TWO SIMPLE SOLUTIONS TO STOP THREATS BEFORE THEY REACH YOUR END USERS

Quickly and Easily Secure On-Premises and Remote Internet Content Access and Usage

Christopher Raye
Senior Account Manager
Networking For Future

William Booth
Cloud Security Specialist
Cisco Systems

Steven Gay
Cybersecurity Account Manager
Cisco Systems

CISCO

NFF

Agenda

Company Overview

Cisco Umbrella

Cisco AMP for Endpoints

Case Studies
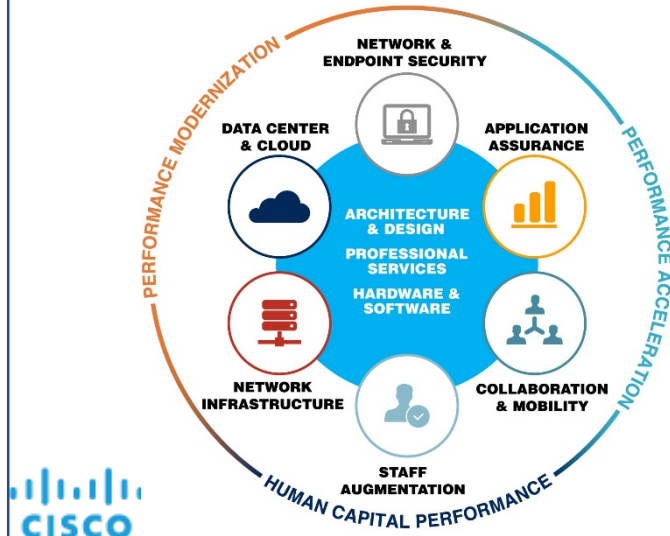
Next Steps

Questions

Networking For Future (NFF) offers a performance-focused approach to delivering transformational IT business solutions

Networking For Future, Inc. (NFF)

- Founded in 1996
- Headquartered in Washington, DC
- 130+ Employees
- 77% of workforce hold industry certifications

IT Business Solutions

Strategic Partners
- Cisco Gold Partner
- Riverbed Premier
- Splunk Partner
- NetApp Gold
- VMware Enterprise Partner
- Microsoft Certified Silver
- Gigamon
- F5 Networks
- CoreSite

Strategic Contract Vehicles
- GSA Schedule (GS-35F-0197L)
- District of Columbia Supply Schedule
  - MOBIS and ITES
- Maryland Education Enterprise Consortium (MEEC)
- Maryland Consulting and Technical Services (CATS+)
- Fairfax County Public Schools
- Maryland DoIT Hardware Master Contract

**District of Columbia Certified Business Enterprise (CBE)**

SARA™
Standards American Registrations Authority
REGISTERED
ISO 9001:2015

Inc.500|5000

ICIC
HALL OF FAME AWARD

NFF

Clients

GOVERNMENT	EDUCATION	NON-PROFIT	COMMERCIAL	TRANSPORTATION AND UTILITIES	HEALTHCARE
■ U.S. Census Bureau ■ U.S. Navy ■ U.S. Air Force ■ General Services Administration ■ United Services Organizations ■ DC Government Offices and Departments	■ Georgetown University ■ Montgomery College ■ Alexandria Public Schools ■ The Catholic University of America ■ University of the District of Columbia ■ DC Public Schools	■ Smithsonian Institution ■ Better Business Bureau ■ National Association of Convenience Stores ■ American Alliance of Museums ■ NeighborWorks America ■ National Association of College and University Attorneys	■ The MITRE Corporation ■ Cisco Systems ■ Contact Solutions ■ Perdue Farms, Inc ■ Hexaware / FREDDIE MAC ■ CSSI, Inc. ■ United Parcel Service ■ National Cooperative Bank ■ Smartronix ■ SpaceNet ■ Virginia Tech Applied Research Corp ■ Newseum	■ Washington Metropolitan Area Transit Authority ■ Metropolitan Washington Airports Authority ■ DC Water ■ Washington Suburban Sanitary Commission ■ DC Office of Cable Television	■ Novant Health Systems ■ Shady Grove Fertility ■ DC Health Benefit Exchange Authority ■ SureScripts

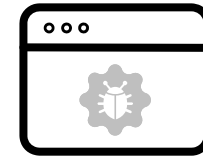# The Way We Work Has Changed
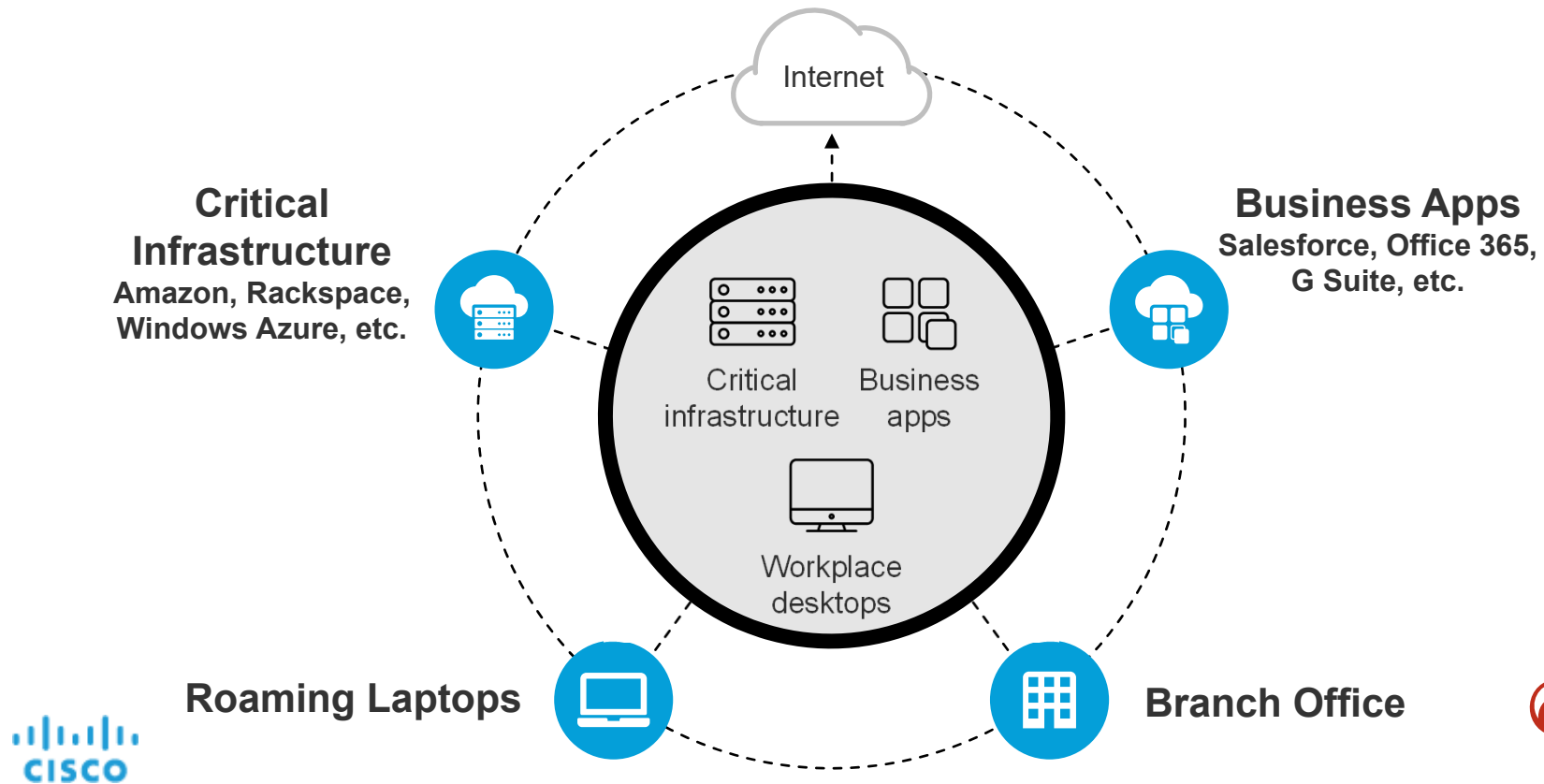
Your Challenges
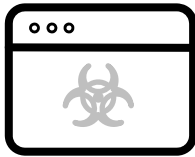
Malware and Ransomware

Command and Control (C2) Callback

Malicious File and Behavior Detection

Outbreak Control and Quarantine

Insta-Poll

How confident are you that you have the coverage you need?

- ○ Very confident (not sure why I'm at this webinar)
- ○ Moderately confident
- ○ Constant worry
- ○ Keeps me up at night
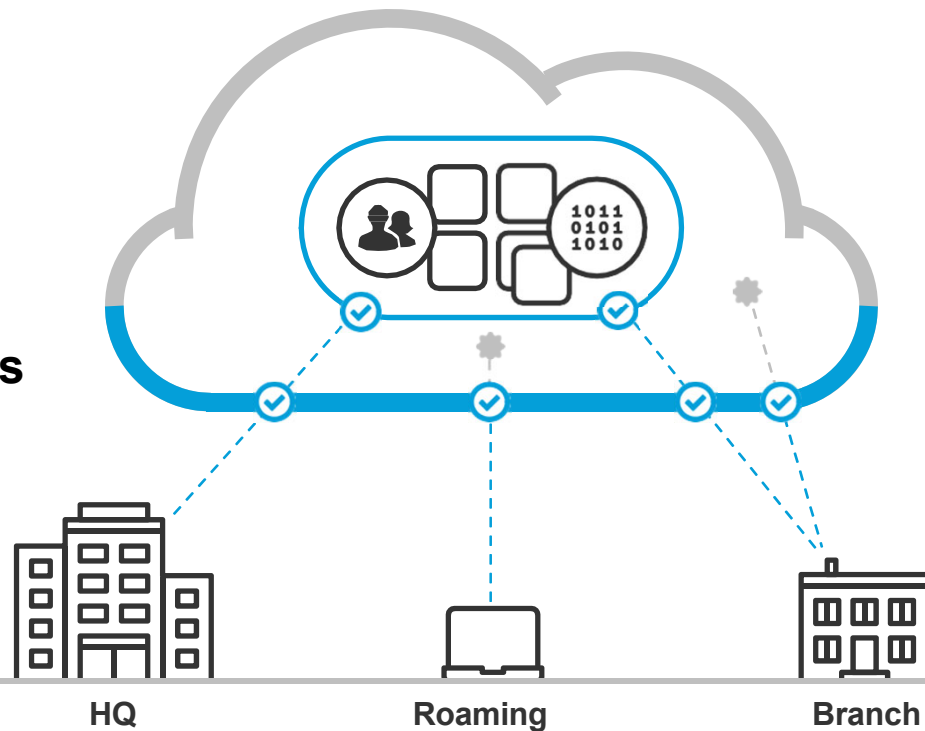- ○ Scared to death (sign me up for a Proof of Value)

CISCO

NFF

Our Solution

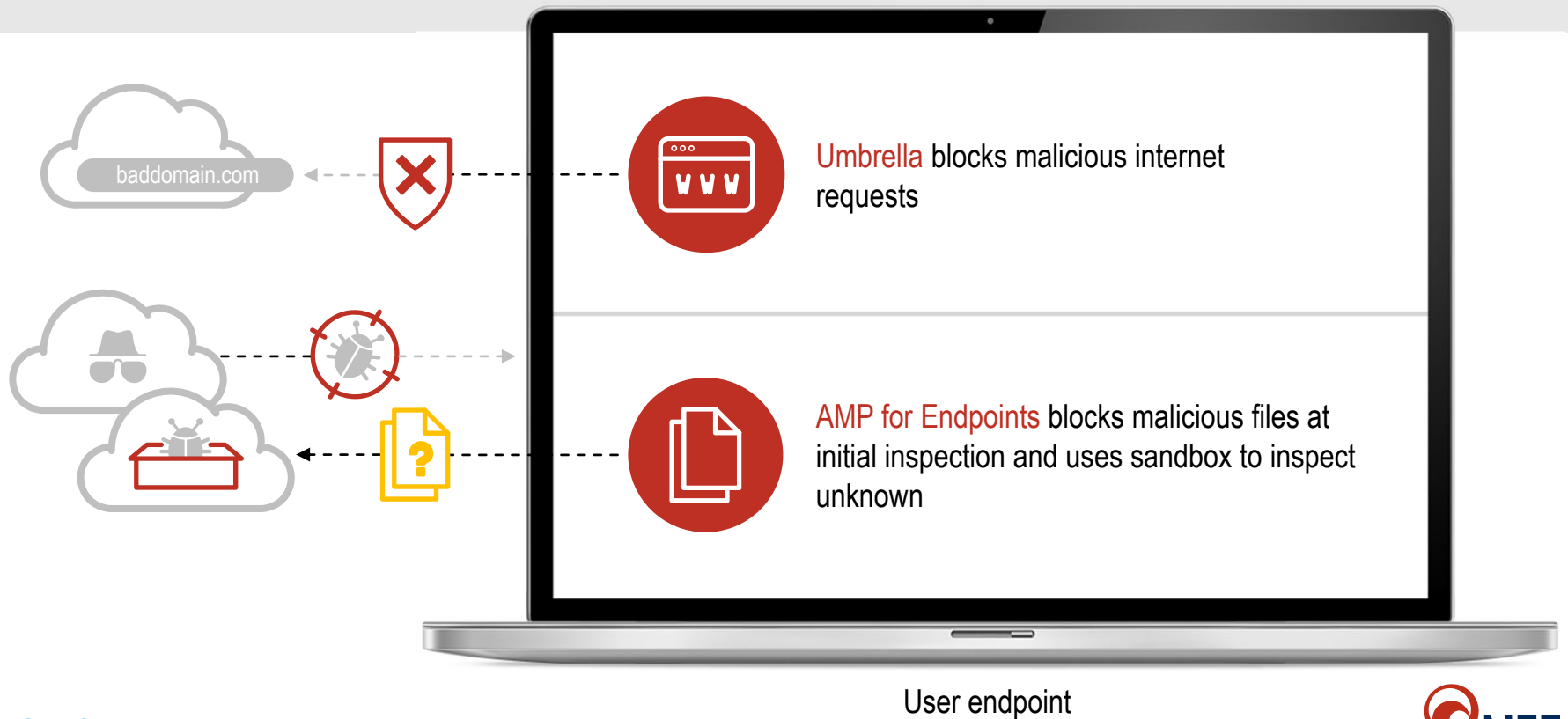## Cisco Umbrella
First line of defense against Internet threats

Cisco AMP for Endpoints
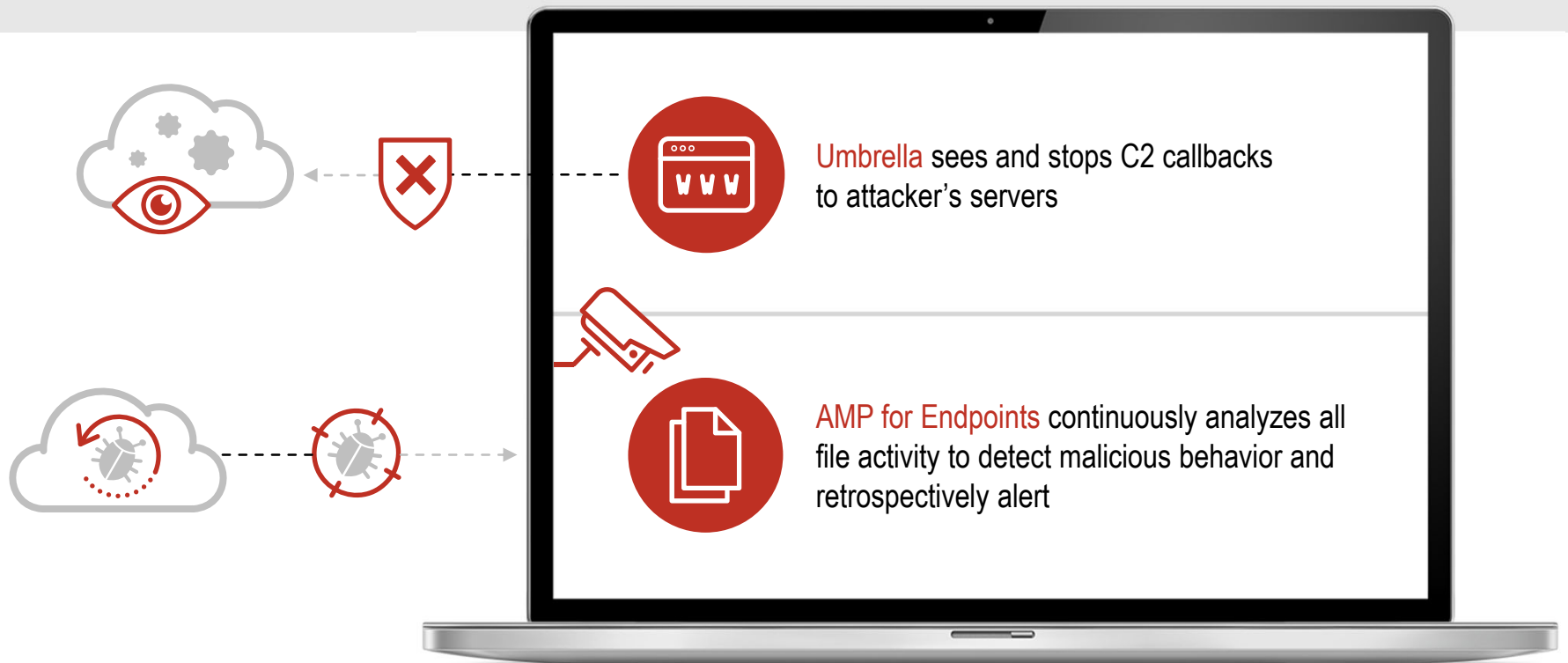**Secures against malicious files and malicious behavior**

HQ

Roaming

Branch Office

Prevent

Umbrella blocks malicious internet requests

AMP for Endpoints blocks malicious files at initial inspection and uses sandbox to inspect unknown

User endpoint

Detect

Umbrella sees and stops C2 callbacks to attacker's servers

AMP for Endpoints continuously analyzes all file activity to detect malicious behavior and retrospectively alert

User endpoint

CISCO

NFF

Respond

DOMAINS

IPs

FILE HASHES

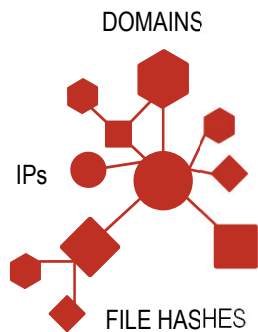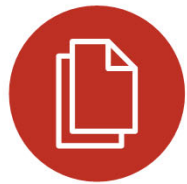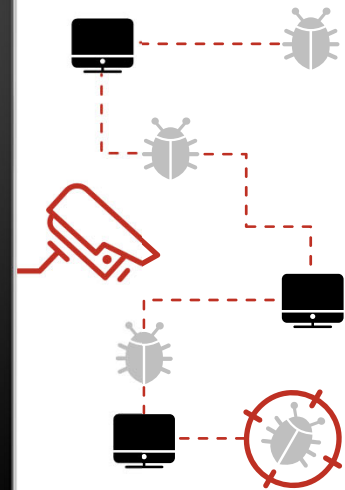**Umbrella** Investigate provides current and historical data on domains, IPs, and file hashes

AMP for Endpoints shows full history of compromise, and provides outbreak control and quarantine capabilities

Security team

CISCO

NFF

Case Study: PTC

ptc®

Number of users and locations protected:
8K end users across 7 major hubs worldwide, including U.S., South America, India, Singapore, and the U.K.

Challenge:
Reduce malware infections, increase insight of potential threat sources, improve reporting.

Solution:
Umbrella and Investigate

Impact:
- Prevent malicious connections and data exfiltration
- Extend protection with FireEye integration
- Obtain intelligence on threat sources before attacks
- Reduced reporting from hours to minute

CISCO

"It took less than ten minutes for us to point our DNS traffic to the Umbrella Global Network. We could protect our remote offices around the world in less than an hour and a half."

Mark Arnold
Director of Information Security

NFF

Case Study: Mobile County Public School System

Employees: 7,500 **Endpoints:** 27,000

Objective: MCPSS knew they needed to increase security as attacks accelerated and became more sophisticated. To reduce administration costs and to optimize performance, the solution had to be cloud-based.

Solution: Cisco AMP for Endpoints

Impact:

- Protection on and off network
- Deep visibility into all endpoint activity
- Rapid time to detection

"'AMP brings Mobile County peace of mind because it's a global product that keeps us safe from emerging threats and the vulnerabilities we couldn't see before.

George Mitchell
Head of Research and Development, MCPSS
Mobile County Public Bus School System

Real Customer Results

Umbrella

"Reduced infections by 98% ... saved 1.7 months of user downtime per year"

"Cut incident response time by 25-30%"

"Increased threat detection by 200%...reduced incident response time by 10 days"

"Decreased the number of ransomware outbreaks to zero for last 8 months."

AMP for Endpoints

CISCO

NFF

Next Steps

- **Discover the impact these solutions can have on your organization**

- **Contact Chris Raye at 240-281-5209 and craye@nffinc.com**
  - **More Information**
  - **Demonstration**
  - **Proof of Value**

- **Share webinar recording with your friends**

Questions?

Your performance improvement
is our measure of success.

Thank You!

Your Challenges
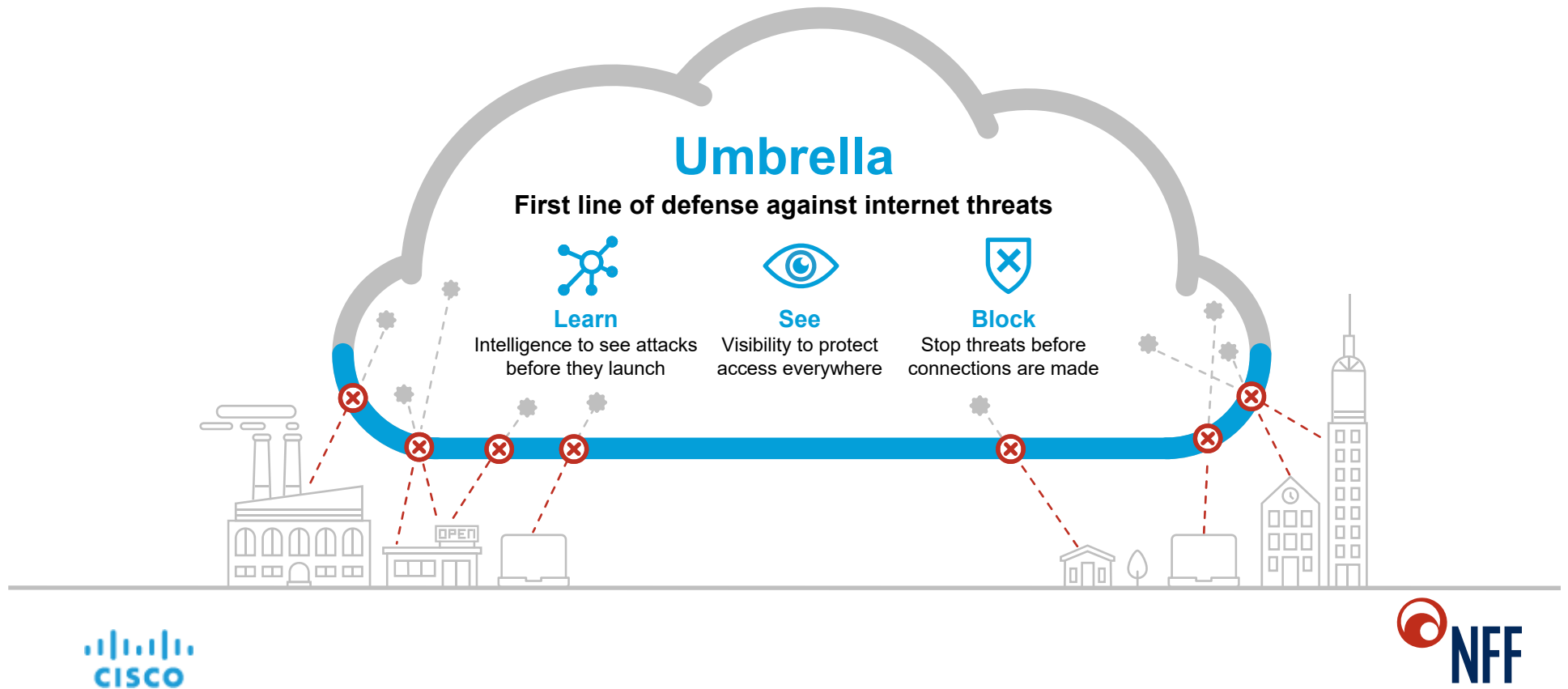
Malware and ransomware

Gaps in visibility and coverage

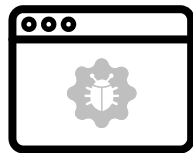Compromised accounts and malicious insiders

Data breaches and compliance

Cisco Umbrella

Umbrella

First line of defense against internet threats

Learn
Intelligence to see attacks before they launch

See
Visibility to protect access everywhere

Block
Stop threats before connections are made

CISCO

NFF

Prevents Connections Before And During The Attack

Web and email-based infection

Malvertising / exploit kit

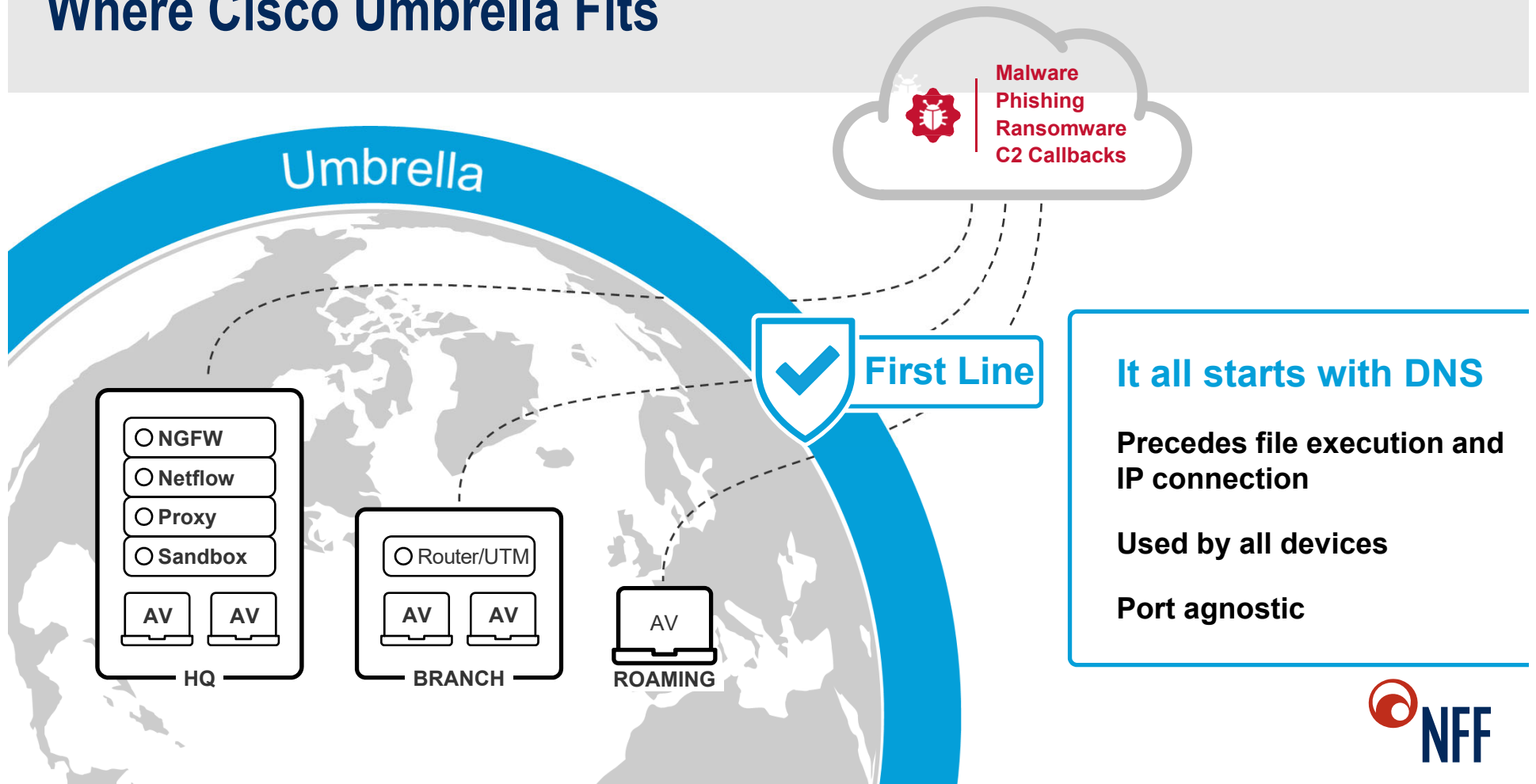**Phishing / web link**

Watering hole compromise

Command and control callback

Malicious payload drop
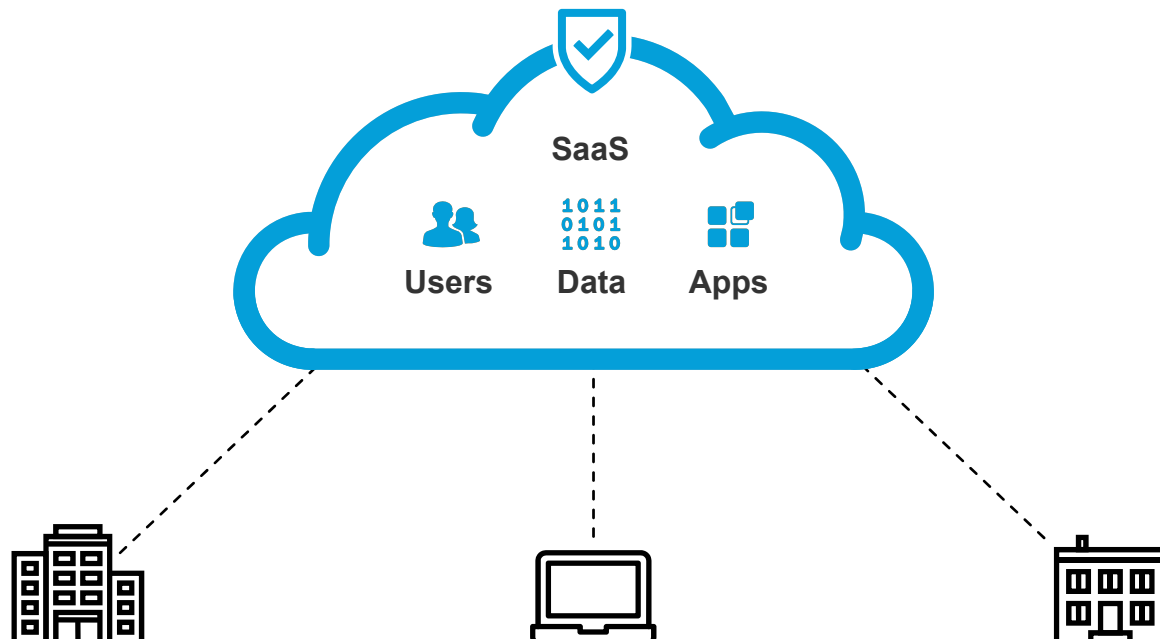
Encryption keys

Updated instructions

Stop data exfiltration and ransomware encryption

Where Cisco Umbrella Fits

Malware
Phishing
Ransomware
C2 Callbacks

Umbrella

First Line

It all starts with DNS

Precedes file execution and IP connection

Used by all devices

Port agnostic

NGFW
Netflow
Proxy
Sandbox

AV   AV

HQ

Router/UTM

AV   AV

BRANCH

AV

ROAMING

NFF

Cisco Cloudlock

Cloud Access Security Broker (CASB)

Addressing Your Most Critical Cloud Security Use Cases

Discover and Control

Compromised Accounts

Insider Threats

Data Exposures and Leakages

Privacy and Compliance Violations

OAuth Discovery and Control

Shadow IT

User and Entity Behavior Analytics

Cloud Data Loss Prevention (DLP)

Apps Firewall

Cloudlock Has Over 70 Pre-Defined Policies

PII

- SSN/ID numbers
- Driver license numbers
- Passport numbers

Education

- Inappropriate content
- Student loan application information
- FERPA compliance

General

- Email address
- IP address
- Passwords/ login information

PHI

- HIPAA
- Health identification numbers (global)
- Medical prescriptions

PCI

- Credit card numbers
- Bank account numbers
- SWIFT codes

CISCO

NFF

Cisco Cloud Security

	Umbrella	Cloudlock
Visibility and control	For all internet activity	For connected OAuth cloud apps
Threat protection	To stop connections to malicious internet destinations	To protect cloud accounts from compromise and malicious insiders
Forensics	To investigate attacks with internet-wide visibility	To audit cloud logs
Data protection	To block C2 callbacks and prevent data exfiltration	To assess cloud data risk and ensure compliance
Malware / ransomware	To prevent initial infection and C2 callbacks	To prevent cloud-native (OAuth) attacks

CISCO

NFF

Case Study: Cloudera

cloudera

Users: 1,600

Objective: As Cloudera grew, the time-intensive access controls it relied on to help safeguard its data secured in Cloud-based applications struggled to scale.

Solution: Cisco Cloudlock

Impact:

- Secures users and data in Salesforce, Google, Okta and Box
- Increased visibility with cloud tracking and monitoring capabilities
- Ensured integrity and accuracy of massive datasets

CISCO

"At a time when businesses must take advantage of the cloud to remain competitive, Cloudlock delivers the visibility and protection essential to working securely in the cloud."

Eddie Garcia
Chief Information Security Officer (CISO)
Cloudera

NFF

Case Study: The University of Oklahoma

Users:
36,000 - Cloudlock   6,000 - Umbrella

Objective:
OU's campus-wide move to Office 365 required a new security approach to protect its highly sensitive and heavily regulated data on-premises and in the cloud.

Solution:
Cisco Cloudlock
Cisco Umbrella

Impact:
• Quickly remediated a set of compromised accounts
• Significantly decreased malware infections
• Increased blocked threats by thousands per hour
• Secured users, data, and apps in the cloud
• Cut security administration and remediation time

" The all around experience with Cloudlock has been terrific. From DLP to UEBA, we've gotten the visibility we need into our cloud environments and have been able to extend our security policy to those locations."
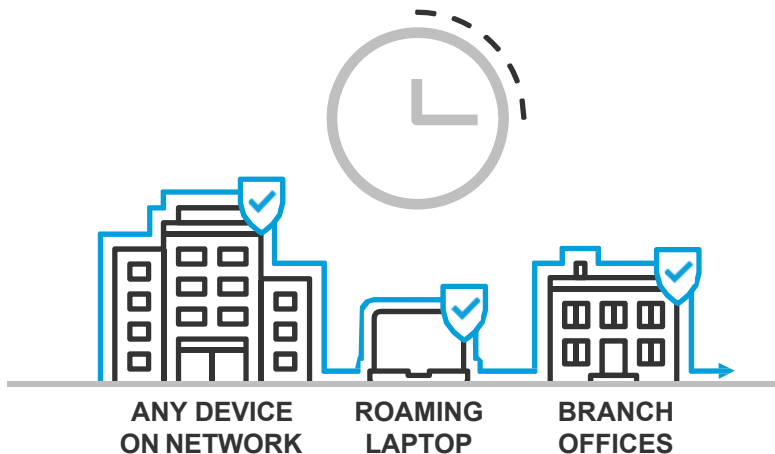
Aaron Baillio
Managing Director, Security Operations and Architecture
University of Oklahoma

Enterprise-Wide Deployment In Minutes

● **Sign up**   ● **Deploy**   ● **Point your DNS**

ANY DEVICE
ON NETWORK ROAMING
LAPTOP BRANCH
OFFICES

On-network coverage

With one setting change

Integrated with Cisco ISR 4K series

Off-network coverage

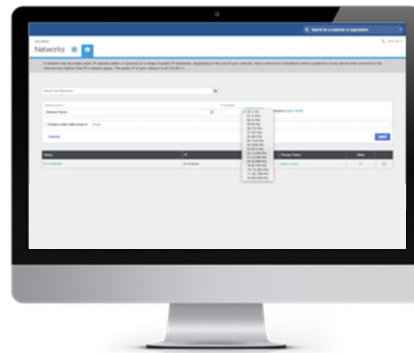**With AnyConnect VPN client integration**

Or with any VPN using lightweight Umbrella client

Enterprise-Wide Deployment In Minutes

1 Point DNS to Cisco Umbrella

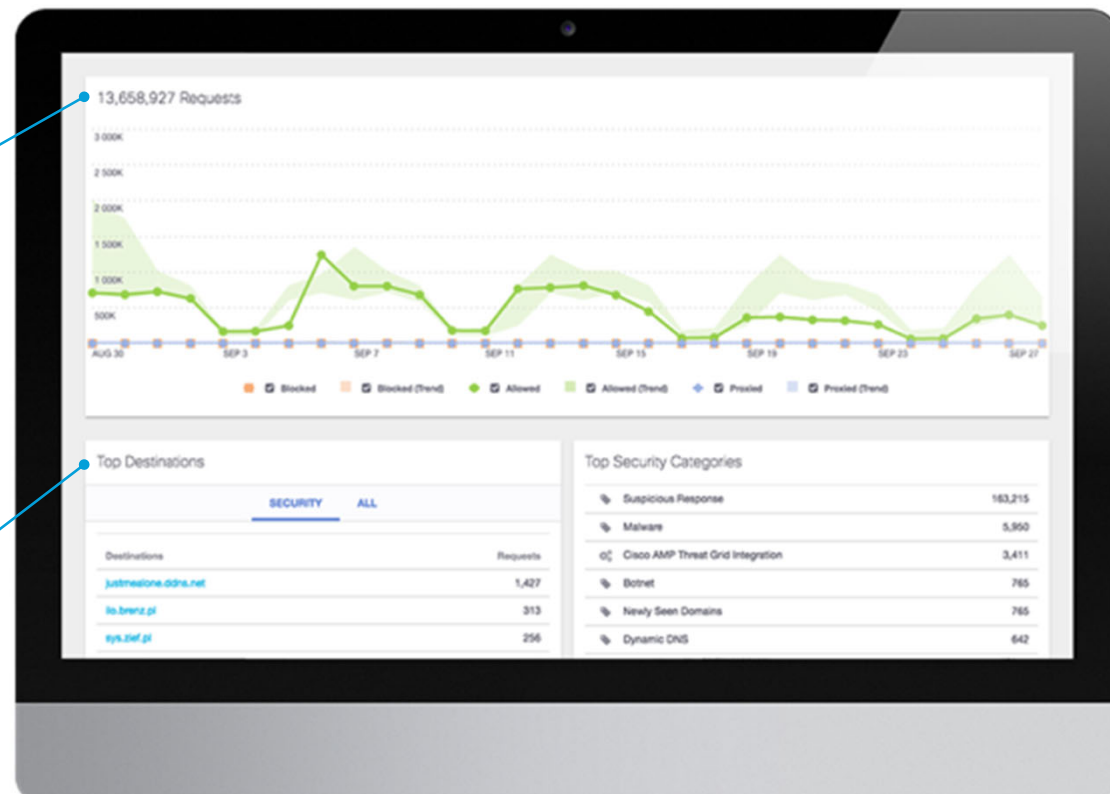**2** Configure network IP address on Cisco Umbrella

3 Enforce and report

Identity Reports: Quickly spot and remediate victims

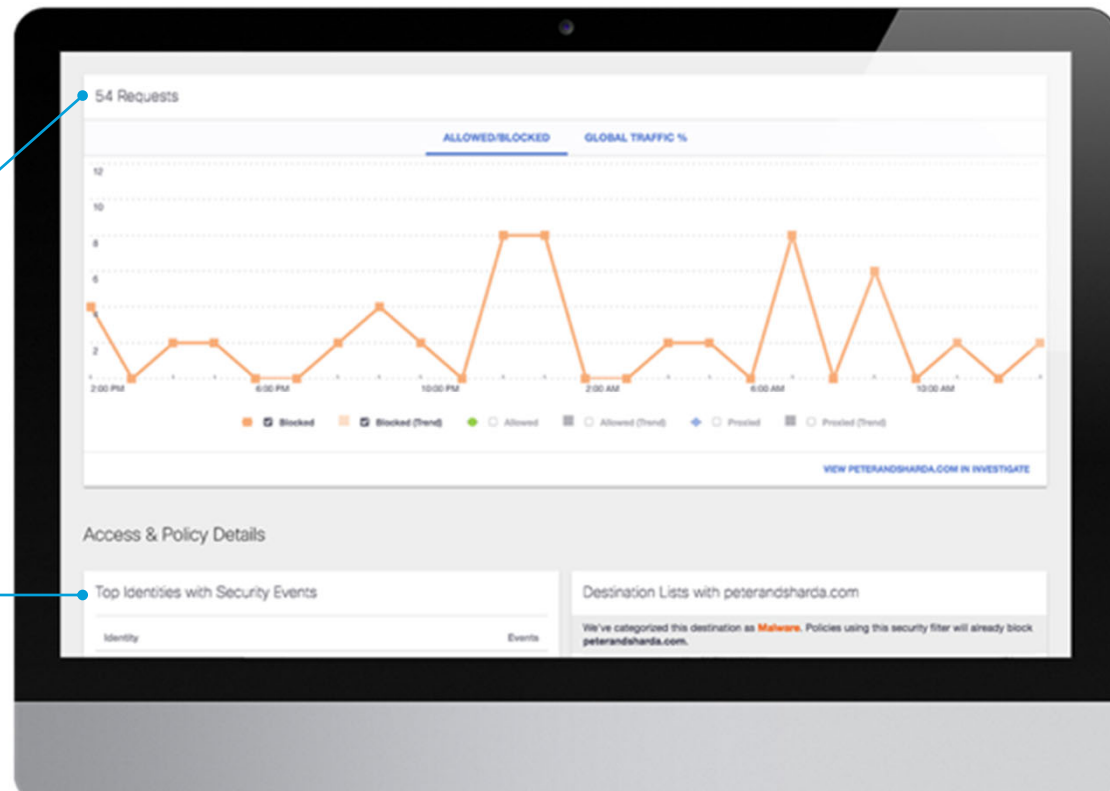**Allowed, blocked, and proxied traffic per device or network**

Top activity and categories per device or network

Destination Reports: Quickly assess extent of exposure
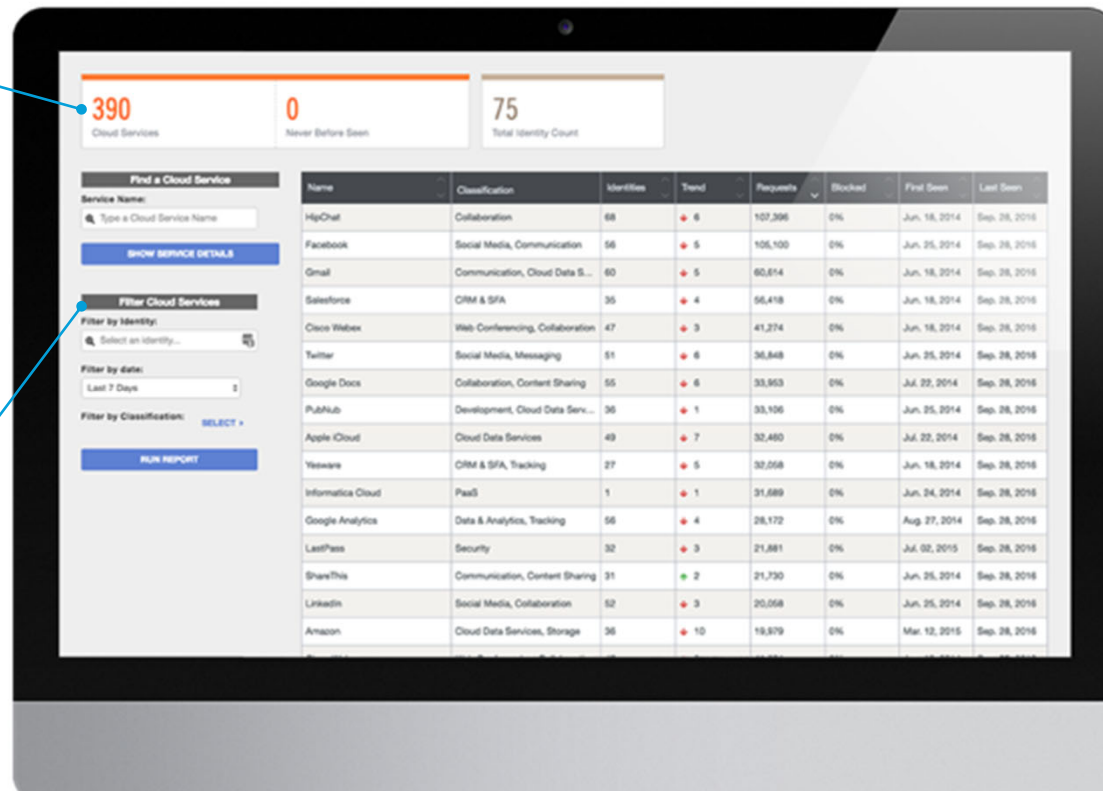

Local vs. global trends for malicious domains

Top identities associated with malicious activity

Cloud Services Report: Effectively combat shadow IT

Total and newly seen cloud services

Cloud apps by classification and traffic volume

Customer testimonials

"Cisco Advanced Malware Protection, in combination with Cisco Umbrella, has decreased the number of ransom-ware outbreaks to zero during the last 8 months."

Freek Bosscha
IT Architect, NHL

"We have much greater confidence in the security of our endpoints with Cisco Umbrella combined with Cisco AMP. We have had zero malware infections since our implementation 3 years ago."

Engineer
Medium Enterprise
Financial Services Company