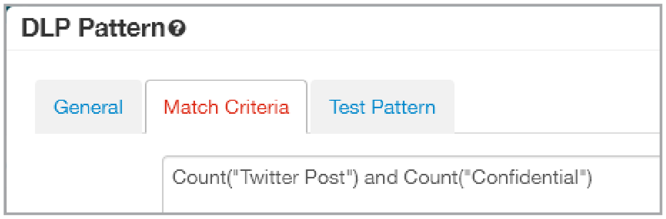


```
[[LUA_AF_REQUEST_SCOPE]]

if ((BG.method == "POST")
   and BG.domain:find("^twitter%.com$")
   and BG.uri:find("^/i/api/1%.1/statuses/update%.json")) then
   BGResult.match = 1
   BGResult.log = "Twitter Post"
end
```

Figure 7: LUA script for detecting and logging Twitter posts

Since an advanced match pattern can reference other match patterns, the pattern for matching Twitter posts can be combined with the pattern to match the word "confidential" to block all Twitter posts containing "confidential" as shown in the example below.



```
Count("Twitter Post") and Count("Confidential")
```

Figure 8: Advanced match pattern that combines a LUA script match pattern with an existing match pattern to block Twitter posts that contain the word "confidential"

LUA scripts can look for a match in any HTTP request attribute (as shown in the table below) as well as the body of the request.

INPUT	TYPE	DESCRIPTION	EXAMPLE
BG.domain	string	domain of an http request	"www.google.com"
BG.method	string	http method name (PUT, POST, GET, etc.)	"POST"
BG.uri	string	directory path of request	"/search"
BG.qs	string	query string of request	"x=1&y=%2Es&z="
BG.cookie	string	request cookie	"k1=v1; k2=v2"

Table 1: HTTP request attributes available for use in a LUA script

Use LUA script match patterns in web content policies to control unsanctioned web applications and use them in proxy policies to control managed web applications.

Forcepoint ONE FPSL lets admins control user interaction with any aspect of any web page and can block various actions like posting messages or editing documents.

FPSL is implemented as LUA scripts in Forcepoint ONE Advanced match patterns, which means you can combine LUA script match patterns with other match patterns to refine your level of control.

Agentless Zero Trust Network Access (ZTNA)

The Forcepoint ONE agentless ZTNA is the extension of our agentless reverse proxy CASB functions to any web application hosted behind a firewall. This includes both custom web applications and enterprise versions of SaaS applications, in both on-premises data centers and in IaaS virtual private clouds.

Our agentless ZTNA leverages the same real-time contextual access control, agentless AJAX-VM technology, and real-time DLP and threat protection as our reverse proxy CASB.

ZTNA is a great alternative to VPN access because in addition to providing contextual access control, malware scanning, and DLP for data in motion, it only allows access to a particular application and no other applications or resources on the same private network.

Enabling Forcepoint ONE ZTNA for a Forcepoint ONE tenant requires installing the Forcepoint ONE ZTNA connector software as a cluster of load-balanced VMs behind the firewall of your private data center, as shown in the figure below.

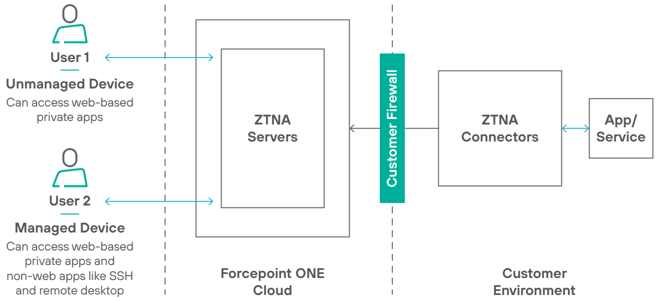


Figure 9: Forcepoint ONE ZTNA Connector Architecture

The ZTNA connector initiates an encrypted connection to a corresponding ZTNA server in a nearby Forcepoint ONE local edge data center on AWS. Because the connection is initiated by the ZTNA connector, no inbound ports need to be opened in the private data center firewall.

The ZTNA connector VM is offered as an OVA image of a hardened Linux kernel configured with Docker, which launches the ZTNA connector software running as a Docker container. A script offered by Forcepoint ONE lets an administrator build an Amazon Machine Image (AMI) for the ZTNA connector, based on a customer supplied CentOS image, which can be deployed in an AWS private virtual cloud.

The ZTNA connector initiates an encrypted connection to a corresponding ZTNA server in a nearby Forcepoint ONE local edge data center on AWS. Because the connection is initiated by the ZTNA connector, no inbound ports need to be opened in the private data center firewall.

The ZTNA connector VM is offered as an OVA image of a hardened Linux kernel configured with Docker, which launches the ZTNA connector software running as a Docker container. A script offered by Forcepoint ONE lets an administrator convert the ZTNA connector OVA into an Amazon Machine Image (AMI) which can be deployed in an AWS private virtual cloud.

Unlike VPN solutions, Forcepoint ONE ZTNA lets you limit access to individual applications while enforcing DLP and malware protection.

Since the Forcepoint ONE agentless ZTNA leverages the same reverse proxy technology as our CASB, it is the perfect solution for organizations who want CASB and ZTNA managed from the same platform.

The Unique Technology Benefits of Forcepoint ONE

→ **Visibility and Reporting.** Forcepoint ONE records all user logins. The agentless reverse proxy allows visibility of file uploads and downloads for managed applications accessed from any device. On-device SWG provides detailed reporting of unsanctioned app usage and file uploads and downloads from managed devices.

→ **Threat Protection.** Forcepoint ONE integration with SAML IdPs provides DoS protection in SAML relay mode. Forcepoint ONE applies granular user access control including a step-up to MFA based on location or device posture. The agentless reverse proxy can apply file blocking, encryption, and DRM for files exchanged with managed applications from any device. On-device SWG can block access to websites based on category or risk score and block transfer of files containing sensitive data or malware.

→ **Flexibility and Ease of Use.** Forcepoint ONE integrates with any SAML IdP. FPSL provides flexible control of any user interaction with any website. Forcepoint ONE CASB, ZTNA, and SWG can all use the same rules for controlling user website interactions and controlling movement of sensitive data or malware.

→ **Reliability and Performance.** The distributed, auto-scaling architecture of Forcepoint ONE on AWS ensures low latency, high performance, and 99.99% uptime. On-device SWG has almost twice the effective throughput of competitors.

Learn more about Forcepoint ONE visit the Forcepoint ONE product page.

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-Top Unique Technologies-Brochure-EN] 18Feb2022