cisco Secure

Cisco Cloud Security TechClub

Milan Habrcetl a Jiří Tesař, Cisco CyberSecurity team

16th November, 2021

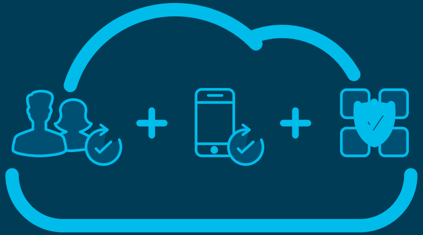
Dnešní agenda - Cisco Cloud Security

Security when accessing the cloud

Cisco Umbrella

Secure Internet Gateway (SIG)

Security for accessing any app



Cisco Secure Access by Duo

Multi-Factor Authentication (MFA),
Single Sign-on (SSO),
Software-Defined Perimeter (SDP)

Security for public cloud

Cisco Secure Cloud Analytics

Public cloud visibility
and threat detection

Security for endpoint

Cisco Secure Endpoint + SecureX

Endpoint protection and XDR
backended from cloud

CISCO SECURE

The bridge to possible

Cisco Umbrella

Co je Secure Internet Gateway?

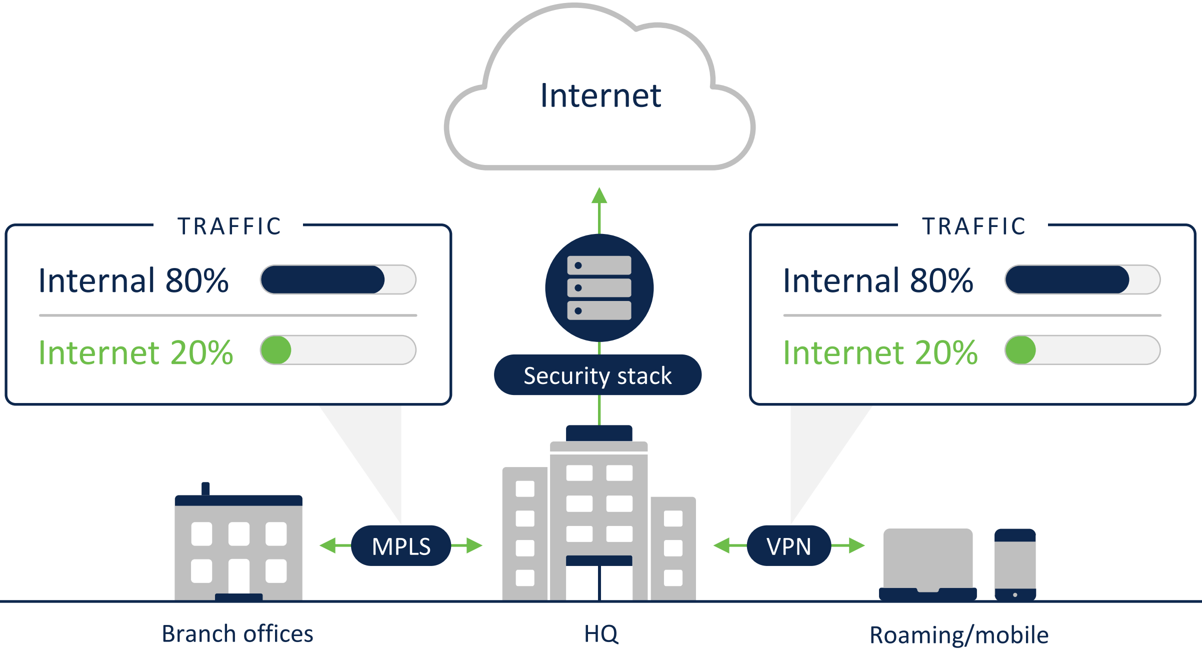
Milan Habrcetl

Historic traffic flows

Led to the age of perimeter-based security and networking

Network:
Centralized

Security:
Single, on-premise security stack

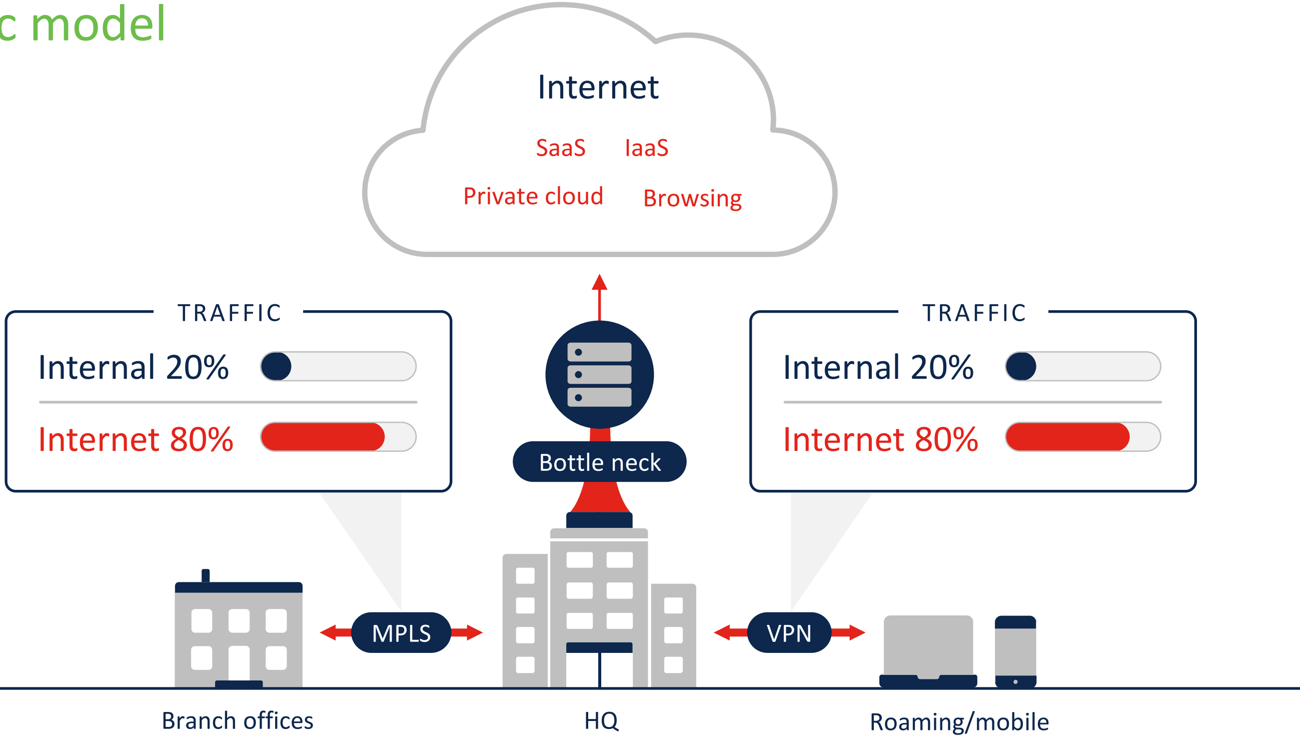


Changes in the types of traffic and destinations

Have inverted the traffic model

Problems:

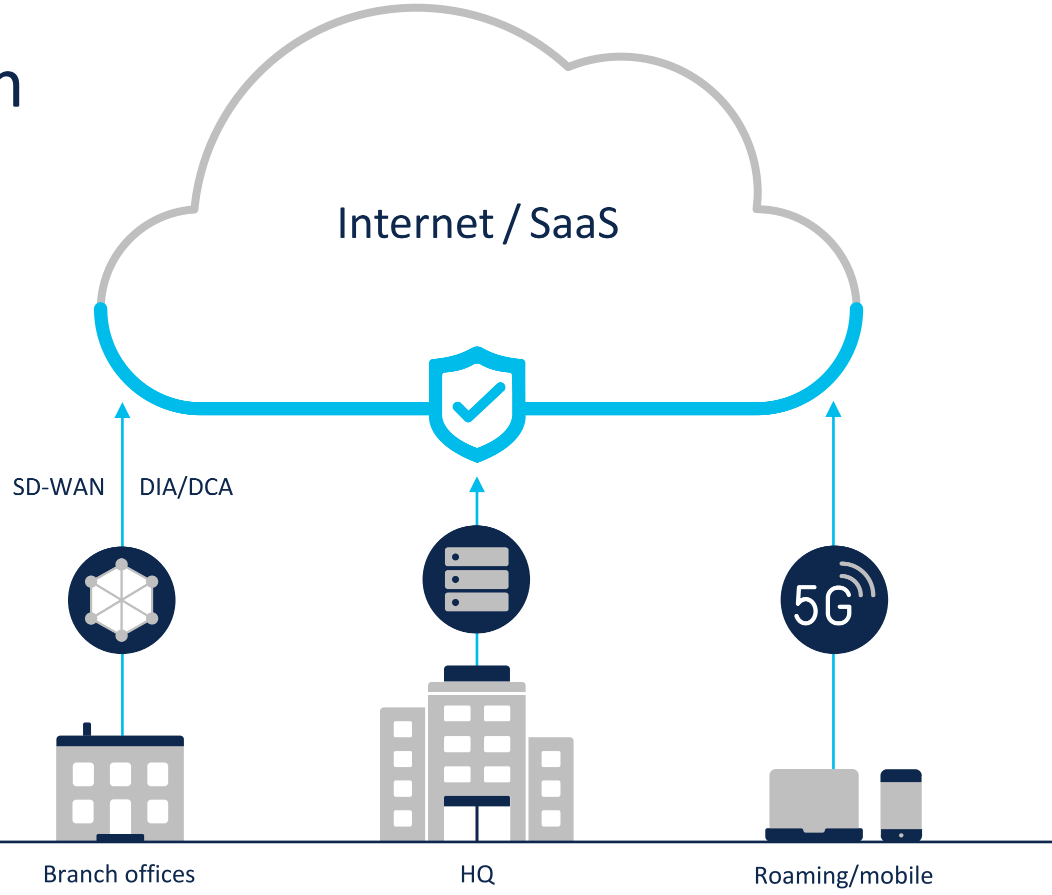
- Costs
- Performance
- # Tools/vendors
- Integrations
- Maintenance



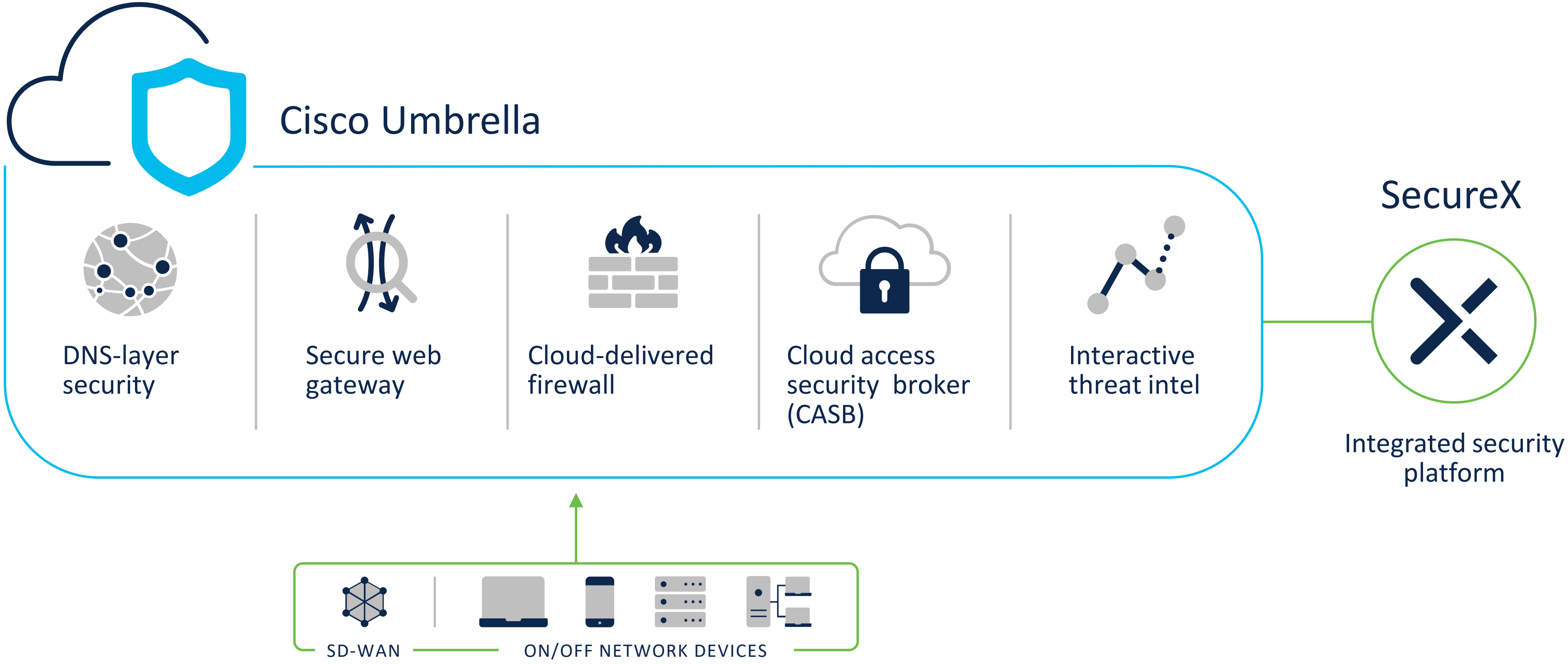
A more modern approach

Security:
Enforced at the cloud edge

Network:
Optimized routing from anywhere to the cloud



The Umbrella multi-function security solution



Cisco Umbrella

DNS-layer security

Secure web gateway

Cloud-delivered firewall

Cloud access security broker (CASB)

Interactive threat intel

SecureX

Integrated security platform

SD-WAN

ON/OFF NETWORK DEVICES

Cisco Umbrella: key capabilities

Secure onramp to the internet, everywhere

Visibility

- On & off corporate network
- All internet & web traffic
- All apps
- All devices
- SSL decryption
- Shadow IT

Protection

- DNS-layer security
- Web inspection
- File inspection
- Threat intel access
- Sandboxing
- Non-web traffic inspection

Control

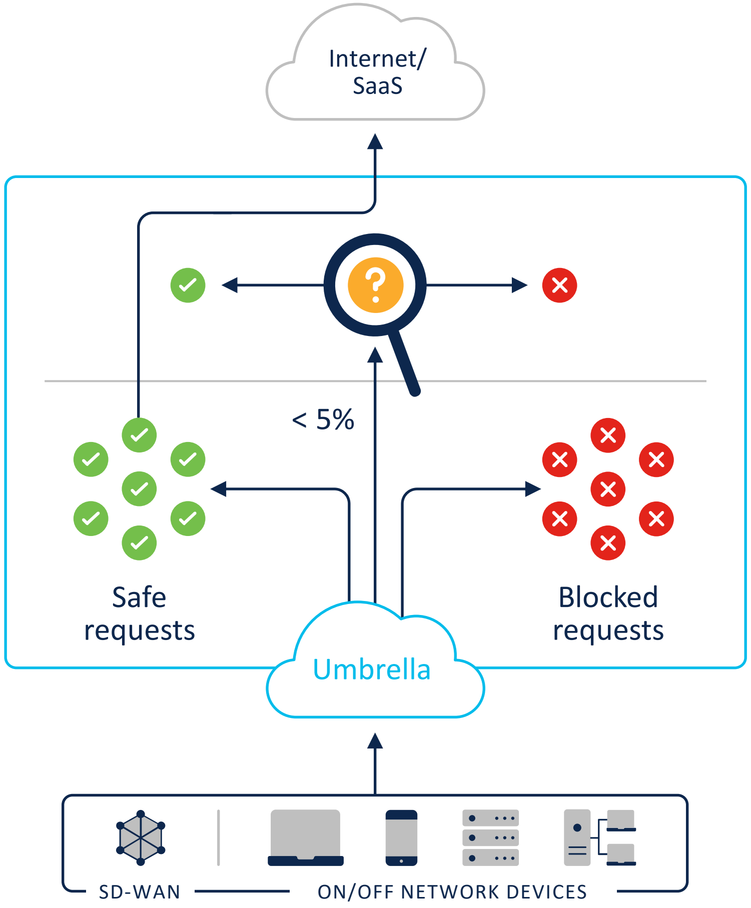
- URL block/allow lists
- Port & protocol rules
- Granular app controls
- Content filtering
- App blocking
- Tenant controls

Built-in platform with Cisco SecureX and threat intelligence by Cisco Talos

DNS-layer security

First line of defense

- Deploy enterprise wide in minutes
- Block domains associated with malware, phishing, command and control callbacks anywhere
- Stop threats at the earliest point and contain malware if already inside
- Accelerate threat response with an integrated security platform
- Amazing user experience — faster internet access; only proxy risky domains



Secure web gateway: full web proxy

Deep inspection and control of web traffic

- Gain additional visibility via full URL logging and cloud app discovery
- Enforce acceptable use policy via app controls, content filtering, and URL block/allow lists

Full web proxy

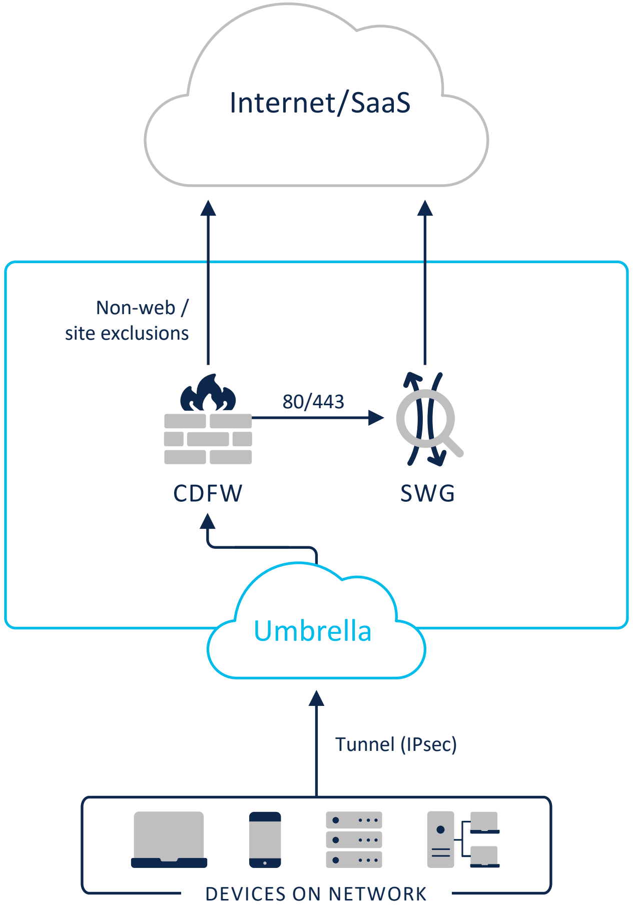
- Extend protection against malware via SSL decryption and file inspection
- Enrich file inspection (with retrospective alerts) via malware defense and analytics

CISCO SECURE

Cloud-delivered firewall

Firewall for the cloud edge

- Tunnel all outbound traffic to Umbrella
- Block high risk, non-web applications
- Centrally manage IP, port, protocol and application rules (layer 3, 4, and 7)
- Forward web traffic (ports 80/443) to secure web gateway
- IPsec tunnel termination



Enforcement that works together

Improved responsiveness and performance

1. DNS-layer security

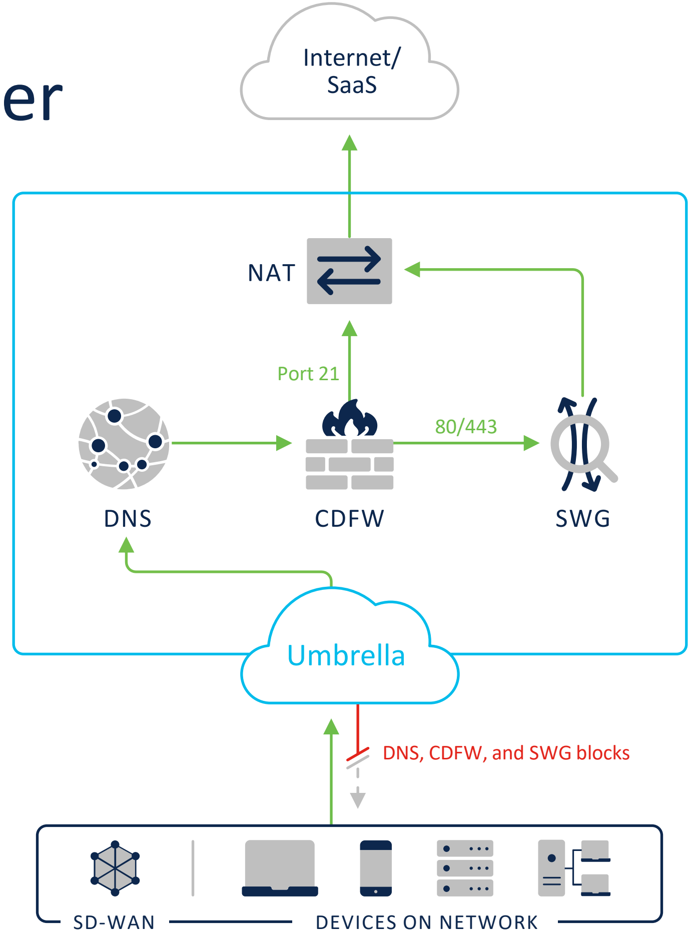
   First check for domains associated with malware

2. Cloud-delivered firewall (CDFW)

   Next check for IP, port, protocol and application rules

3. Secure web gateway (SWG)

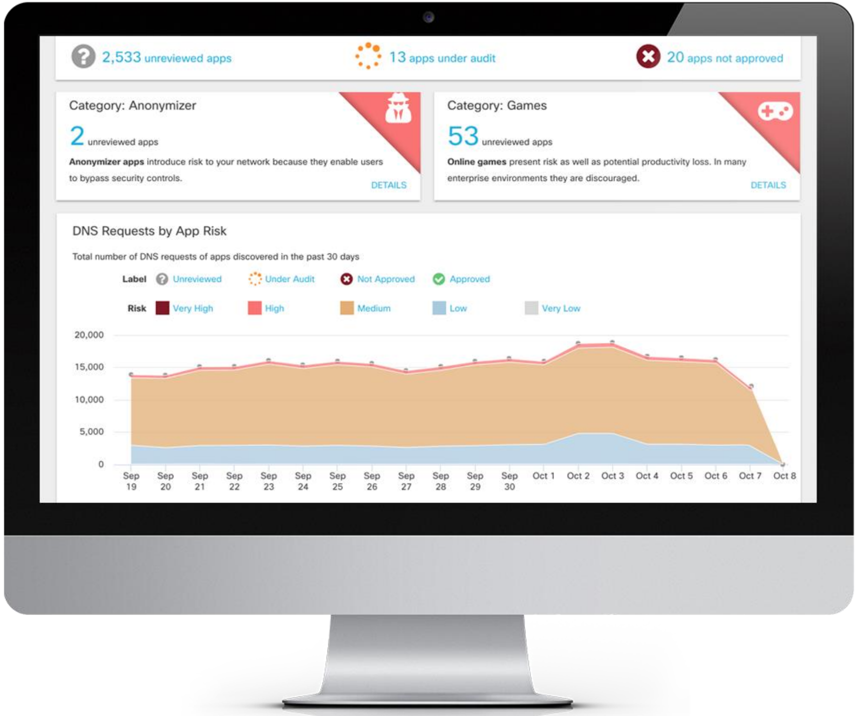
   Final check of all web traffic for malware and policy violations



CASB functionality

Visibility control and protection

- A dashboard that highlights risky apps and activity trends
- Deeper visibility into cloud app usage
- Content and app control including specific app/URL block or allow policies
- Activity controls for popular SaaS apps (uploads/attachments/post/share)
- SecureX unifies visibility of security metrics related to cloud app usage
- Cloud malware detection for data at rest in core SaaS apps



2,533 unreviewed apps

13 apps under audit

20 apps not approved

Category: Anonymizer

2 unreviewed apps

Anonymizer apps introduce risk to your network because they enable users to bypass security controls.

Category: Games

53 unreviewed apps

Online games present risk as well as potential productivity loss. In many enterprise environments they are discouraged.

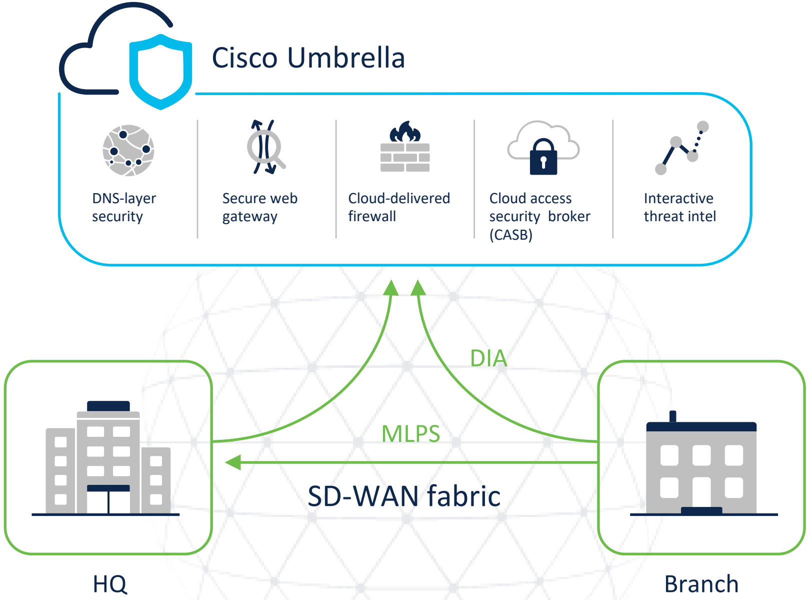
DNS Requests by App Risk

Total number of DNS requests of apps discovered in the past 30 days

Umbrella for Cisco SD-WAN

Fast forward time to value with automated security

- Hands-off automation: deploy cloud security across thousands of branches in minutes
- Top notch protection: defend against threats at the branch with the leader in security efficacy
- Simplified management: single pane of glass across all offices and users
- Deeper inspection & controls: SWG and cloud-delivered firewall with IPsec tunnels



NEW

Global cloud architecture

What's under the hood matters. A lot.

Capabilities:

- Containerized architecture for scalability and reliability
- 620 billion DNS requests per day
- 1000+ peering partners with top IXPs, CDNs, and SaaS platforms
- 6,000 peering sessions create shortcuts to major ISPs – decrease latency by 73%
- Global footprint with huge capacity
- Carrier neutral data centers that meet or exceed ISO27001/SOC2 and GDPR compliance

NEW

New AV-TEST security efficacy report!

Featuring Cisco Umbrella

- AV-TEST places Cisco Umbrella first in secure web gateway to protect remote workers
- With this new report AV-TEST places Umbrella is #1 in security efficacy — again!

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Umbrella consistently performed better than the competition!

Secure web gateway test	Umbrella	Zscaler	Palo Alto	Netskope	Akamai
Total detection rate	**96.39**	**89.67**	**73.15**	**61.90**	**58.43**

% Detected (higher is better)

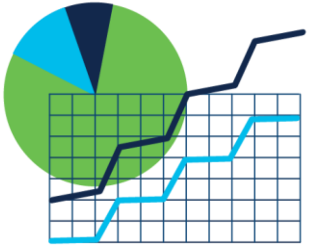
NEW

Umbrella Reporting API v2

Reimagined searching and filtering in Cisco Umbrella Reporting API v2 empowers faster information access.

Key benefits

- Gives customers access to 30+ endpoints
- Removes one-to-one matching limitation in searches
- Provides a more trusted, scalable platform for filtering and querying



Learn more

- References: docs.umbrella.com/umbrella-api/docs/reporting_api_overview
- V2 endpoints for service providers: docs.umbrella.com/umbrella-api/reference#deletepolicyidentities-2

NEW

Umbrella data loss prevention (DLP)

Overview: Umbrella data loss prevention (DLP) is a cloud-native service that leverages the Umbrella SWG proxy to analyze sensitive data in-line and provide visibility and control to sensitive data leaving your organization.

Features

- Leverage 80+ built-in content classifiers including PII, PCI, and PHI
- Customize built-in content classifiers with threshold and proximity to tune and reduce false positives
- Create user-defined dictionaries with custom phrases (such as project code names)
- Detect and report on sensitive data usage and use drill-down reports to help identify misuse
- Inspects cloud app and web traffic content and enforce data policies to protect

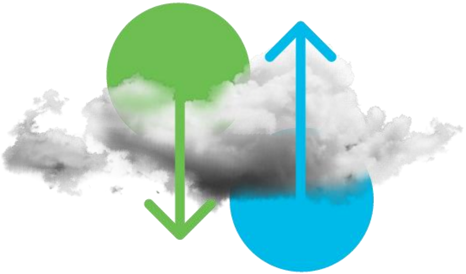
* **Current Apps Supported:** OneDrive, Box, Slack, Gmail, SharePoint and PasteBin

Benefits

- Identifies sensitive data in motion for identities, data, and select cloud applications
- Monitor and protect against data leakage

Use Cases

- Protect sensitive data from spreading outside to unwanted locations
- Maintain security compliance and security needs



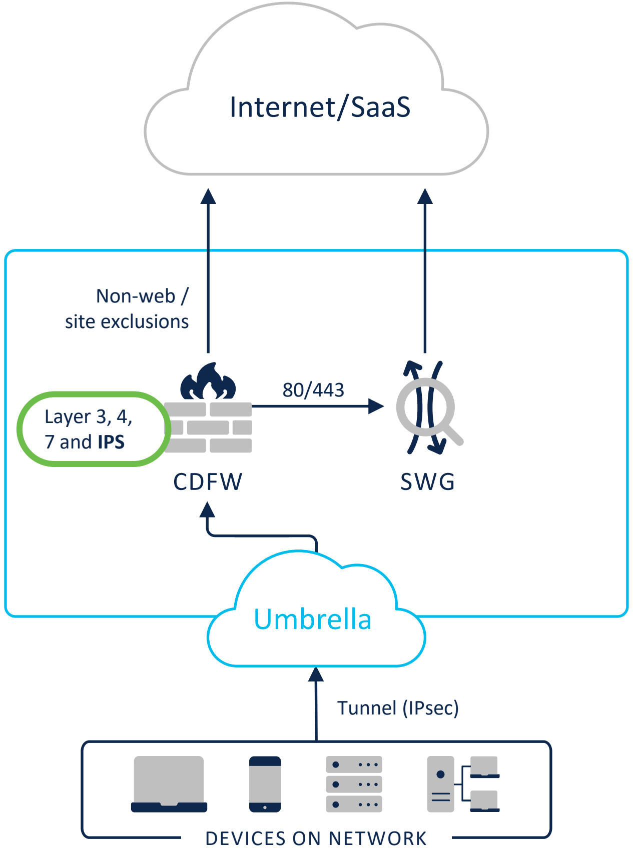
NEW

Umbrella cloud-delivered firewall IPS

Intrusion Prevention System

IPS capabilities:

- Deepen Umbrella cloud firewall protection for outbound traffic (IPS + layer 3 / 4 and 7)
- Add layer of detection/blocking for malware, botnets, phishing, and command and control callbacks
- Detect and correlate threats in real-time by comparing traffic against threat signatures
- Use 40,000+ signatures (and growing) from Cisco Talos



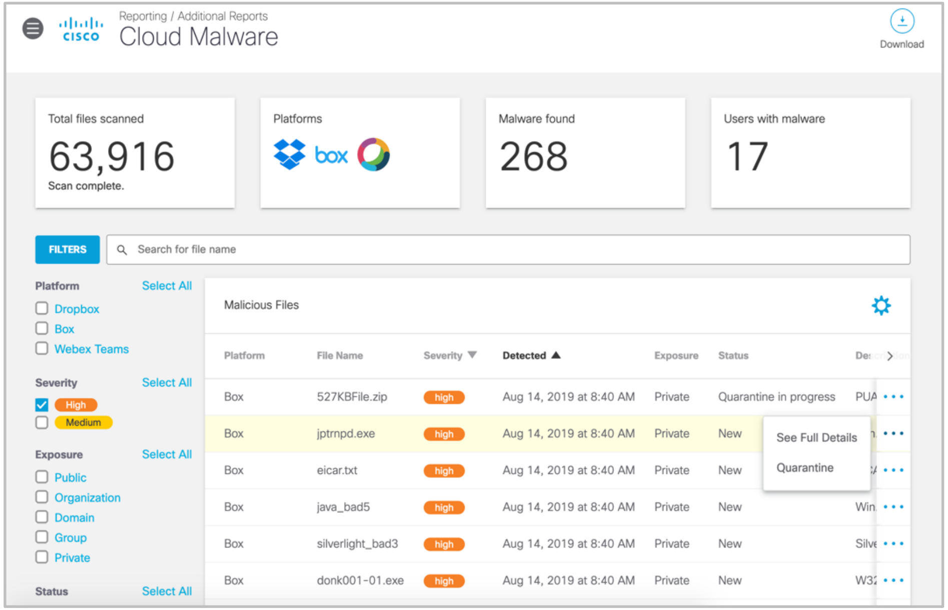
NEW

Cloud malware detection (data at rest)

Increase security for SaaS file storage apps

Features

- Scans file storage repositories
- Detects malware
- Prevent the spread of infection by deleting or quarantining malicious files



Reporting / Additional Reports

Cloud Malware

Total files scanned
63,916
Scan complete.

Platforms

Malware found
268

Users with malware
17

Platform — Select All
- □ Dropbox
- □ Box
- □ Webex Teams

Severity — Select All
- ☑ High
- □ Medium

Exposure — Select All
- □ Public
- □ Organization
- □ Domain
- □ Group
- □ Private

Status — Select All

Malicious Files

Platform	File Name	Severity ▼	Detected ▲	Exposure	Status	Des
Box	527KBFile.zip	high	Aug 14, 2019 at 8:40 AM	Private	Quarantine in progress	PUA
Box	jptrnpd.exe	high	Aug 14, 2019 at 8:40 AM	Private	New	n.
Box	eicar.txt	high	Aug 14, 2019 at 8:40 AM	Private	New	:/
Box	java_bad5	high	Aug 14, 2019 at 8:40 AM	Private	New	Win.
Box	silverlight_bad3	high	Aug 14, 2019 at 8:40 AM	Private	New	Silve
Box	donk001-01.exe	high	Aug 14, 2019 at 8:40 AM	Private	New	W32

CISCO SECURE

CISCO The bridge to possible

Cisco DUO Security

Praktická ukázka

Jiří Tesař

CISCO
SECURE

CISCO The bridge to possible

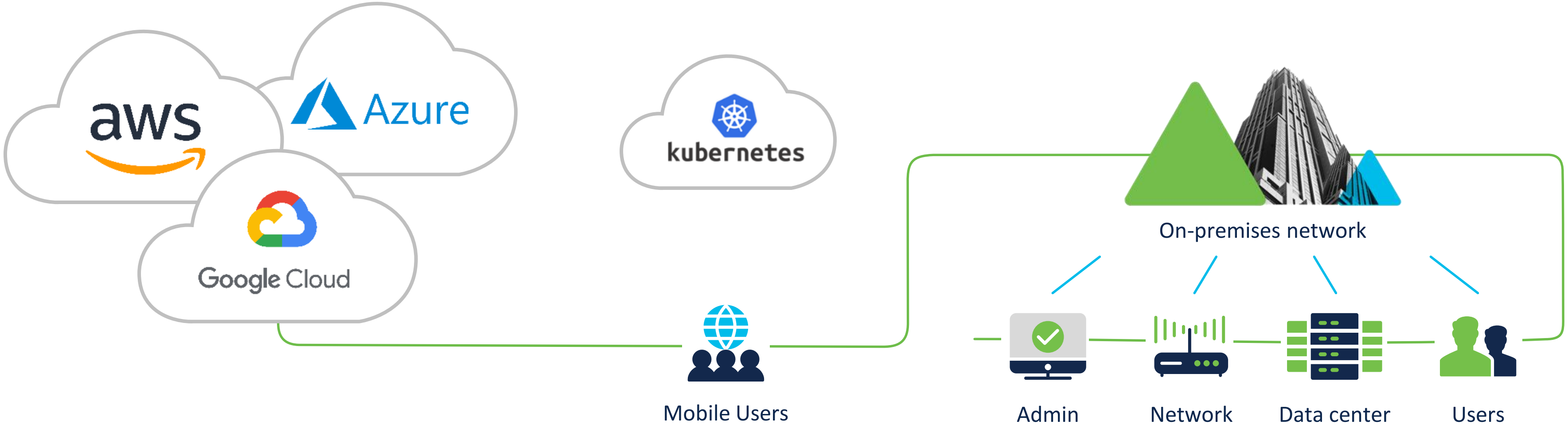
Cisco Secure Cloud Analytics

Stealthwatch cloud

Milan Habrcetl

Effective security depends on total visibility

- Know every entity
- See every conversation
- Understand what is normal
- Be alerted to change
- Respond to threats quickly

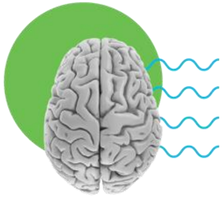


Cisco Secure Cloud Analytics

Gain confidence in your security effectiveness

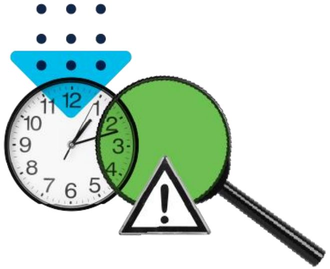
Contextual network-wide visibility

Agentless, using existing network and cloud infrastructure, even in encrypted traffic



Predictive threat analytics

Combination of behavioral modeling, machine learning and global threat intelligence



Automated detection and response

High-fidelity alerts prioritized by threat severity with ability to conduct forensic analysis

Entity modeling to baseline behavior and detect anomalies

Collect input

- IP Telemetry
- Enhanced NetFlow
- Cisco Secure Network Access user data
- DNS Snooping
- External threat intel
- Endpoint metadata
- System/Account logs

Perform analysis

Dynamic
entity modeling

Draw conclusions

Role	What is the role of the device? Is its behavior consistent with that type of role?
Group	What ports/protocols does the device continually access? Do other similar roles do the same?
Consistency	What connections does it continually make? What is the reputation of the IPs it connects to?
Rules	Does it communicate internally only? What geographies does it normally talk to?
Forecast	How much data does the device normally send/receive? Is it consistent with expectations?

cisco SECURE

Visibility and powerful analytics = high fidelity alerts

Automatic threat detection

ALERT: Anomaly detected

95% Secure Cloud Analytics
alerts rated as "helpful" by customers

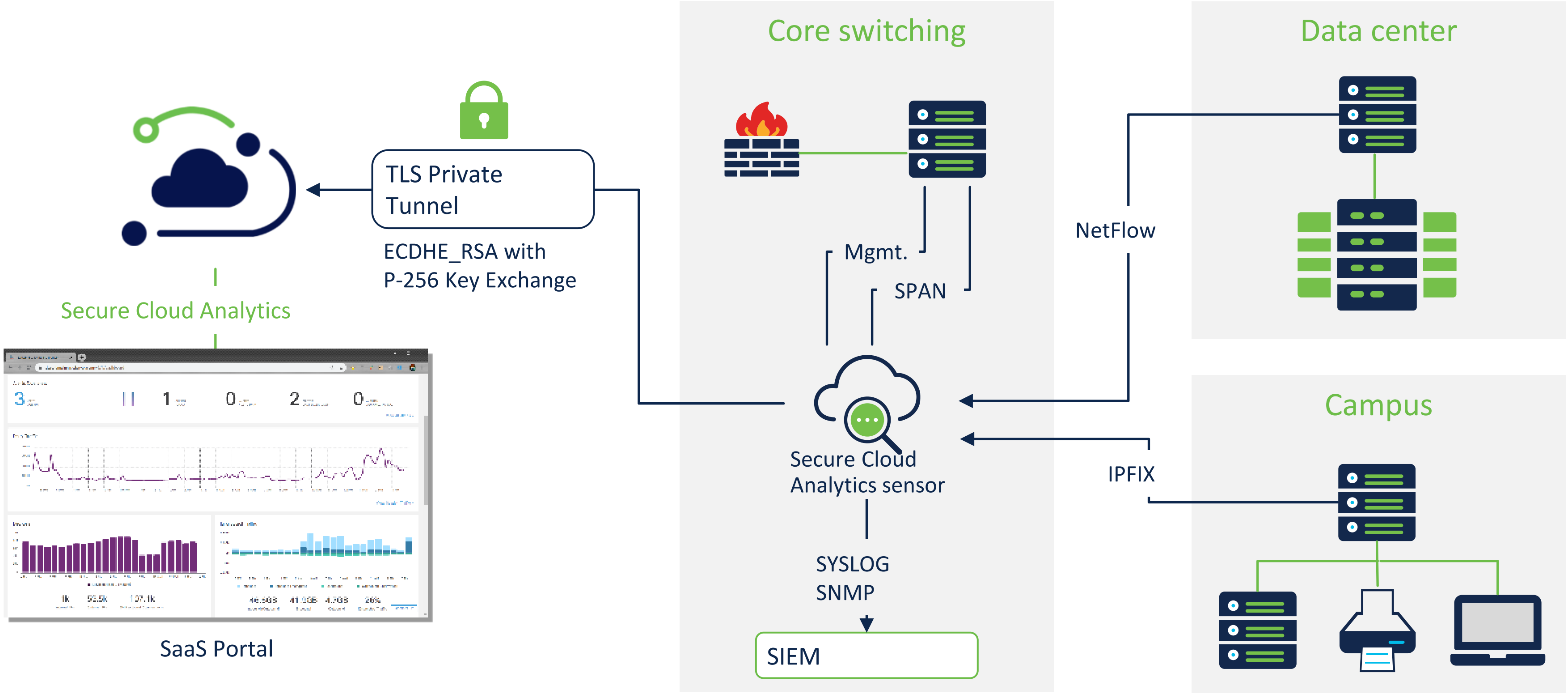
- Excessive failed access attempts
- DDoS and amplification attacks
- Potential data exfiltration
- Geographically unusual remote access
- Connection to a suspicious destination
- Custom segmentation and configuration policies

Key use cases

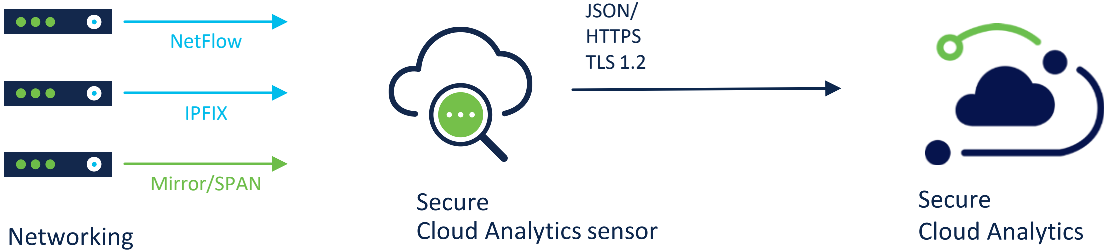
Secure
Cloud Analytics

Hybrid cloud visibility	Natively integrate with multiple infrastructures in the public and private cloud as well as on-premises to get a unified view of the entire workload framework
Entity detection and visibility	Automatically classify and monitor entities and workloads on a network
Behavioral threat detection	Detect threats using multiple mechanisms – behavioral modeling, machine learning and threat intelligence powered by Cisco Talos
Configuration risk exposure	Expose configuration risks by detecting permissive rules, aging API keys and native compliance alerts in the cloud infrastructure
Event risk visibility	Cloud event visibility and configured alerts that trigger on cloud-based system and user activities
Network segmentation	Network segmentation compliance allows for network monitoring based on user defined watchlists
Response and remediation	Native cloud remediation integration with cloud-enabled response resources such as webhooks, alert messaging and storage facilities

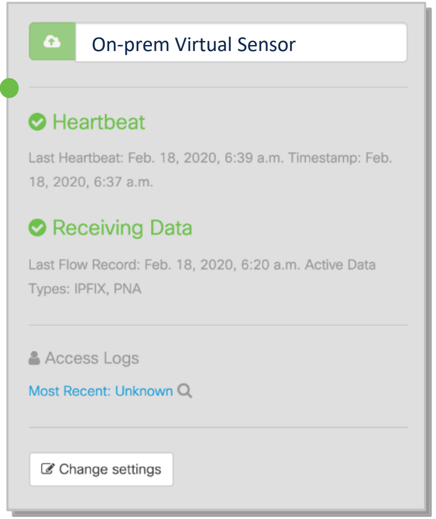
Monitoring all on-premises network areas



Secure Cloud Analytics sensor data flow



Sensor data status


On-prem Virtual Sensor

Heartbeat

Last Heartbeat: Feb. 18, 2020, 6:39 a.m. Timestamp: Feb. 18, 2020, 6:37 a.m.

Receiving Data

Last Flow Record: Feb. 18, 2020, 6:20 a.m. Active Data Types: IPFIX, PNA

Access Logs

Most Recent: Unknown

Common public cloud integration process

Enable Logging

Native flow logs can be ingested by Secure Cloud Analytics to provide network conversations

Create Access Policy

Create a policy to allow Secure Cloud Analytics to read resource information such as vm details, security groups, and configuration change logs.

Create a Role or Application with the appropriate access policy

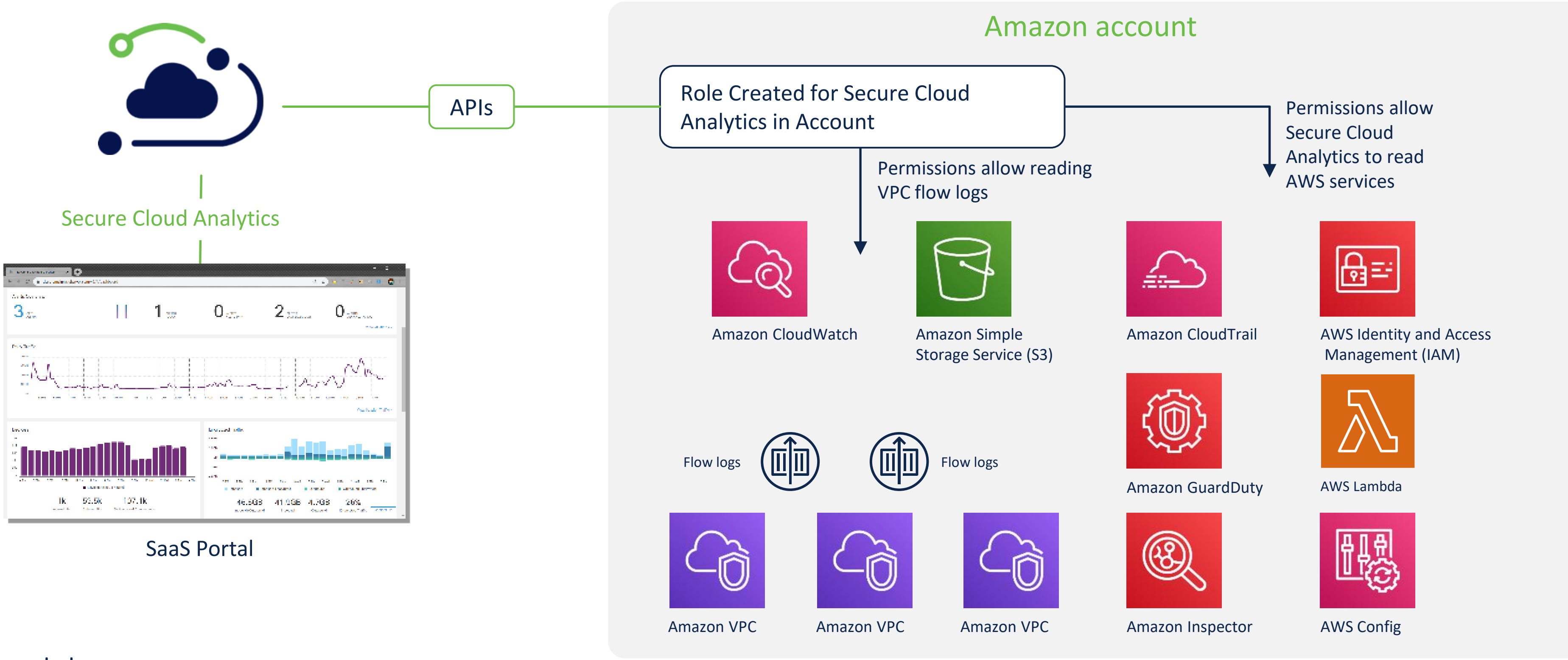
Create an IAM role or custom application that the previously created policy can be associated with.

Configure Secure Cloud Analytics

Put the appropriate access details (storage details, role) in Secure Cloud Analytics

https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/cloud/configuration/SWC_PCM_AWS_DV_1_5.pdf

Accessing telemetry for AWS deployments



Secure Cloud Analytics

APIs

SaaS Portal

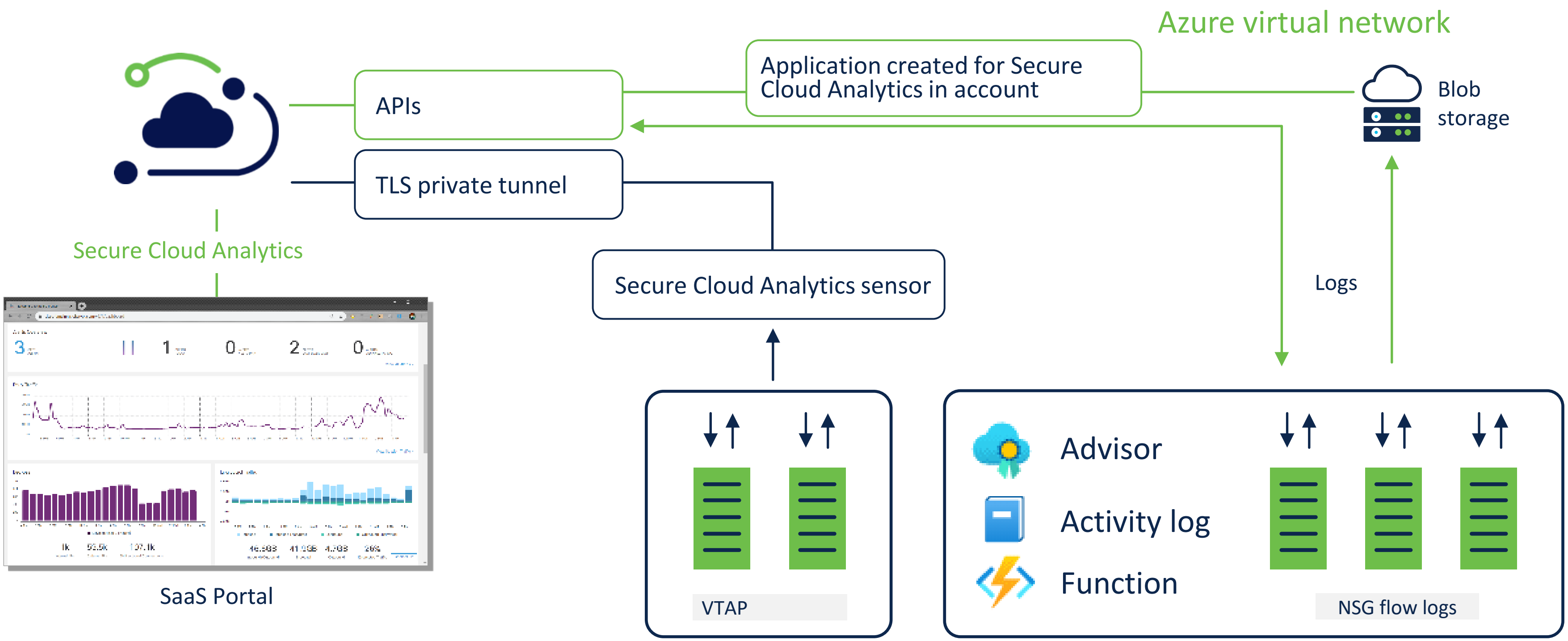
Amazon account

Role Created for Secure Cloud Analytics in Account

Permissions allow reading VPC flow logs

Permissions allow Secure Cloud Analytics to read AWS services

Accessing telemetry for Microsoft Azure



Azure virtual network

APIs

TLS private tunnel

Application created for Secure Cloud Analytics in account

Blob storage

Secure Cloud Analytics

Secure Cloud Analytics sensor

Logs

SaaS Portal

VTAP

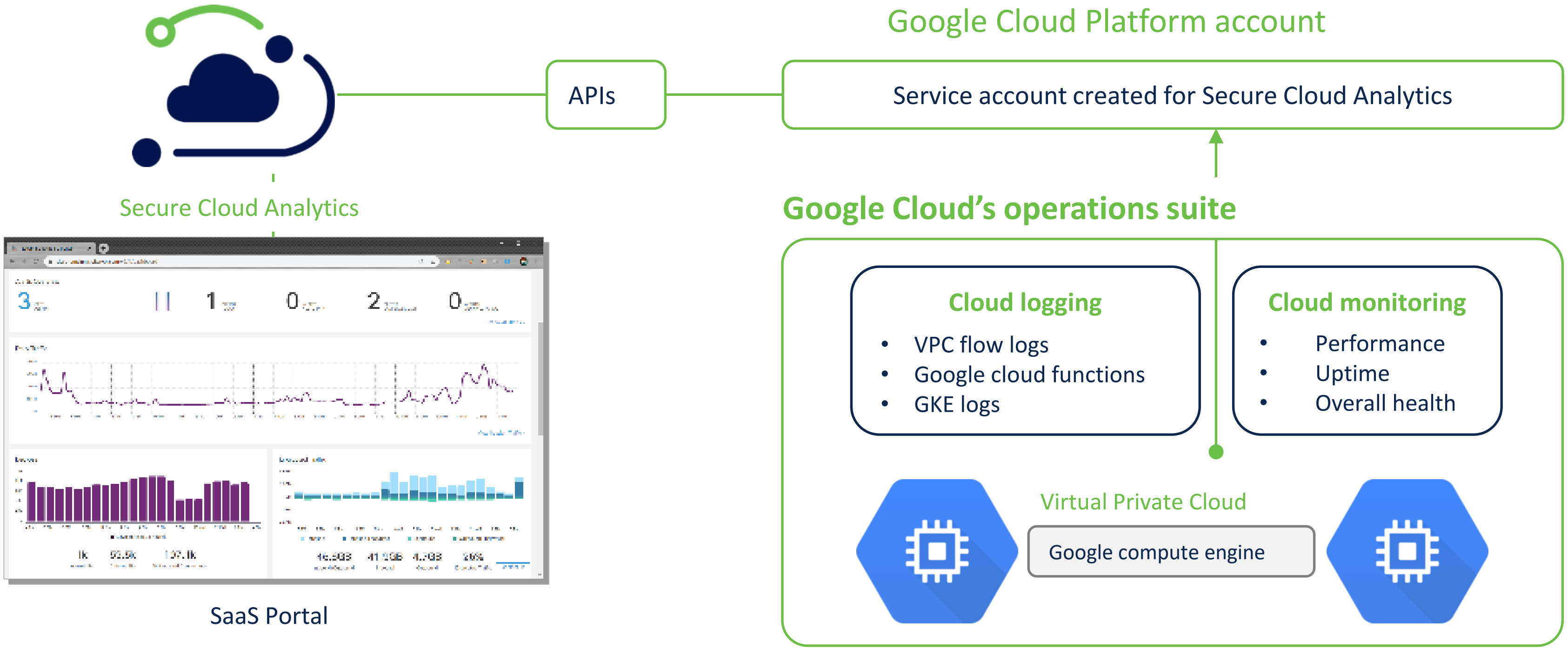
Advisor

Activity log

Function

NSG flow logs

Accessing telemetry for Google Cloud Platform



Secure Cloud Analytics

APIs

Google Cloud Platform account

Service account created for Secure Cloud Analytics

Google Cloud's operations suite

Cloud logging

- VPC flow logs
- Google cloud functions
- GKE logs

Cloud monitoring

- Performance
- Uptime
- Overall health

Virtual Private Cloud

Google compute engine

SaaS Portal

CISCO
SECURE

CISCO The bridge to possible

Cisco Secure Endpoint + SecureX

Praktická ukázka

Jiří Tesař

cisco Secure