Secure SD-WAN
Security functions

PRODUCT BRIEF

Open Systems delivers powerful security protection at every level of the SD-WAN

Open Systems services are ISO 27001 certified.

Secure SD-WAN

Integrated security means you don't have to manage – or even worry about – disparate third-party solutions

Open Systems delivers integrated, multi-layered network security and protection that is seamlessly built-in to our Secure SD-WAN, and present in every edge device. In addition, our next-gen firewall, secure web gateway, DNS filter, and intrusion detection and prevention technologies all provide continuous data for advanced machine-learning algorithms that enhance our detection and response capabilities. This highly automated system is fully integrated with our expert-level engineers, who work with you daily to ensure your security posture.

Simplify and enhance network security

We take a holistic approach to SD-WAN security

Avoid the need to acquire and manage multiple additional bolt-on security packages in your SD-WAN. Open Systems integrates comprehensive security features, so you can manage centrally and run worry-free.

Enable firewalls within your SD-WAN

Our Next-Gen Firewall protects your organization's network servers and end-user machines not just by filtering traffic from both the internal network and the internet – but by leveraging multiple security zones within the network itself. Easily deploy a multi-tiered corporate security policy globally by managing everything from a single pane of glass, with filtered communications between zones, access-control granularity, including optional site-specific rules, and logging.

Maximize protection against malicious sites

Enforce your organization's internet access and security policy for resources located in the public internet. Our integrated Secure Web Gateway, which includes SSL scanning, URL filtering, and malware protection, increases the level of protection of client machines against malicious content and restricts access to URL categories.

Whether from malware or an inadvertent software connection, Open Systems' DNS Filter blocks connections to malicious and undesirable domains in the internet by interrupting communications regardless of connection type.

Leverage data from across your network

Turn your network into a global mesh of virtual traffic sensors – without additional appliances. Open Systems' AI-driven Network Security Monitoring provides the answer – detecting compromised systems quickly and enabling efficient analysis and response. As with all Open Systems features, you can monitor current network threats globally from the Open Systems Customer Portal, including host details and notifications of suspected malicious activity.

Built-in features that ensure high security

Define a corporate firewall policy centrally, deploy it globally, and allow customization locally

Condense and simplify firewall rules through application-level filtering

Protect all users from malicious web traffic, independent of protocol or client configuration

Apply and control corporate web browsing policy per-user group

Monitor current network threats and get immediate notifications of malicious activity

Activate distributed traffic sensors on your SD-WAN edges with one click

Key differentiators

- Advanced filtering of all network traffic
- Multi-zone approach provides an effective response to a multiplicity of attack surfaces
- Global and local policies provide security with operational flexibility

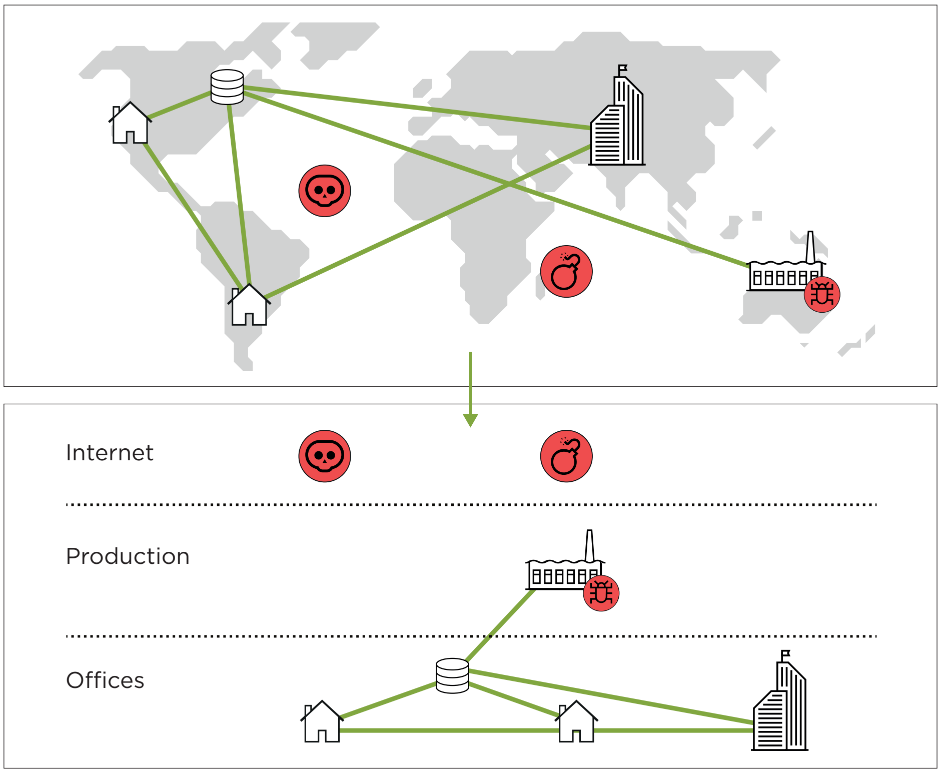
Next-Gen Firewall

Protect global networks from internal and external threats

What are the critical security gaps in today's networks?

Modern businesses employ a local internet breakout strategy to expand their connectivity and agility. In doing so, organizations expose their WAN edge devices directly to the internet and greatly expand the available attack surfaces in a network. Moreover, edge defenses are no longer enough: a secure SD-WAN needs to address the fact that threats can come not only from outside the network (the internet), but from inside as well.

In short, the modern enterprise network is no longer fully trustworthy. So the modern firewall needs to adapt.



Separate your trusted network not only from internet threats but also from doubtful internal sources through multi-security-zone firewalls

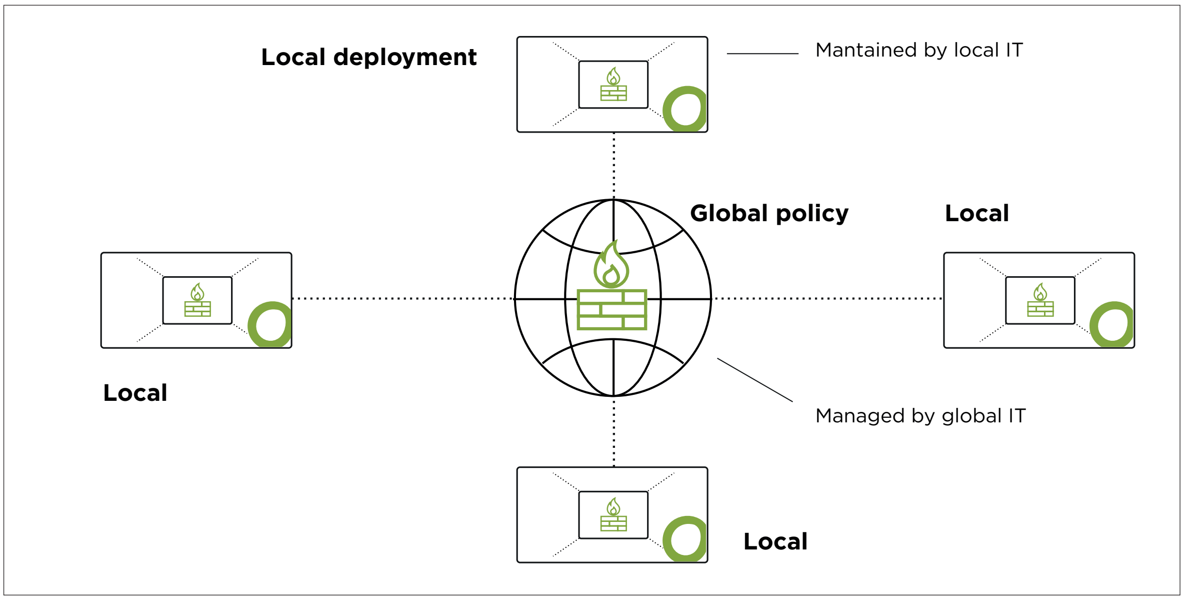
How we protect your network

To address networks in which all locations and connections offer different levels of trust, Open Systems introduced a firewall architecture with distinct security zones, which segments the global network into different zones of security and trust and enables communication between zones to be properly controlled. With this feature, we can filter traffic at transitions between different security zones and maintain security within each zone. Thus, the overall integrity of the SD-WAN can be shielded not only from internet threats but also from doubtful internal sources in untrusted security zones.

High security, low operational overhead

In enforcing multi-zone network firewall policies, we aim for the right balance between security and operability. The Open Systems Secure SD-WAN enables both security and operability in the following ways:

- **Security**. Assets from different security zones can only communicate via certain protocols, as defined in individual firewall rules, and security zones can be shielded from each other by restricting or blocking their zone transitions. For more granular filtering, individual site-specific firewall rules can be implemented to allow access on certain protocols for assets from different zones.
- **Operability**. Through the zoning concept, a lot of different network segments or interfaces can be grouped into one zone of a certain security level. This enables us to define a simple zone transition policy instead of implementing multiple access rules for each individual communication.



The Open Systems distributed firewall provides the ideal balance between security and operability.

From a policy perspective, we offer a hybrid administration model that allows an organization's global IT to enforce a security policy while providing flexibility for local IT to customize the policy where needed.

- **Global IT** defines a global corporate security policy by defining general zone transitions
- **Local IT** maintains and updates local firewall objects. In addition, exceptions or new zones can be defined in collaboration with global IT.

Secure Web Gateway and DNS Filter
Control and protect your users' web traffic

Key differentiators

- Hybrid approach covers all clients
- Protect users from web threats via global access policies
- Prevent malicious connections before they're established

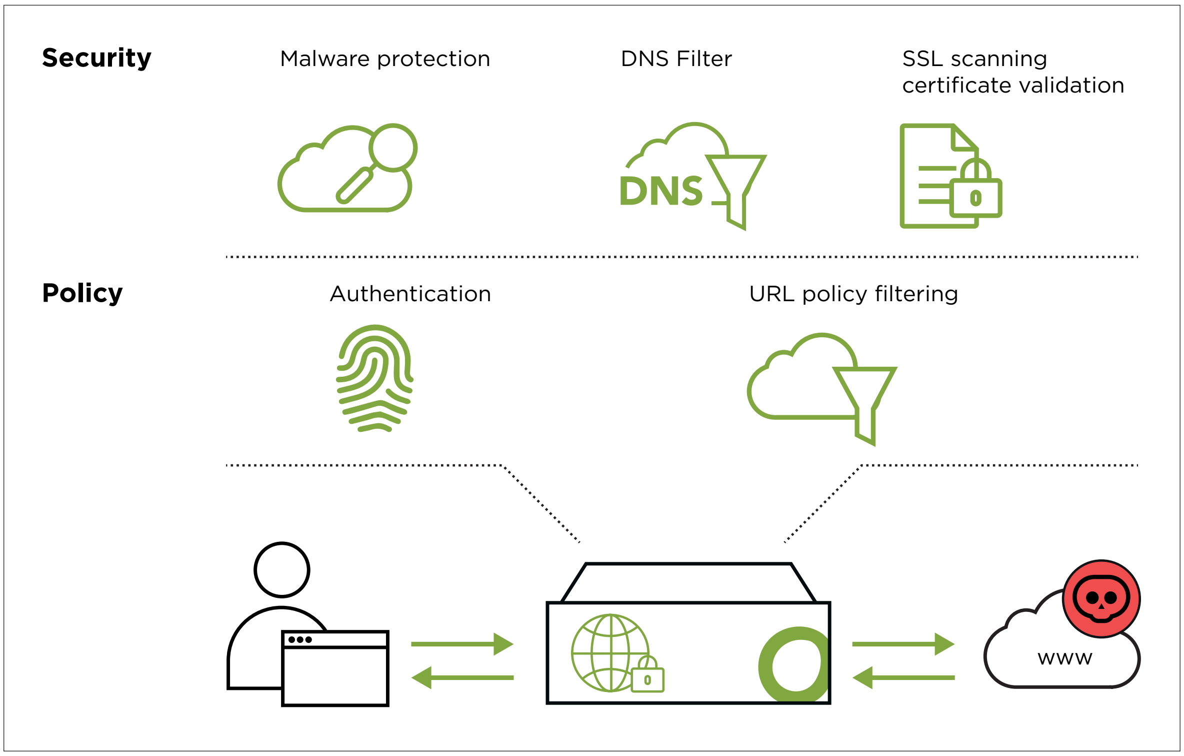
Why do we need to filter web traffic?

Every organization should have a global internet access security policy – not only to protect day-to-day operations but to defend the brand itself. Working together to enforce this security policy, the Open Systems Secure Web Gateway and DNS Filter ensure that network-wide web usage is business-aligned and that users are shielded from malicious web content.

How we protect your network

From a policy perspective, the Open Systems Secure SD-WAN enables organizations to easily manage the enforcement of company business policies through customizable user groups (authentication) and category-based URL and DNS filtering.

At the same time, since most successful cyberattacks start with browsing a compromised website, the Open Systems Secure SD-WAN provides various threat protection measures – such as URL and DNS filtering, malware protection, SSL scanning or certificate validation – to help prevent security breaches.



The Secure Web Gateway helps protect from web threats and enforce your business policy

A hybrid approach to cover all clients in your network

Web traffic policy enforcement, filtering, and protection are delivered through two different built-in modules. While the standalone DNS Filter runs on the Firewall, full-fledged functionality like URL filtering and malware protection, as well as SSL scanning and authentication, are provided through the dedicated Secure Web Gateway module.

The Secure Web Gateway contains the following functions:

- **Authentication** of users enables the creation of different policy groups and different levels of malware protection, URL filtering, and SSL scanning.
- **URL filter** enforces an organization's internet access policy and protects against risks associated with employees' internet use.
- **SSL scanning and certificate validation** applies an existing security and internet usage policy to the HTTPS protocol, expanding coverage of an organization's policy to encrypted traffic (about 85% of all web traffic these days) and preventing viruses, spyware, and Trojans from bypassing malware protection by using HTTPS encryption.
- **Malware protection** uses protocol scanning technologies for HTTP and FTP, as well as a combination of filters, to detect both unknown and known malware. One highlight is the ability to filter for malicious Macros of all Microsoft Office files (Excel, Word, etc.).
- **Phishing protection** (only in combination with the Secure Email Gateway) is a feature in which the Secure Email Gateway and the Secure Web Gateway join forces to make it even more unlikely that users become victims of phishing attacks. The Phishing Protection function combines multiple threat intelligence feeds for both web and email security. If either the Secure Web Gateway or the Email Gateway know that a URL is related to phishing, the user will be protected.

Network Security Monitoring

Eliminate your network blind spots with AI-driven detection of potential attacks.

What are the blind spots in a modern network?

As cyberattacks get more sophisticated, perimeter security is no longer enough to protect the network from external threats. In addition, internal threats (infected clients or machines, USB sticks, etc.) contribute significantly to today's threat landscape. Open Systems Network Security Monitoring, a distributed intrusion detection system, helps to identify and act on signs of a possible cyberattack.

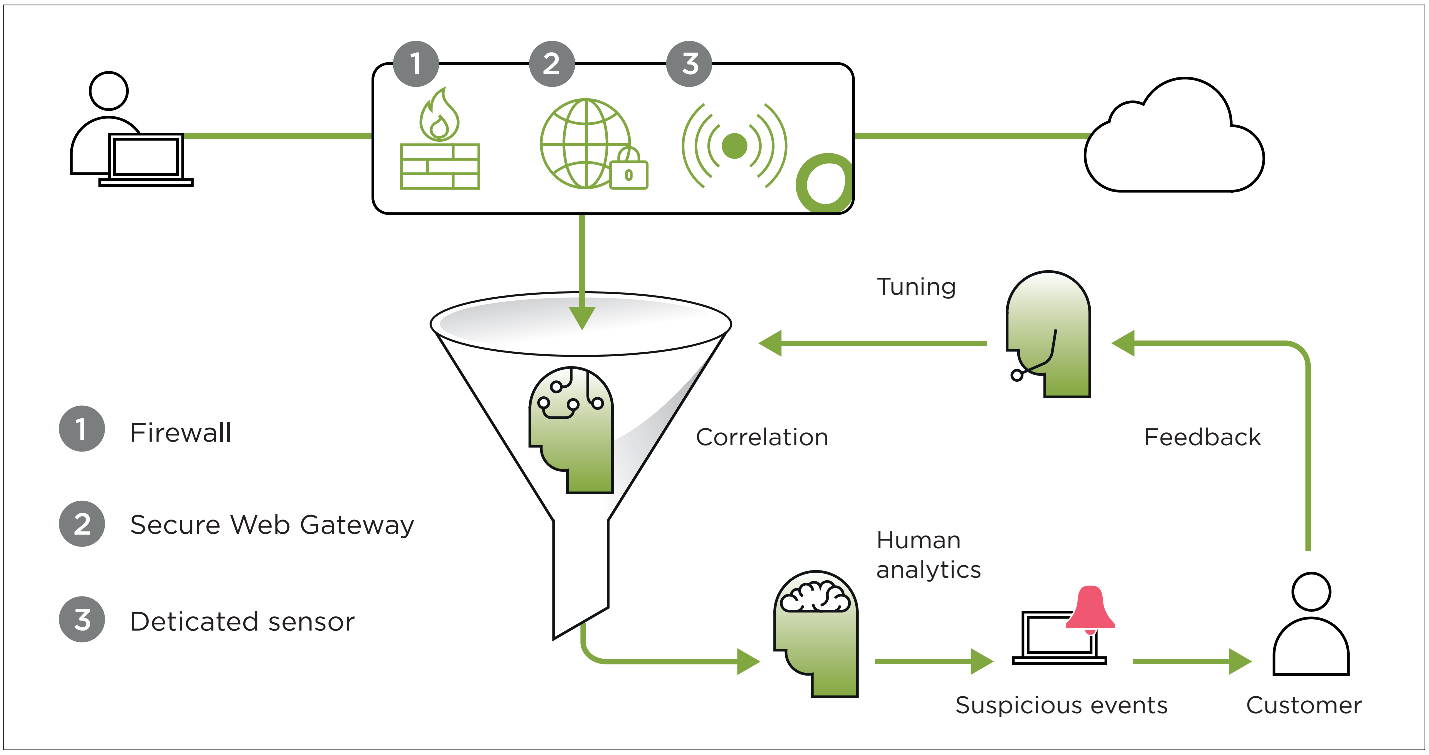
Network Security Monitoring delivers a holistic situational awareness of your network and threat scores for all of your internal assets. With this information, you can act immediately whenever you receive alerts about suspicious activity in your network.

Attacks follow a fairly consistent pattern

Modern cyberattacks proceed from scanning for a network's vulnerabilities, to delivery of malware, to exploitation of a breach. Network Security Monitoring works by checking event logs for indicators of malware delivery – for instance, when downloaded during web browsing – and detecting whether malicious software communicates with a control server outside the WAN. In its focus on finding malware moving data out of the network, Network Security Monitoring is significantly more efficient than other services.

Key differentiators

- Continuous, global monitoring of network threats
- AI-driven data analysis and expert-level engineers
- Functionality is built-in and ready to activate in every edge device



Network Security Monitoring by Open Systems correlates, tunes and analyzes your WAN data and alerts you when needed

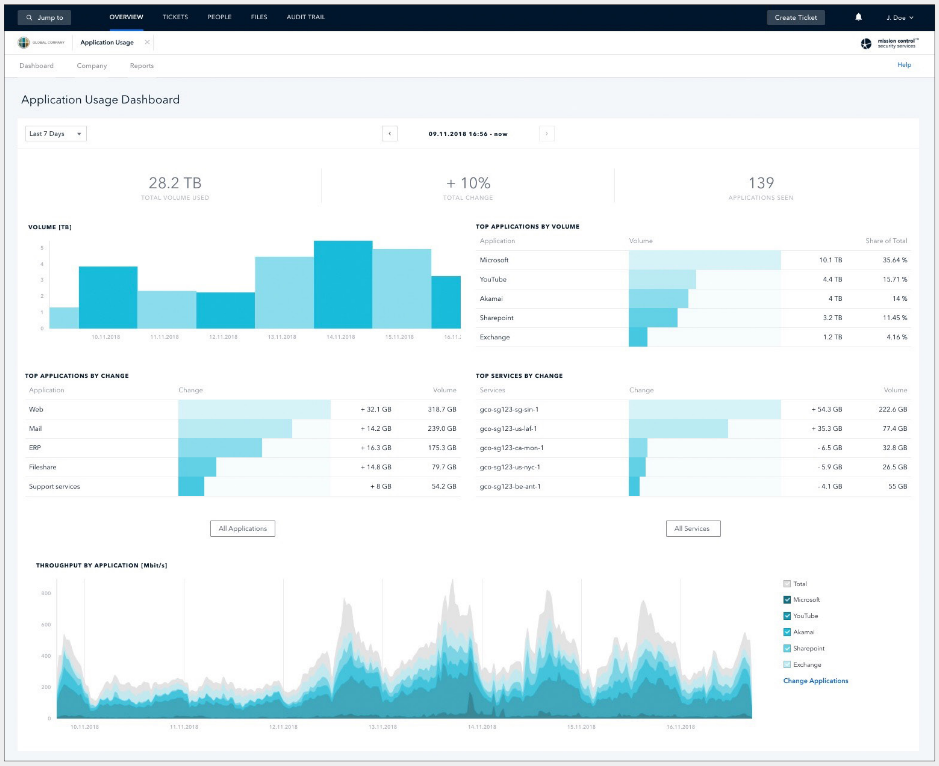
We use data correlation, analytics, alerting, and tuning

Pulling data from the Next-Gen Firewall, Secure Web Gateway, and from dedicated, strategically placed sensors within the network, the Network Security Monitoring system correlates log data to match event signatures by type, behavior, and historical rating, and assigns a running threat level to all internal assets. Highly trained engineers cut through the typical «noise» of the network by reviewing any suspicious events and continuously tuning the correlation process, in effect teaching the system to be better and better in its analysis. Any serious events are escalated to the customer to begin a response.

To give one example of this: for a large customer recently, during a single month of operations, the Open Systems Secure SD-WAN processed 800 TB of data while monitoring 26,000 clients. Just 5 events were ultimately escalated to the customer.

Open Systems Customer Portal

Get high-level views of your security situation in real-time, and drill down for specific information on any host, application, or key value.



Application Usage Dashboard

28.2 TB
TOTAL VOLUME USED

+ 10%
TOTAL CHANGE

139
APPLICATIONS SEEN

TOP APPLICATIONS BY VOLUME

Application	Volume	Share of Total
Microsoft	10.1 TB	35.64 %
YouTube	4.4 TB	15.71 %
Akamai	4 TB	14 %
Sharepoint	3.2 TB	11.45 %
Exchange	1.2 TB	4.16 %

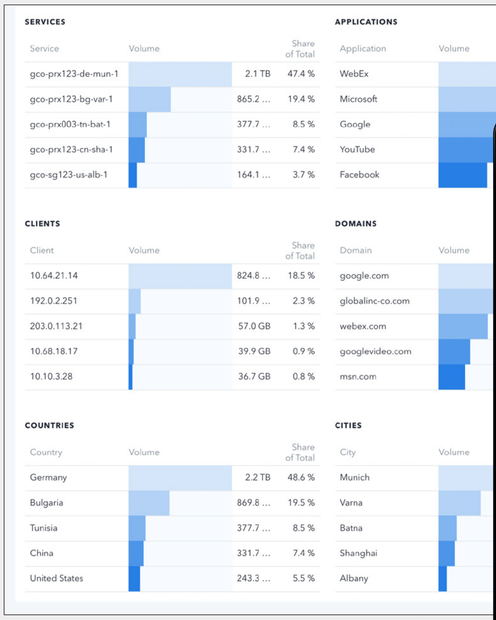
TOP APPLICATIONS BY CHANGE

Application	Change	Volume
Web	+ 32.1 GB	318.7 GB
Mail	+ 14.2 GB	239.0 GB
ERP	+ 16.3 GB	175.3 GB
Fileshare	+ 14.8 GB	79.7 GB
Support services	+ 8 GB	54.2 GB

TOP SERVICES BY CHANGE

Services	Change	Volume
gco-sg123-sg-sin-1	+ 54.3 GB	222.6 GB
gco-sg123-us-laf-1	+ 35.3 GB	77.4 GB
gco-sg123-ca-mon-1	- 6.5 GB	32.8 GB
gco-sg123-us-nyc-1	- 5.9 GB	26.5 GB
gco-sg123-be-ant-1	- 4.1 GB	55 GB

Next-Gen Firewall
Complete overview of global application traffic



SERVICES

Service	Volume	Share of Total
gco-prx123-de-mun-1	2.1 TB	47.4 %
gco-prx123-bg-var-1	865.2 …	19.4 %
gco-prx003-tn-bat-1	377.7 …	8.5 %
gco-prx123-cn-sha-1	331.7 …	7.4 %
gco-sg123-us-alb-1	164.1 …	3.7 %

APPLICATIONS

Application	Volume	Share of Total
WebEx	400.2 …	9.0 %
Microsoft	345.4 …	7.7 %
Google		
YouTube		
Facebook		

CLIENTS

Client	Volume	Share of Total
10.64.21.14	824.8 …	18.5 %
192.0.2.251	101.9 …	2.3 %
203.0.113.21	57.0 GB	1.3 %
10.68.18.17	39.9 GB	0.9 %
10.10.3.28	36.7 GB	0.8 %

DOMAINS

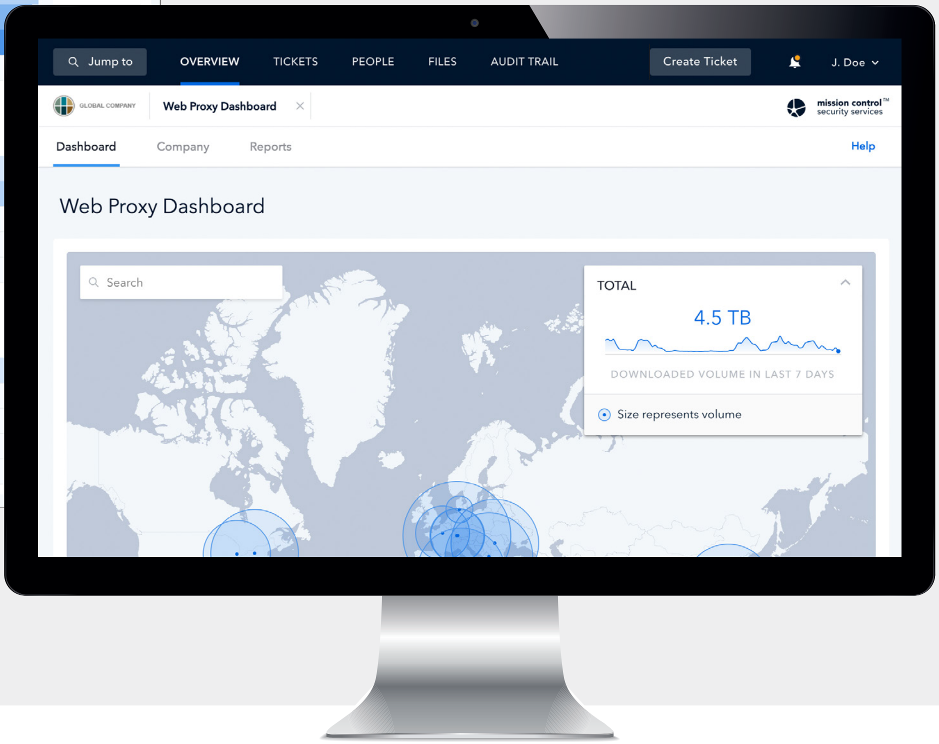
Domain	Volume
google.com	
globalinc-co.com	
webex.com	
googlevideo.com	
msn.com	

COUNTRIES

Country	Volume	Share of Total
Germany	2.2 TB	48.6 %
Bulgaria	869.8 …	19.5 %
Tunisia	377.7 …	8.5 %
China	331.7 …	7.4 %
United States	243.3 …	5.5 %

CITIES

City	Volume
Munich	
Varna	
Batna	
Shanghai	
Albany	

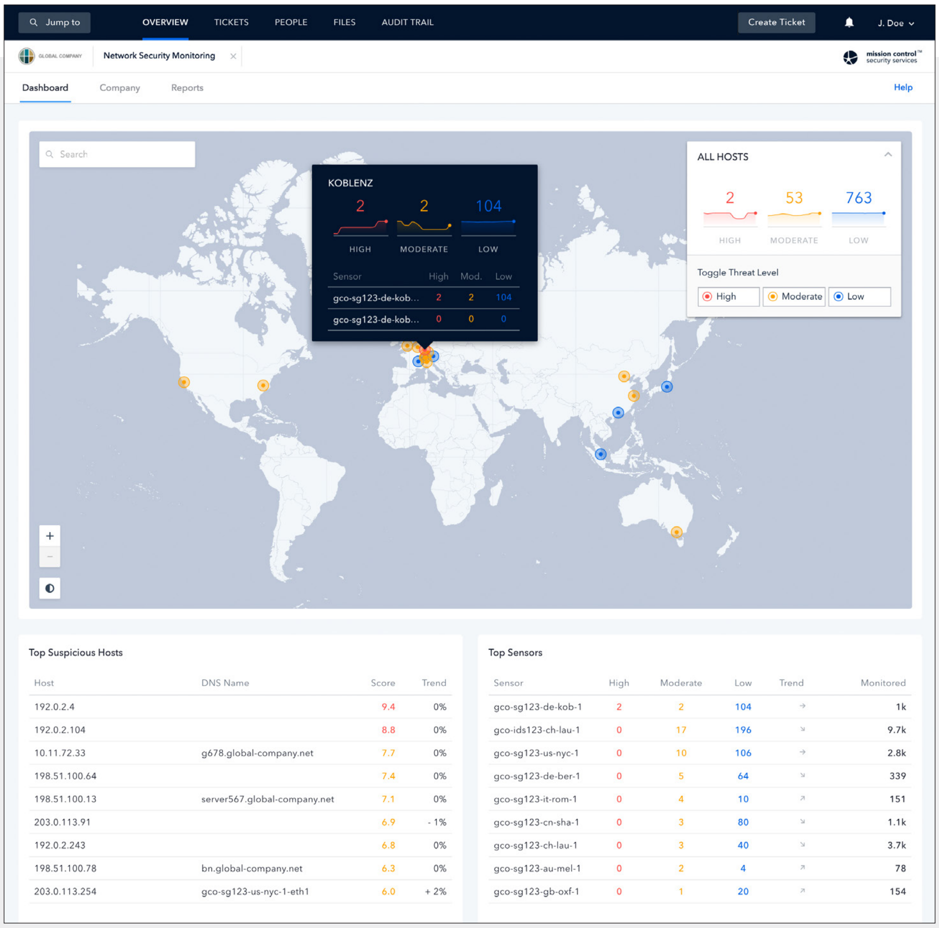


Web Proxy Dashboard

TOTAL
4.5 TB
DOWNLOADED VOLUME IN LAST 7 DAYS
◉ Size represents volume

Secure Web Gateway
Global overview of operational information, in this case throughput. Complete overview of global web traffic with drill-down capabilities

open systems



KOBLENZ

2	2	104
HIGH	MODERATE	LOW

Sensor	High	Mod.	Low
gco-sg123-de-kob...	2	2	104
gco-sg123-de-kob...	0	0	0

Top Suspicious Hosts

Host	DNS Name	Score	Trend
192.0.2.4		9.4	0%
192.0.2.104		8.8	0%
10.11.72.33	g678.global-company.net	7.7	0%
198.51.100.64		7.4	0%
198.51.100.13	server567.global-company.net	7.1	0%
203.0.113.91		6.9	- 1%
192.0.2.243		6.8	0%
198.51.100.78	bn.global-company.net	6.3	0%
203.0.113.254	gco-sg123-us-nyc-1-eth1	6.0	+ 2%

Top Sensors

Sensor	High	Moderate	Low	Trend	Monitored
gco-sg123-de-kob-1	2	2	104	→	1k
gco-ids123-ch-lau-1	0	17	196	↘	9.7k
gco-sg123-us-nyc-1	0	10	106	→	2.8k
gco-sg123-de-ber-1	0	5	64	↘	339
gco-sg123-it-rom-1	0	4	10	↗	151
gco-sg123-cn-sha-1	0	3	80	↘	1.1k
gco-sg123-ch-lau-1	0	3	40	↘	3.7k
gco-sg123-au-mel-1	0	2	4	↗	78
gco-sg123-gb-oxf-1	0	1	20	↗	154

Network Security Monitoring
Global threat overview with all assets categorized by threat score

You’re known by the company you keep. Meet just a few of our customers.

gategroup™ UBS Chemours™ Swiss Re

Open Systems is a leading global provider of a secure SD-WAN that enables enterprises to grow without compromise. With assured security, AI-assisted automation and expert management that free valuable IT resources, Open Systems delivers the visibility, flexibility and control you really want with the performance, simplicity and security you absolutely need in your network.

To learn more, visit **open-systems.com** Follow us