Cisco Virtual Update on Cloud Security

Mikael Grotrian, CISSP, CISM, CCSK, GISF, ITIL, PRINCE2, TOGAF Certified

Consulting Systems Engineer, Cyber Security, Denmark

25/10 – 2017

Enable your business to see, secure, and protect with Cisco cloud security

Stealthwatch Cloud

Public Cloud Visibility

Extend visibility to public and hybrid cloud environments

Cloudlock

Cloud access security brokers (CASB)

Secure users, data, and applications in the cloud

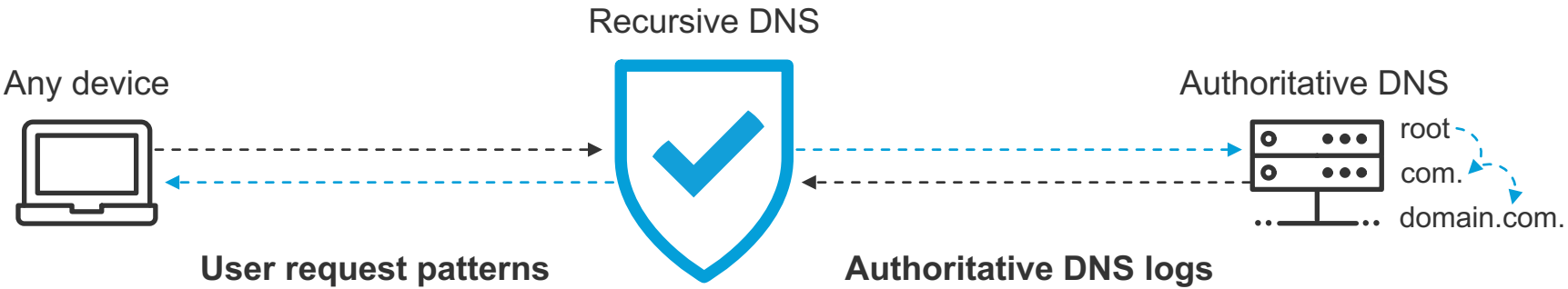
Umbrella

DNS Security

Protect users anywhere they go

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco

Gather intelligence and enforce security at the DNS layer



User request patterns

Used to detect:

- Compromised systems
- Command and control callbacks
- Malware and phishing attempts
- Algorithm-generated domains
- Domain co-occurrences
- Newly registered domains

Authoritative DNS logs

Used to find:

- Newly staged infrastructures
- Malicious domains, IPs, ASNs
- DNS hijacking
- Fast flux domains
- Related domains

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco

Built into foundation of the internet

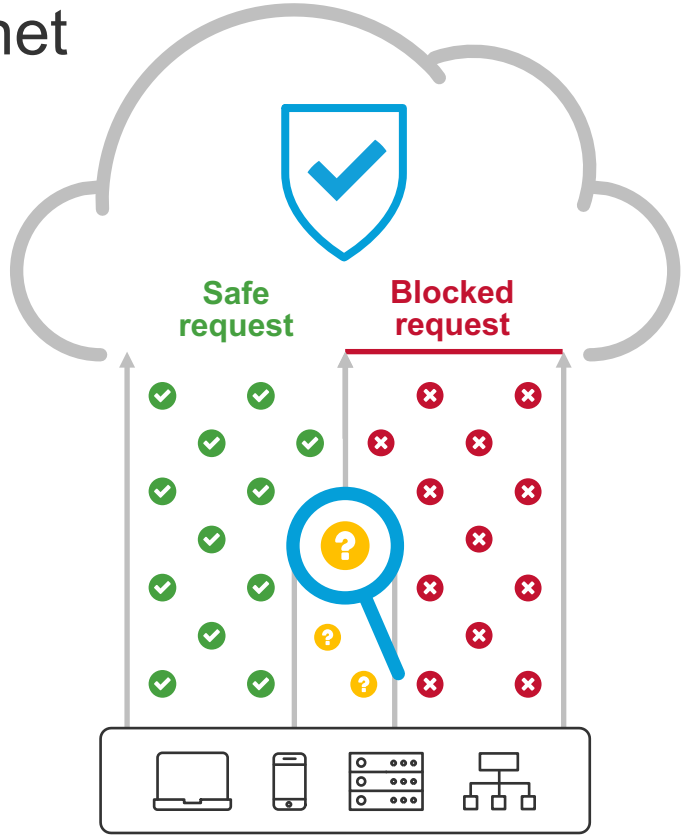
Umbrella provides:

Connection for safe requests

Prevention for user and malware-initiated connections

Proxy for:

- URL Inspection
- SSL Decryption
- AV Scan
- Advanced Malware Protection
- Threat Grid sandboxing



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco

Our view of the internet

100B
requests per day

85M
daily active users

12K
enterprise customers

160+
countries worldwide

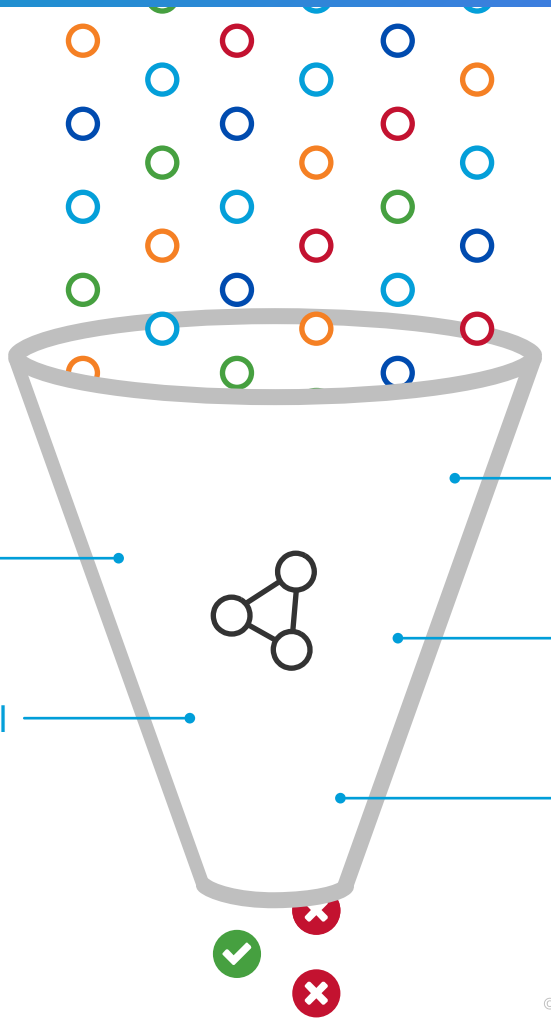
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco

Intelligence

Statistical models

2M+ live events per second

11B+ historical events



Spike rank model
Detect domains with sudden spikes in traffic

Predictive IP space monitoring
Analyzes how servers are hosted to detect future malicious domains

Dozens more models

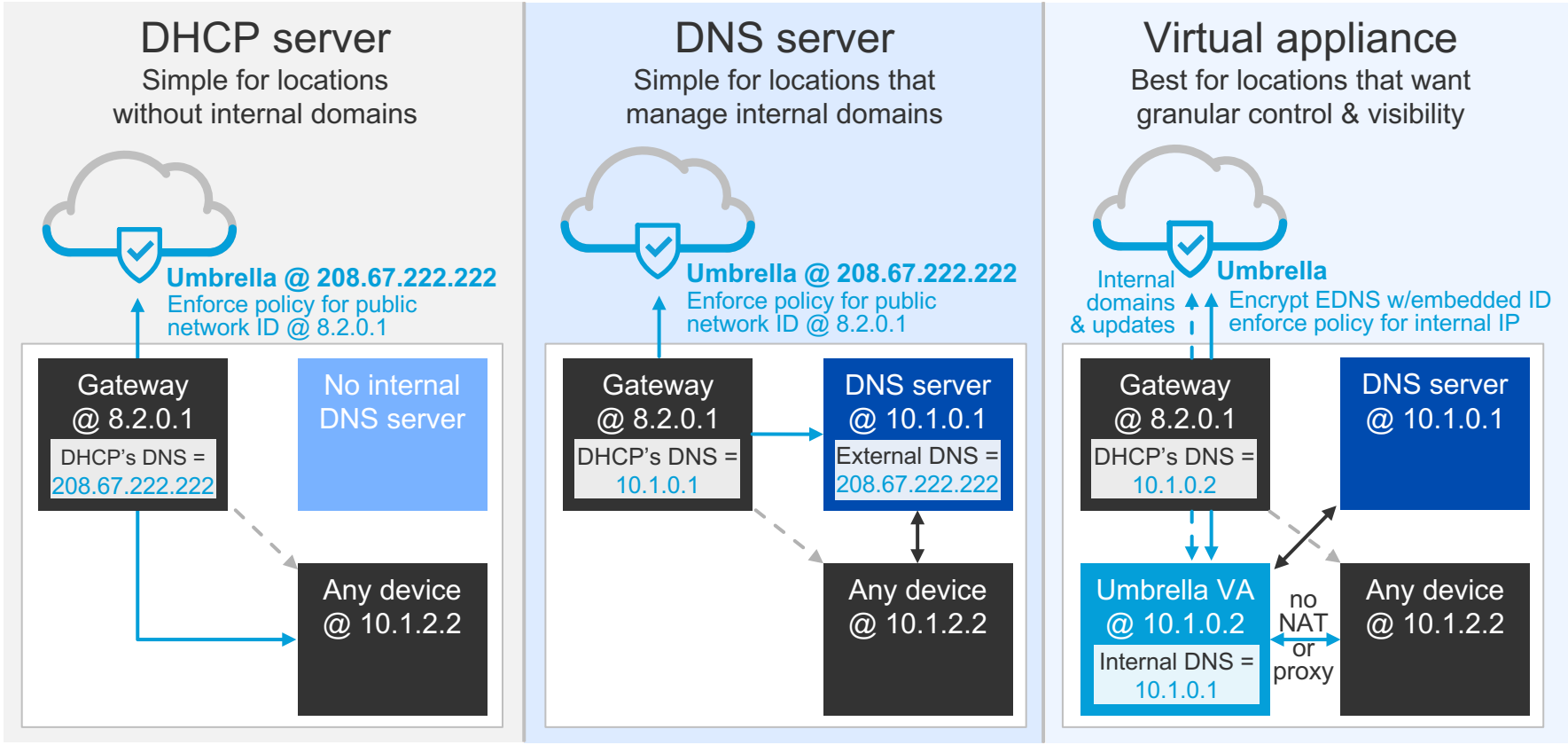
Co-occurrence model
Identifies other domains looked up in rapid succession of a given domain

Natural language processing model
Detect domain names that spoof terms and brands

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco

DEPLOYMENT

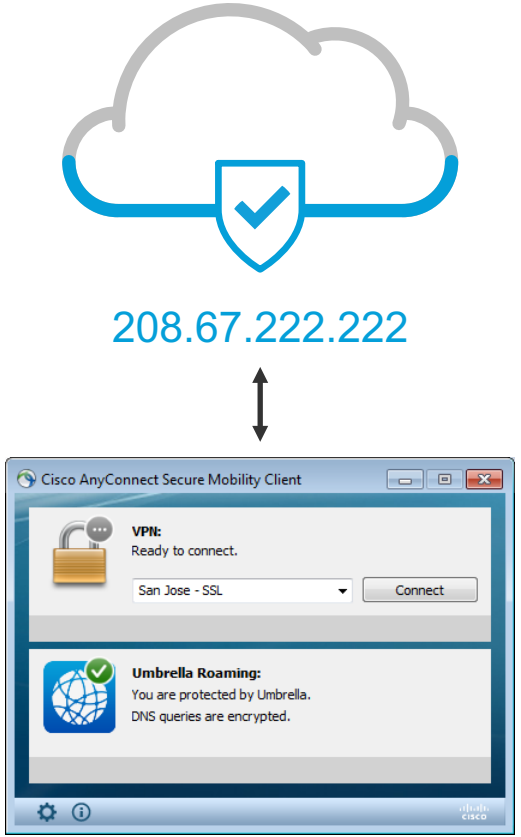
On-network: simple to point external DNS without clients



Cisco AnyConnect module

Roaming protection without another agent

1. Enable roaming security module
2. Set roaming policy in Umbrella
3. Gain visibility into internet activity and detailed logs for incident response



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco

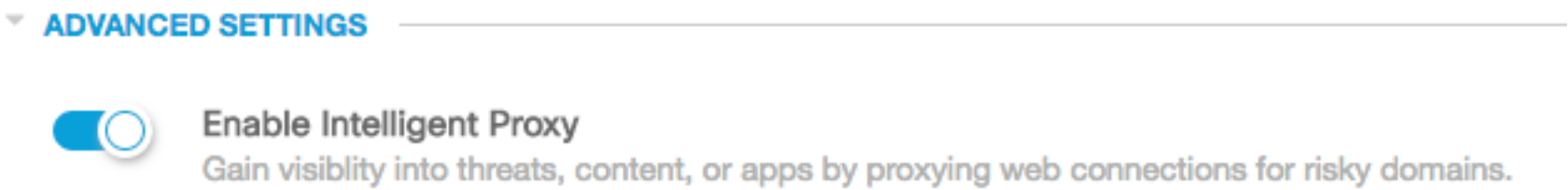
Releases

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco

May 2017		New Policy Wizard
June 2017		Revamped Reporting
July 2017		ISR4K Umbrella Integration: LAN / Private IP Address Reporting
August 2017		SafeSearch
September 2017		File Inspection Services
September 2017		Custom Block URLs
September 2017		Insights Onboarding Setup Wizard
Oct 4th		Active Directory Integration and IP reporting for Roaming

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco

Intelligent Proxy (Released)



Customers can gain visibility into threats by proxying web (80/443) connections for risky domains.

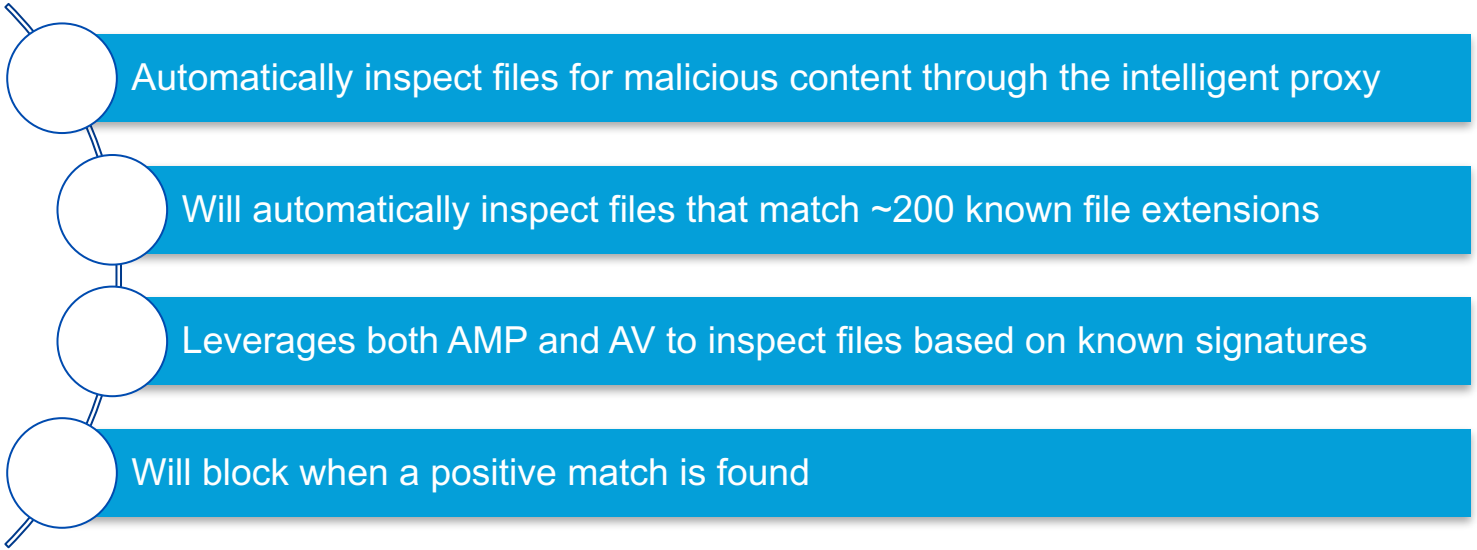
- Enabled by default on all new Policies
- Traffic is proxied if it is currently on the Umbrella ”Grey List”. The Grey List is a set of domains that are considered ”suspicious” but not blocked. This is maintained by the Umbrella team.
- Traffic is **automatically** proxied through our infrastructure if this is enabled and the identity is part of the policy

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco

File Inspection w/ AMP and AV (Released)

Inspect Files

Selectively inspect files for malicious content using antivirus signatures and Cisco Advanced Malware Protection.



© 2017 Cisco and/or its affiliates. All rights reserved. Cisco

Custom URL Blocking (Released)

Enables organizations to block individual URLs by leveraging our Intelligent Proxy

- Customers can block specific URLs that they do not want their customers to go to, either for threat and/or policy reasons
- URL's are blocked within Destination Lists and can be reused
- Adding in a URL also blocks all child URL's if they exist

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco

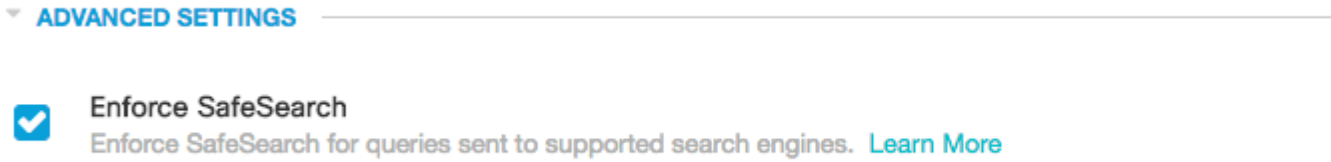
SafeSearch (via DNS)

Enables organizations who want to block access to offensive content as a toggle within their Policy Profile.

- Enabled on a per Policy basis

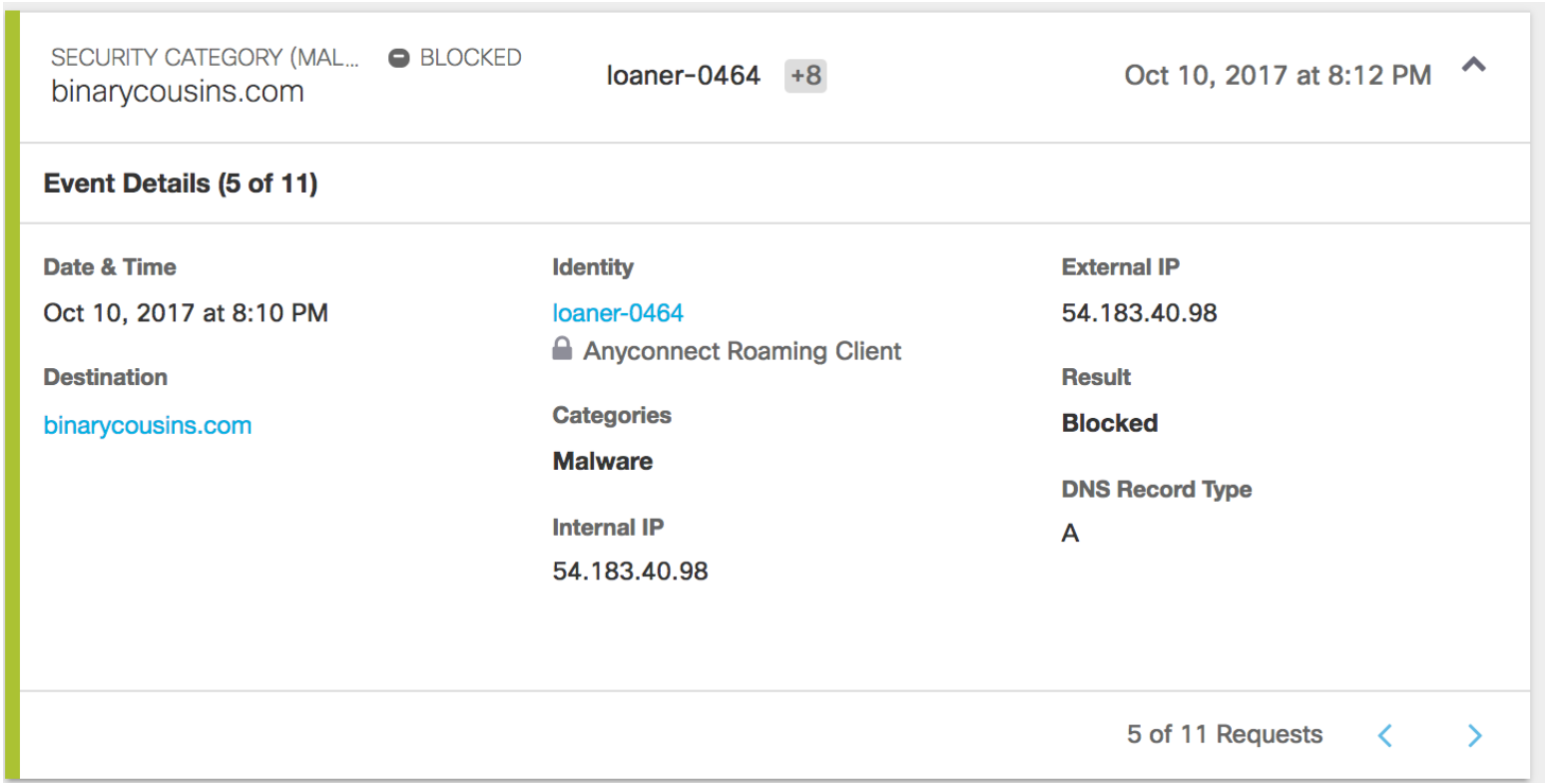
Enabling SafeSearch turns on support for the following SafeSearch entities:

- Google
- Bing
- YouTube



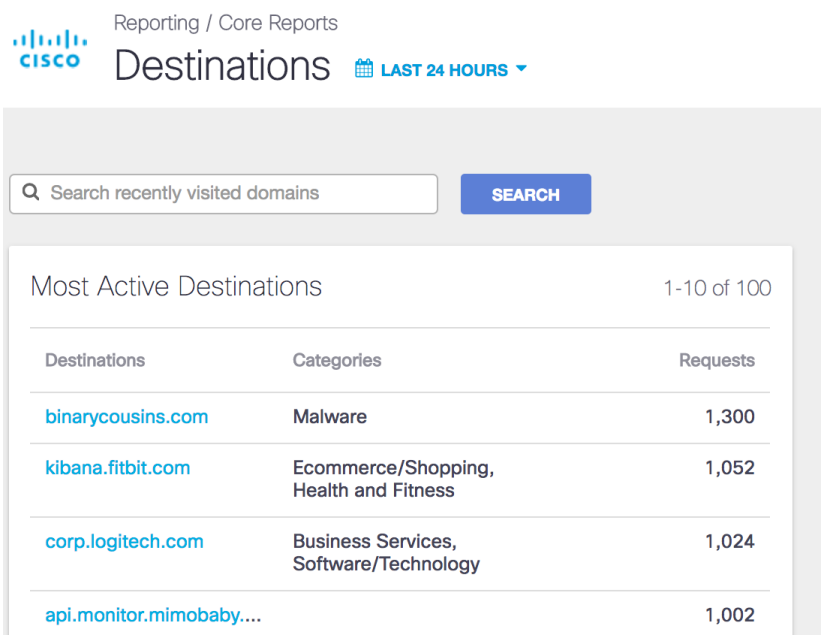
© 2017 Cisco and/or its affiliates. All rights reserved. Cisco

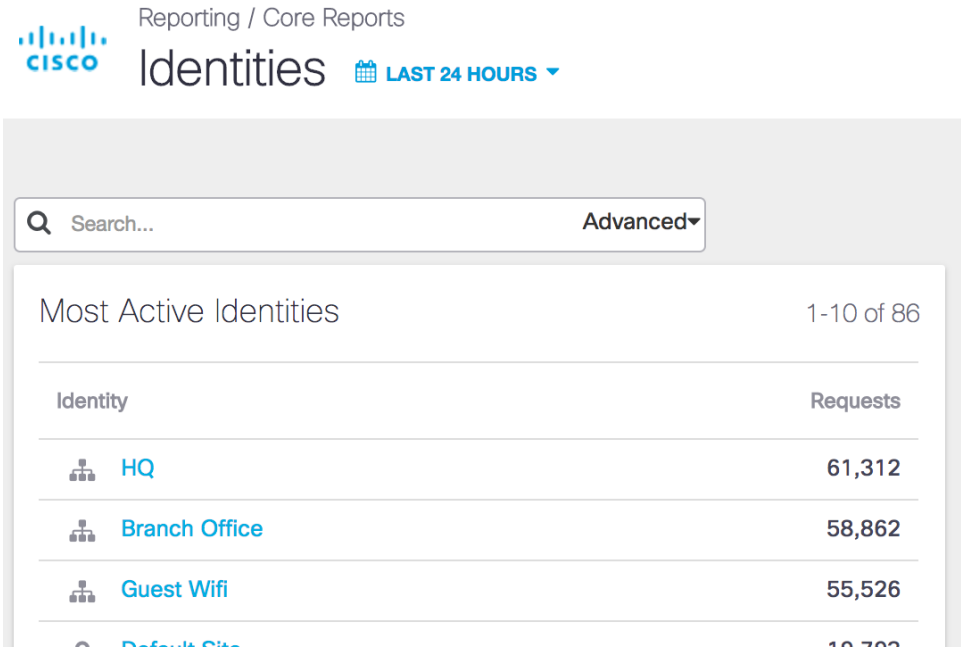
Reporting – Event History feature



© 2017 Cisco and/or its affiliates. All rights reserved. Cisco

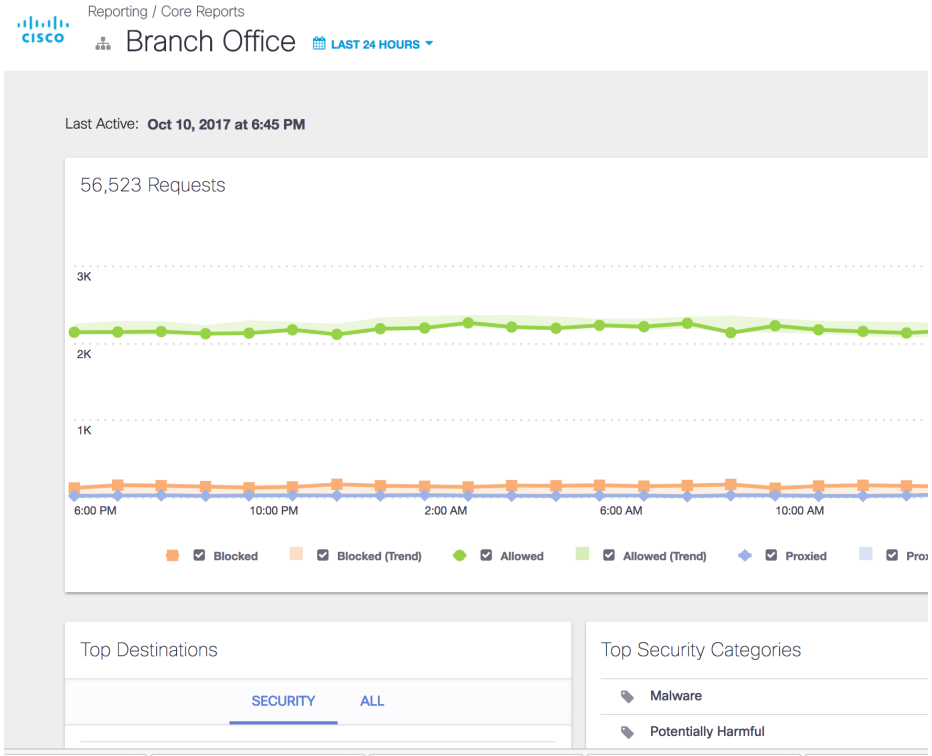
Reporting – Destinations / Identities





© 2017 Cisco and/or its affiliates. All rights reserved. Cisco

Reporting – Granular Identities

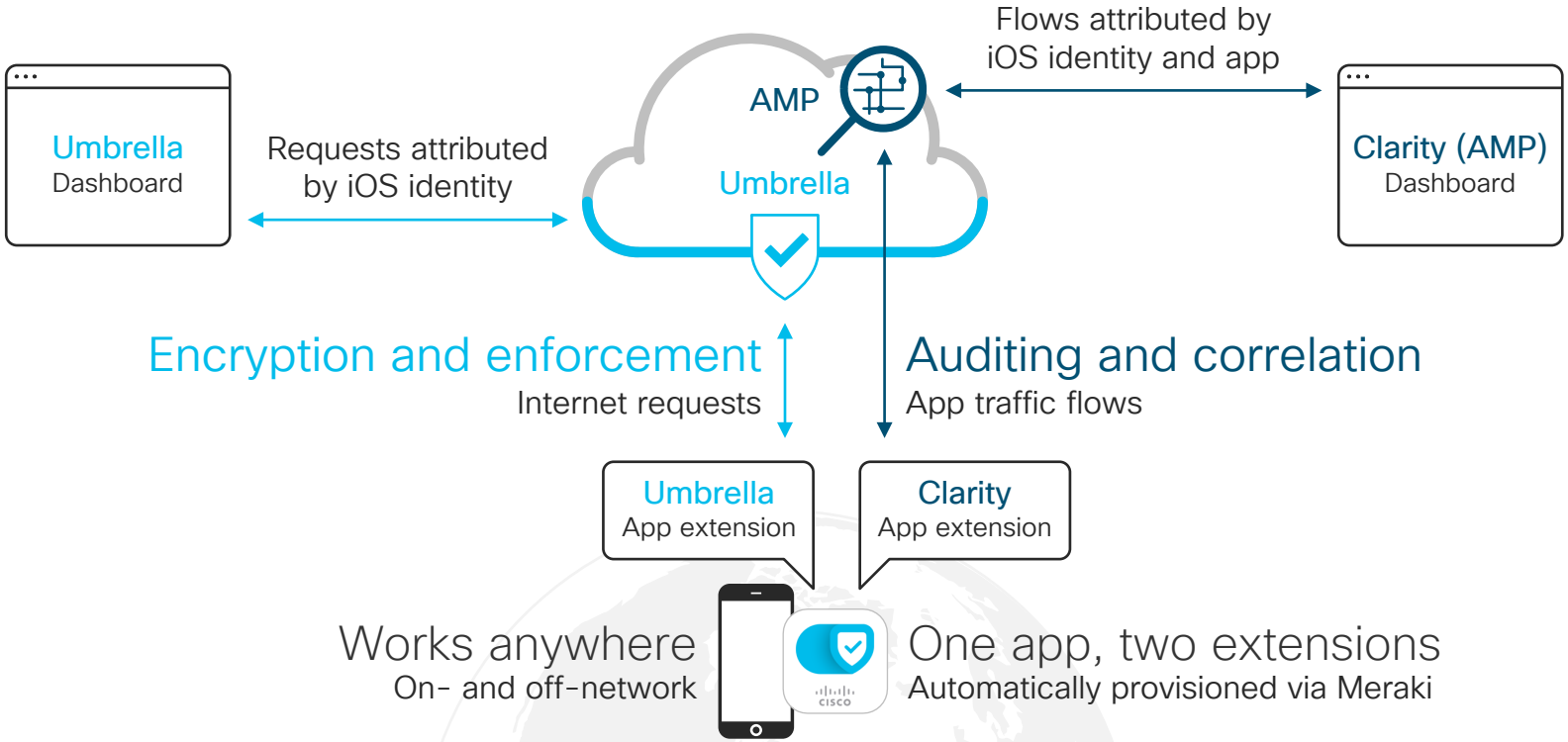


- Limited Availability
- Allows you to pivot on identities in all reports

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco

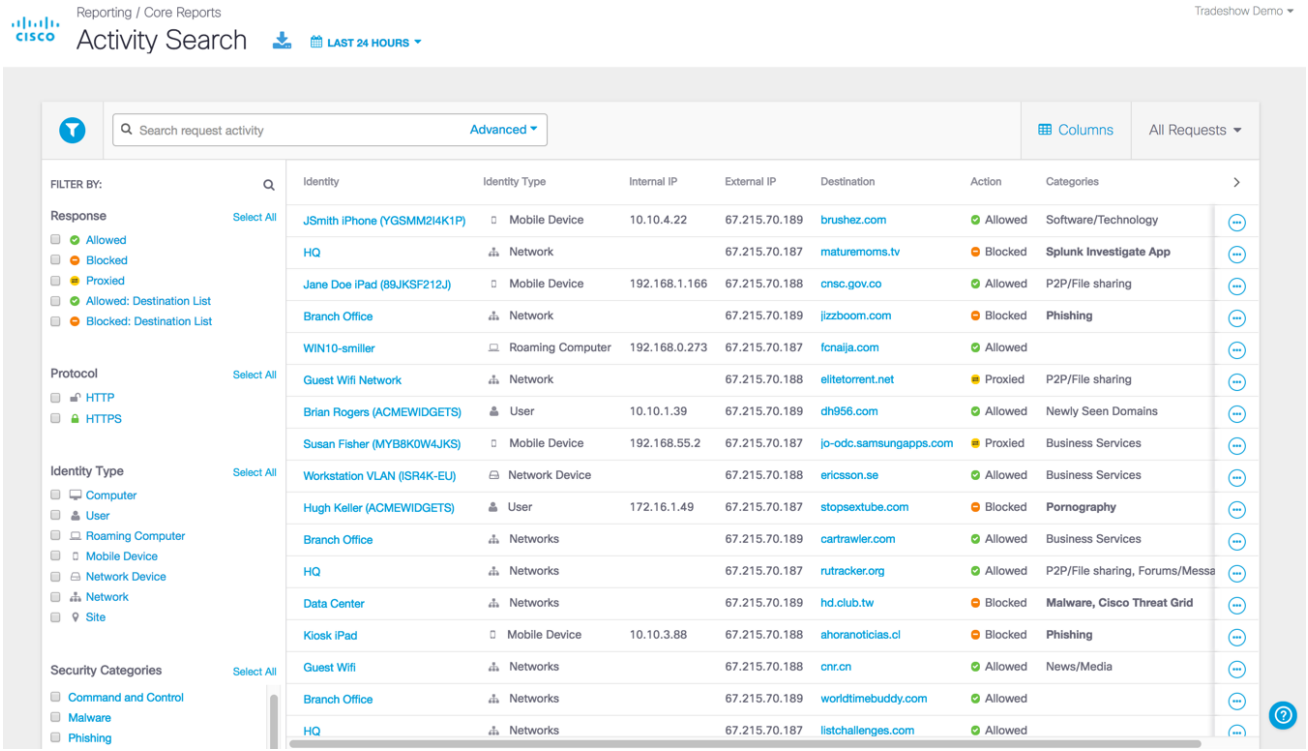
Cisco Security Connector (In Beta)

One App, two layers of Security



SOLUTION

New Identity type



© 2017 Cisco and/or its affiliates. All rights reserved. Cisco

Connectors

AnyConnect

- Integrations with AnyConnect for Windows and Mac (Released)
  - Enables AnyConnect users to be protected with Umbrella when on an untrusted network

Roaming Client

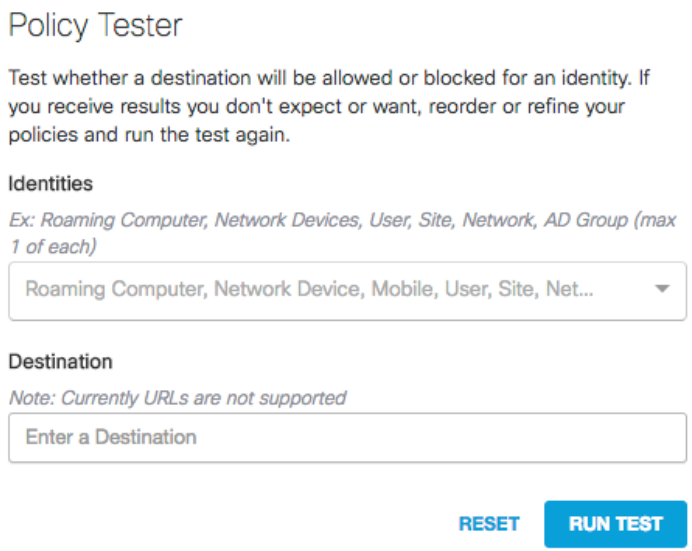
- Customer ability to proxy and enforce at the IP Layer with the Windows and Mac Roaming Client (Released)
- Active Directory Support in the Roaming Client, enabling the ability for customers to gain visibility and leverage identity within Umbrella (In Progress)

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco

Policy Tester (Released)

Enables administrators to understand whether or not a particular identity is blocked or allowed to go to a particular domain.

Administrators can now test the end state across all the policies they have configured to ensure their policies are working



© 2017 Cisco and/or its affiliates. All rights reserved. Cisco

S3 Log Export (Released and Upcoming)

Released

- Customers can export Umbrella logs to their company own S3 bucket
- Then can consume those logs at their leisure into other tools, such as a SIEM, for cross correlation and investigations with other tools
- Customers control how long their logs are retained in S3

Upcoming

- Umbrella will allow users to automatically create S3 buckets managed by Cisco, but used by the end customer for log extraction
- For customers who don't currently have a relationship with Amazon

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco

Application Blocking via DNS (In Progress)

Capability for Umbrella to block “applications” within Policy through DNS

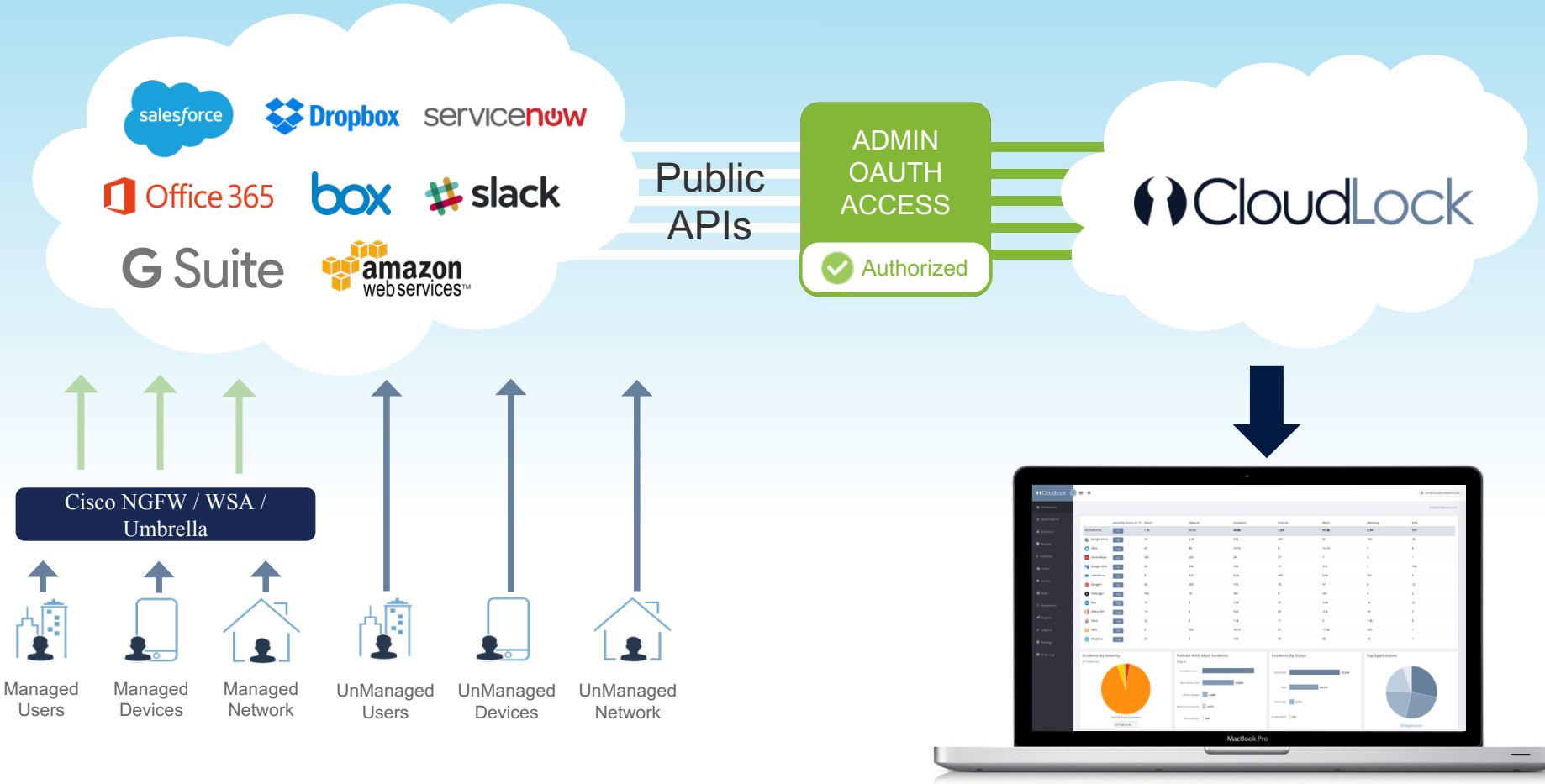
- Enables organizations to block applications such as “Facebook” or “Box” through Umbrella Enforcement Policy
- Customers can block applications on a per Policy basis

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco

CloudLock

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco

CASB - API Access (Cloud to Cloud)



Cloudlock for ServiceNow Update

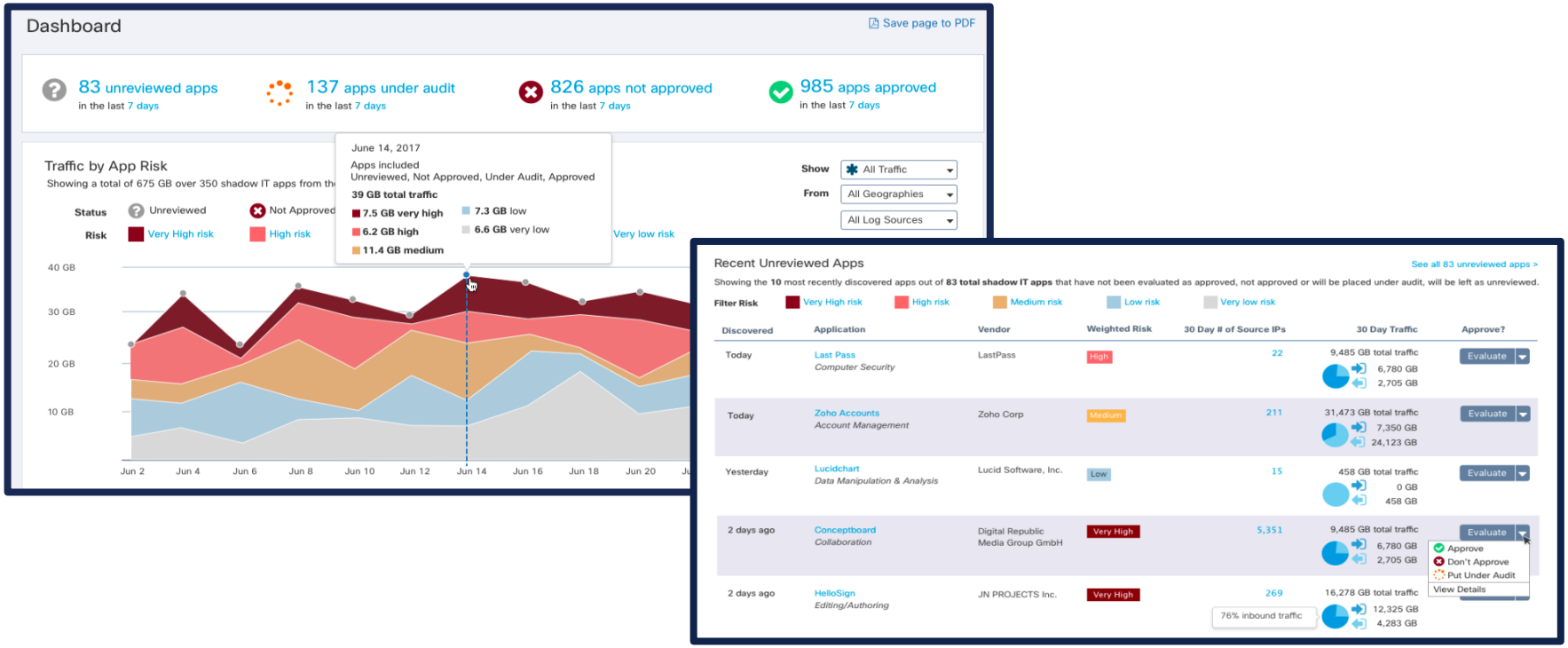
Recent Improvements

- Support for ServiceNow Istanbul version
- In progress: awaiting certification for ServiceNow Jakarta.

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco

Cloudlock App Discovery (Shadow IT)

Currently In BETA

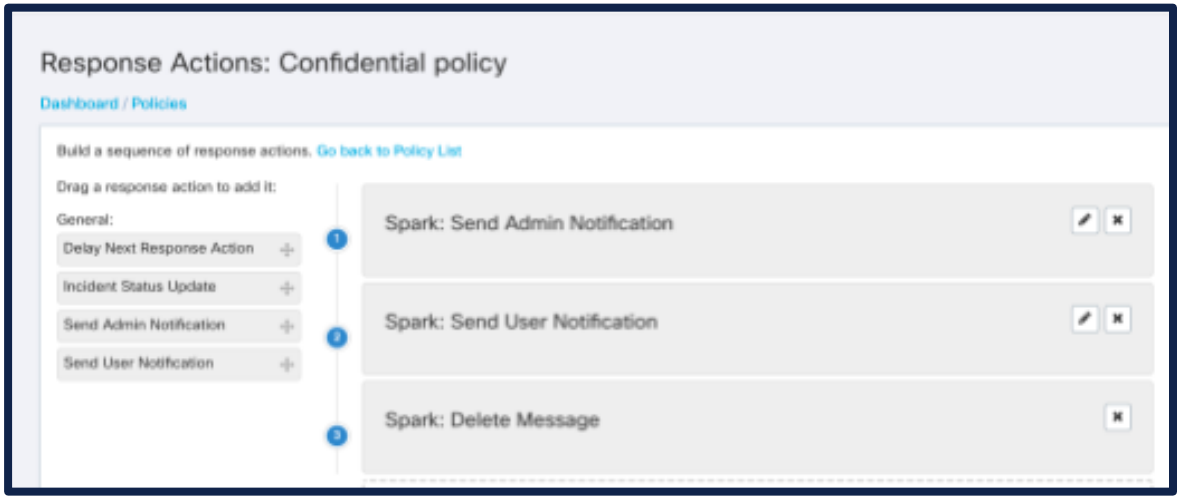


© 2017 Cisco and/or its affiliates. All rights reserved. Cisco

Cloudlock for Cisco Spark

Currently In BETA

- Identify sensitive information that exists in Spark spaces and uploaded files
- Notify end-users of policy violations within Spark
- Delete sensitive messages and files



© 2017 Cisco and/or its affiliates. All rights reserved. Cisco

Stealthwatch Cloud

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco

Stealthwatch Cloud makes it simple to see everything

Get complete visibility into your network and public cloud

Detect threats automatically

Deploy and manage easily

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco

Oktober | November | December | **Alle**

Oktober

Dato	Seminar/event	Målgruppe	Sted
24.	Cisco Virtual Update – Video Endpoints	Slutkunder/Partnere	Online
25.	Cisco Virtual Update – Cloud Security	Slutkunder/Partnere	Online

November 2017

Dato	Seminar/event	Målgruppe	Sted
7. & 9.	Cisco Tech Update – Security nyheder	Slutkunder/Partnere	Århus & København
15.	Cisco Virtual Update – ACI 3.0	Slutkunder/Partnere	Online
21.	Cisco Virtual Update – Cisco Spark Service	Slutkunder/Partnere	Online
22.	Cisco Virtual Update – Programmering i LAN netværk	Slutkunder/Partnere	Online
28. & 30.	Cisco Tech Update – Nexus Switching	Slutkunder/Partnere	Århus & København

December 2017

Dato	Seminar/event	Målgruppe	Sted
13.	Cisco Virtual Update – Core Switching	Slutkunder/Partnere	Online

ates. All rights reserved. Cisco

Følg med

- Talos blog
- Cisco security blog
- Security nyhedsbrev
- Tech Updates
- Afholdte seminarer
- Security Chalk Talks

- Umbrella / OpenDNS
- CloudLock
- Stealthwatch
- Umbrella
- CloudLock
- Stealthwatch cloud

Tag fat i jeres Account Manager, Jesper Rathsach, Tue Frei Noergaard, Jan Minche eller Mikael Grotrian for en dybere gennemgang, Proof of Value eller en Dcloud demo adgang.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco

CISCO
TOMORROW starts here.