Executive Report - JohnnyLab

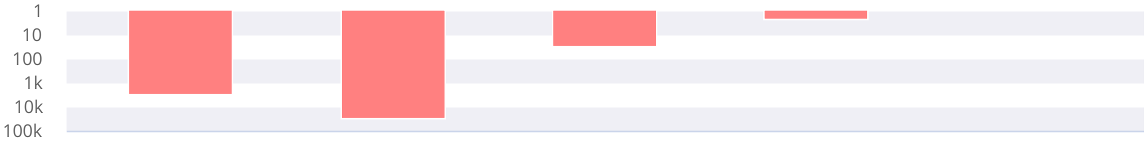
Network Activity August 2023

Aug 1, 2023 - Aug 31, 2023

ADVANCED SECURITY FLOW

REQUESTS PROCESSED

CLOUD FIREWALL	THREAT PROTECTION	ISOLATION	CONTENT ANALYSIS	SANDBOX
3010 requests scanned	**12.6 M** requests scanned		**14909** requests scanned	**0** requests scanned
3010 blocked	**27762** blocked	**28** isolated	**2** blocked	**0** threats detected

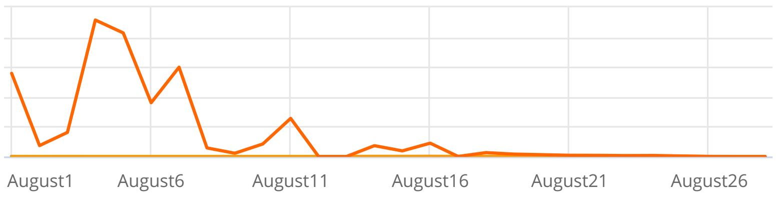


REQUESTS PROCESSED

CHANGE FROM PREVIOUS PERIOD

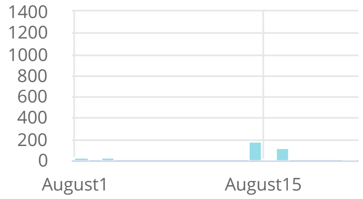
●	Content Analysis	▼	--80.0%
●	Firewall	▼	--33.0%
●	Isolation	▲	+7.0%
●	Sand Box	▲	+0.0%
●	Threat Protection	▲	+361.0%

TREND

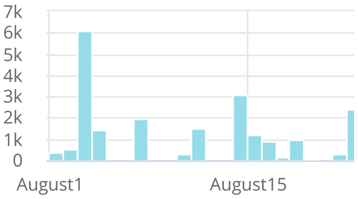


REQUESTS BLOCKED

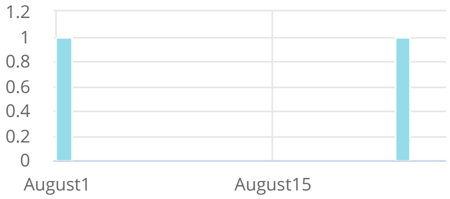
FIREWALL ▼33.362851450077486%



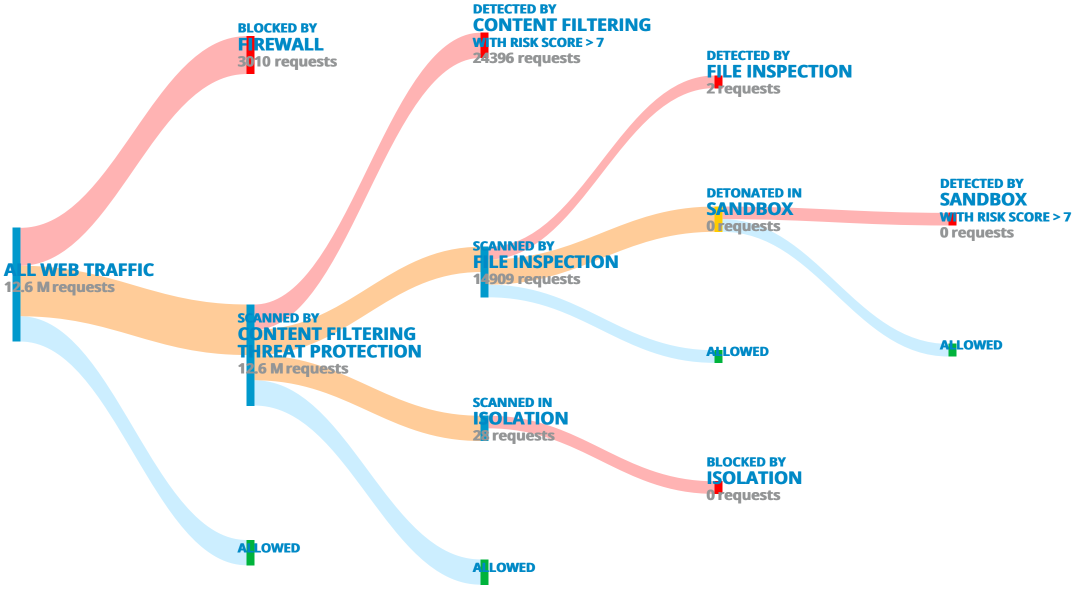
THREAT PROTECTION ▲12.569945665396157%



CONTENT ANALYSIS ▲0.0%



BLOCKED BY ADVANCED SECURITY FLOW



BLOCKED BY FIREWALL

TOP 5	BLOCKED REQUESTS

DETECTED BY FILE INSPECTION IN CONTENT ANALYSIS

TOP 5	BLOCKED INSTANCES
Blacklisted file	2

DETONATED IN SANDBOX WITH RISK SCORE >7

TOP 5	REQUESTS

SENT TO ISOLATION

TOP 5	BLOCKED REQUESTS
sadmin@bcm-demo136.com	26
ssedemo@bcm-demo136.com	2

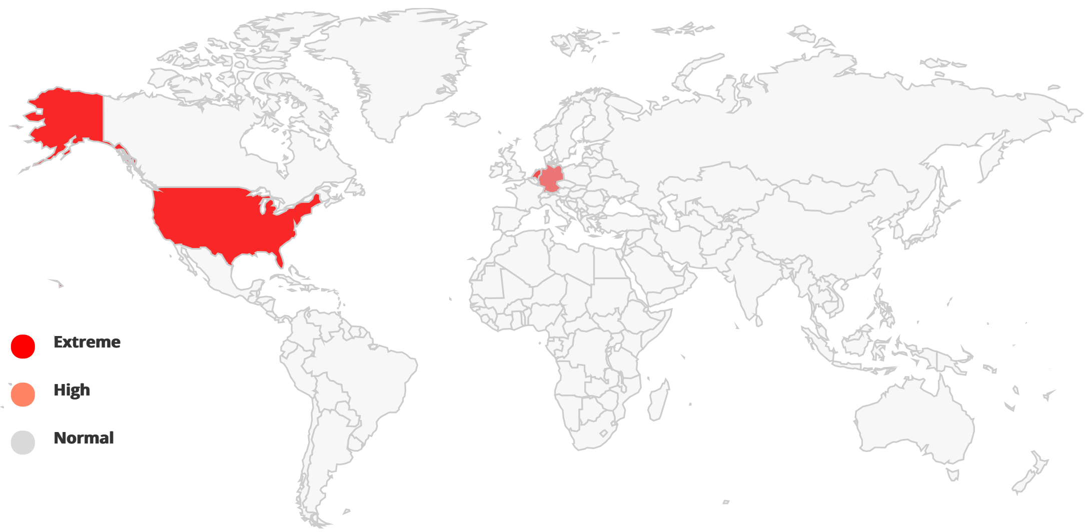
DETECTED BY CONTENT FILTERING WITH THREAT PROTECTION

TOP 5	BLOCKED INSTANCES
johnny	6425
guest1	1077
sadmin@bcm-demo136.com	1

USERS BLOCKED BY ADVANCED SECURITY FLOW

TOP 5	BLOCKED REQUESTS
sadmin@bcm-demo136.com	8906
guest1	7389
johnny	7240
ssedemo@bcm-demo136.com	335

THREATS BLOCKED BY COUNTRY



HIGHEST RISK GEO
BLOCKED BY RISK SCORE

top blocked destination:

Russian Federation

100% of all traffic to that geo with a risk score of **7+**

HIGHEST RISK GEO
BLOCKED BY RATIO

top blocked destination:

Singapore

43% of all traffic blocked

HIGHEST RISK GEO
BLOCKED BY USER RATIO

top blocked destination:

-

100% of all users attempting to access this geo blocked

RISK SCORE 9+

TOP 5	BLOCKED REQUESTS
Russian Federation	1
Netherlands	1

MALICIOUS TRAFFIC

TOP 5	SHARE
Russian Federation	0%
Netherlands	0%

ALL BLOCKED TRAFFIC

TOP 5	SHARE
Singapore	46%
United States	0%
Russian Federation	0%
Netherlands	0%

RISK SCORE 7+

TOP 5	BLOCKED REQUESTS
United States	1
Russian Federation	1
Netherlands	1

SUSPICIOUS TRAFFIC

TOP 5	SHARE

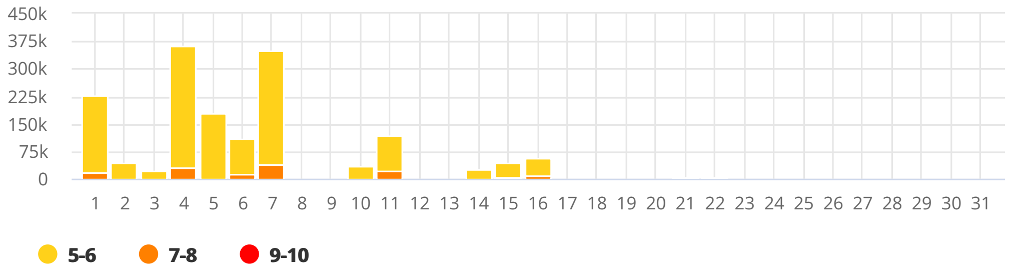
ALL DESTINATION IP'S BLOCKED

TOP 5	SHARE
20.197.71.89	16%
20.198.162.76	15%
20.198.162.78	15%
172.253.118.188	0%

RISK LEVEL BY DAY

Risk Level By Day

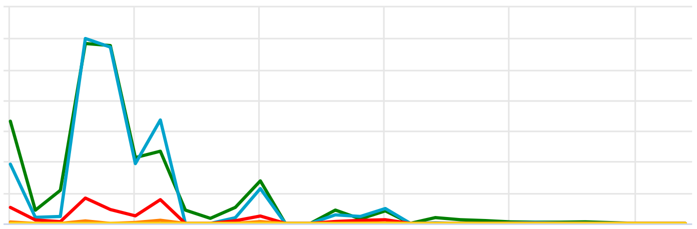
Look for unusual spikes in traffic



CHANGE FROM PREVIOUS PERIOD

🟢	1 2	▲	+409.0%
🔵	3 4	▲	+1591.0%
🟡	5 6	▲	+1502.0%
🟠	7 8	▲	+1277.0%
🔴	9 10	▼	--46.0%

3 MONTH TREND



MALWARE ANALYSIS ADVANCED TOP THREATS

NAME	REQUESTS	SHARE	CHANGE

BLOCKED BY CLOUD FIREWALL

NAME	REQUESTS	SHARE	CHANGE
112.106.161.138	390	12%	▼ -169%
52.148.114.188	285	9%	▼ -69%
129.6.15.28	257	8%	▼ -58%
129.6.15.29	254	8%	▼ -58%
129.6.15.30	189	6%	100%

ISOLATED CATEGORIES BY BANDWIDTH

NAME	BYTES	SHARE	CHANGE
Technology/Internet	2.2 M	91%	50%
Mixed Content/Potentially Adult	88504	3%	100%
Audio/Video Clips	88504	3%	100%
Gambling	21409	0%	100%

TOP ISOLATED USERS

NAME	REQUESTS	SHARE	CHANGE
sadmin@bcm-demo136.com	26	92%	0%
ssedemo@bcm-demo136.com	2	7%	100%

SYMANTEC SECURITY SERVICES

Your Services

Symantec's software adapts to your changing security needs. To further secure your company, you may wish to see additional or deeper insights about your network traffic. Contact us if you'd like to explore new options.

Cloud Secure Web Gateway	Your business' web and cloud application access policies are being enforced and your environment is being protected from web and network-based threats.
Malware Analysis Advanced	Includes file based malware detection technologies. It includes static detection methods including heuristic analysis and emulation and cloud-delivered sandbox to identify and block advanced zero-day attacks.
Intelligent Services Advanced	Your business has access to important URL-specific Threat Risk Levels, geographic hosting data and application controls which can be used to fine tune web access and threat prevention policies.
Hosted Reporting	Your business is hosting its secure web gateway logs in the cloud and benefiting from a unified view of the web activity of all users across all Symantec Secure Web Gateway products and services.
Selective Web Isolation	Your business is using Selective Web Isolation to protect your organization from advanced threats targeting your end user's web browsers and email applications from risky sites.

More Services Available

To activate additional services contact your account rep.

Full Web Isolation	Your business has not activated Full Web Isolation. This service is required to protect your organization from advanced threats targeting your end user's web browsers and email applications. Without Isolation, your business is exposed to these types of attacks.
High Risk Isolation	Your business has not activated High Risk Isolation. This service is required to protect your organization from advanced threats targeting your end user's web browsers and email applications. Without Isolation, your business is exposed to these types of attacks from risky sites.
Cloud DLP	Your business has not activated Data Loss Prevention (DLP). This service helps prevent data loss and enforces data compliance and information security policies.
Mobile Device Security	Your business is not using SEP to route mobile and laptop traffic to the Cloud Secure Web Gateway. If you are running endpoint protection on your devices, converting to Symantec will eliminate the need for a separate endpoint agent to route traffic to Cloud SWG. One less agent to install and manage simplifies device management for your IT team.
Cloud Firewall	Your business does not have Cloud Firewall Service. This service provides next-generation firewall capabilities and extends network security beyond the standard web ports (80/443). CFS enables you to define firewall policies to control all TCP or UDP traffic based on IP addresses, destination ports, locations, users, and groups.