

Modern attacks and malware

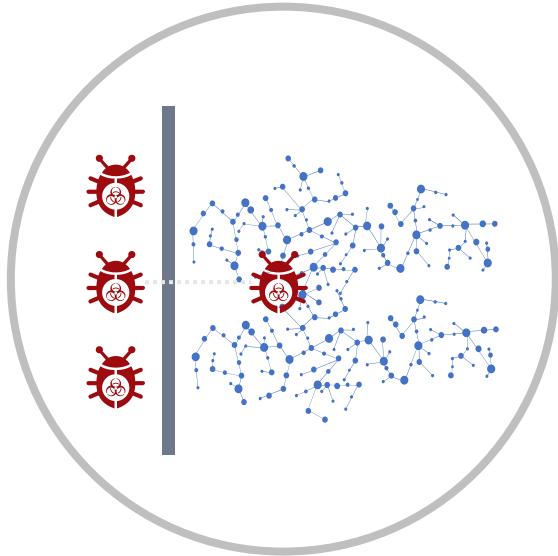


Everything starts with an email and web

Dragan Novakovic
Cisco Systems



New Cyber Threat Reality



Your environment
will get breached



You'll most likely be
infected via email



Hackers will likely
command and control
your environment via web

Cisco Email Security Solutions





Email is still the #1 threat vector



Phishing leaves businesses on the line



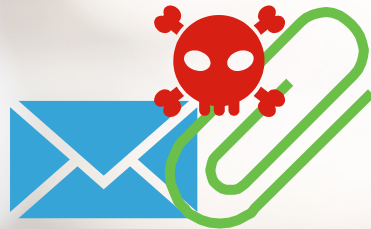
Phishing



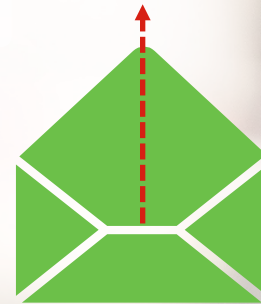
Spoofing



Ransomware



94%
of phish mail has
malicious attachments¹



30%
of phishing messages
are opened¹

\$500M

Loss incurred due
to phishing
attacks in a year
by US companies²

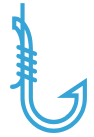
¹2016 Cisco Annual Security Report
²2016 Verizon Data Breach Report, Kerbs on Security

Messages contain
attachments and URL's

Socially engendered
messages are well crafted
and specific

Credential "hooks" give
criminals access to your
systems

Spoofing rates are on the rise



Phishing



Spoofing



Ransomware



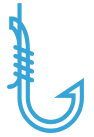
¹FBI Warns of Dramatic Increase in Business email scams, 2016

Forged addresses fool recipients

Threat actors extensively research targets

Money and sensitive information are targeted

Ransomware attacks are holding companies hostage



Phishing



Spoofing



Ransomware



Ransomware represents the biggest jump in occurrences of crimeware¹



\$60M



Cost to consumers and companies of a single campaign²

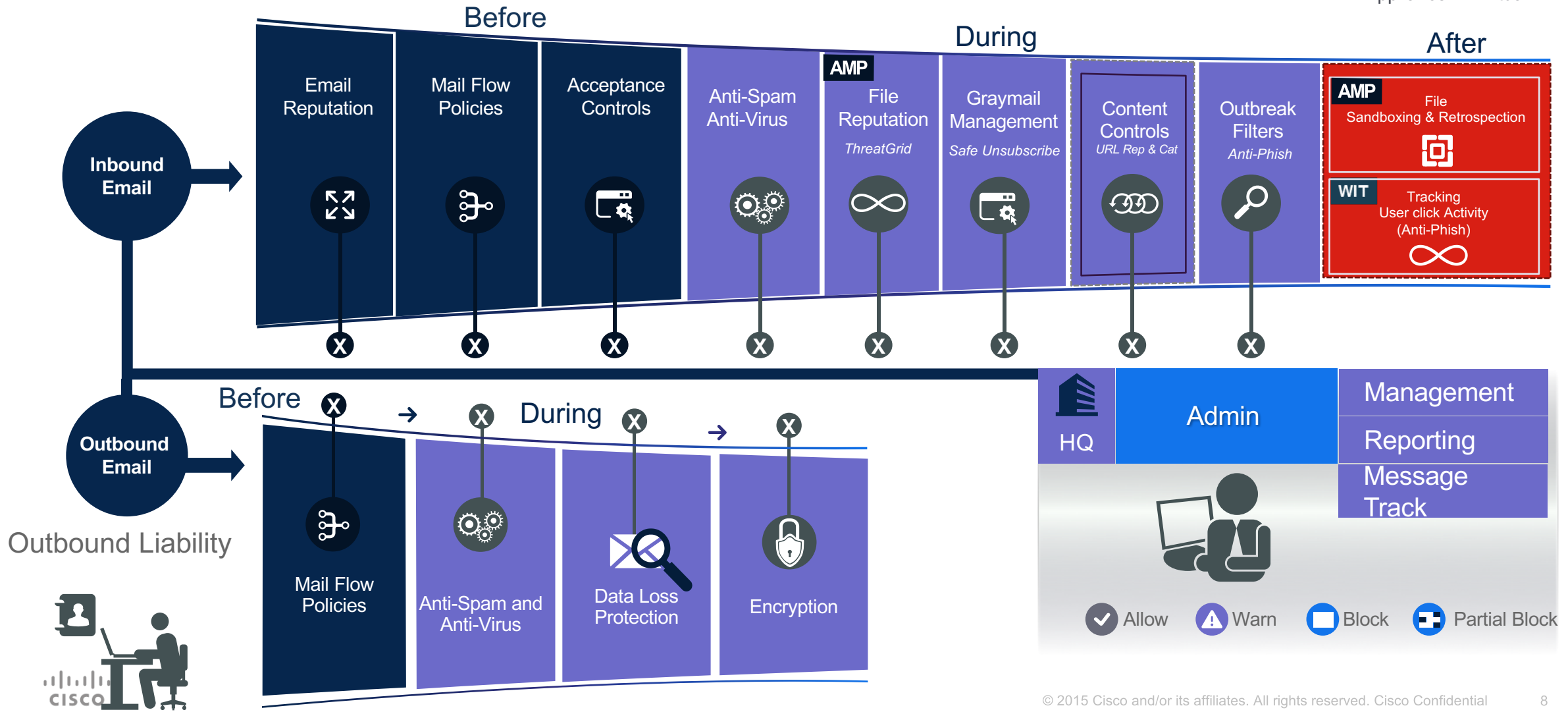
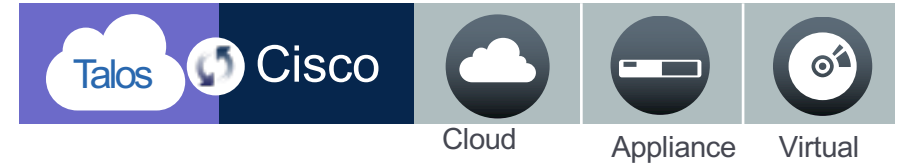
¹2016 Verizon Data Breach Report, Kerbs on Security
²2016 Cisco Annual Security Report

Malware encrypts critical files

Locking you out of your own system

Extortion demands are made

Cisco Email Security



Gain security backed by the most advanced threat intelligence

TALOS



Detect threats embedded in email content

Optimize detection with machine and human intelligence

Stop more than 99% of Spam

Keep good emails flowing with a < 1 in 1M false-positive rate



Guard against malicious attachments

Track email behavior with over 560 indicators

Quickly neutralize threats with Zero Hour Malware Protection

Continuously track files with retrospective security

Anti virus File reputation Advanced sandboxing Retrospective alerting Auto remediation for Office 365 Virus outbreak filters



Reduce the hassle of compliance



Protect intellectual property

- DLP prevents confidential information from leaving your network
- Ensure compliance with industry and government regulations
- RSA and Digital Guardian partnership

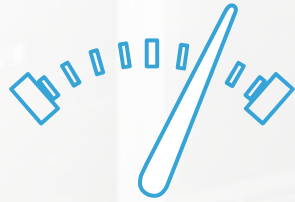


Enable users to do business

Encryption ensures your email is confidential with complete control as the sender

- Send confidential mail
- Read receipts
- Recall ability
- Secure reply and forwarding
- ZIX or CRES or S/MIME or TLS

Move to the cloud with confidence



Maintain peak performance with capacity assurance

- Ensure performance with continuous monitoring of system health
- Count on the stability and reliability of a strong tier one infrastructure
- Add capacity easily as message volumes increase



Avoid downtime with 99.999 availability

- Enjoy the highest levels of service availability with dedicated cloud infrastructure
- Receive dedicated IPs and storage
- Prevent shared-fate with compute instances

Expand with security that grows with you



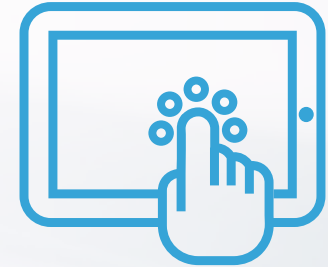
Grow in the cloud

Increase dedicated instances up to 50% of the originally sized environment at no cost



Expand geographically

Utilize Cisco's data center footprint as you grow into new regions



Gain full admin access

- Maintain full admin level access to your appliances at all times
- Easily orchestrate changes or access reports

Optimize security resources to focus on business outcomes



Keep consistent policy as you shift to cloud email



Reduce investigations and response times



Identify trends with scheduled and ad-hoc reporting

AsyncOS 10.0 – Feature rich release



Improved AMP Reporting



Forged Email Detection



Cisco Email Security
AsyncOS 10.0



AMP Private Cloud



Language Detection & Filter Actions



SAML Authentication

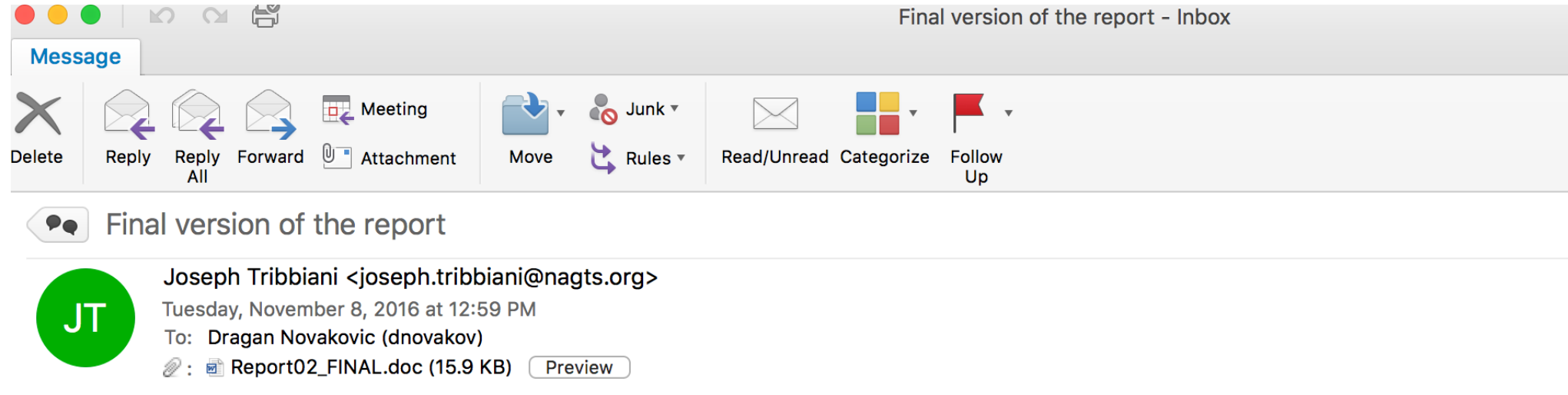


Malware Auto-Remediation
for Office 365 Customers



URL Logging & Message Tracking

Think Before You Click



The screenshot shows an email client window titled "Final version of the report - Inbox". The interface includes a "Message" header and a toolbar with various actions: Delete, Reply, Reply All, Forward, Attachment, Meeting, Move, Junk, Rules, Read/Unread, Categorize, and Follow Up. Below the toolbar, the subject of the email is "Final version of the report". The sender is identified as Joseph Tribbiani with a green circular profile picture containing the initials "JT". The email was sent on Tuesday, November 8, 2016, at 12:59 PM to Dragan Novakovic (dnovakov). An attachment named "Report02_FINAL.doc" (15.9 KB) is listed with a "Preview" button next to it.

Dear Dragan,

Alisha Calderon asked me to send you the attached document, which contains the final version of the report. Please let me know if you have any trouble with the file, and please let Alisha know if you have any questions about the contents of the report.

Kind regards,

Joseph Gibson
Program Mgr, Operations



This is an approved phishing test delivered by the Cisco Information Security team.

You just opened an attachment in a test phishing e-mail. If this was not a test, your action may have exposed Cisco to risk of malware or data compromise. The following signs should have alerted you that this was a phishing email:

- Unknown Sender - unexpected external message, sender does not match name at bottom of e-mail
- Unexpected attachment - unsolicited e-mails with attachments are a common sign of phishing

This phishing sample is based on a real phishing e-mail used to deliver the Locky ransomware and JSDDropper malware. The good news is this - it was just a test. Please visit our Phishpond awareness site, <http://phishpond.cisco.com>, to validate this test, learn about the various types of phishing attacks, and understand how to handle them.

Please send questions or comments about this training program to infosec-phishing-feedback@cisco.com.

What is ransomware?

Ransomware is a type of malicious code that if executed on your system, usually through an attachment or link, will lock your system, encrypt the hard drive, and demand a payment in return for the key to unlock your files. You can protect yourself through the following steps:

1. Do not open unexpected attachments from unknown senders. Exercise caution.
2. Make sure your work and home computers are protected by antimalware software.
3. Enable pop-up blockers.
4. Backup your systems regularly



Some phishing attacks simply need you to click a link in order to launch an exploit against your web browser, infecting your computer with viruses and malware.

We have seen successful phishing attempts against CEOs of Fortune 500 companies, security professionals, IT administrators, customer service representatives, and accountants alike.

Every user **will** be targeted at some point.

With Cisco email security, you can...

Reduce exposure



with advanced threat protection

Support growth



with availability and assurance

Achieve agility



through operational efficiency

Cisco Web Security Solutions



CISCO  SEC

The Cisco SEC logo features the word "CISCO" in a sans-serif font, followed by a stylized fingerprint icon, and then the word "SEC" in a bold, sans-serif font.

Cisco Web Security Protects the Web Vector While Supporting Your Business

Comprehensive
Defense



Advanced
Threat Protection



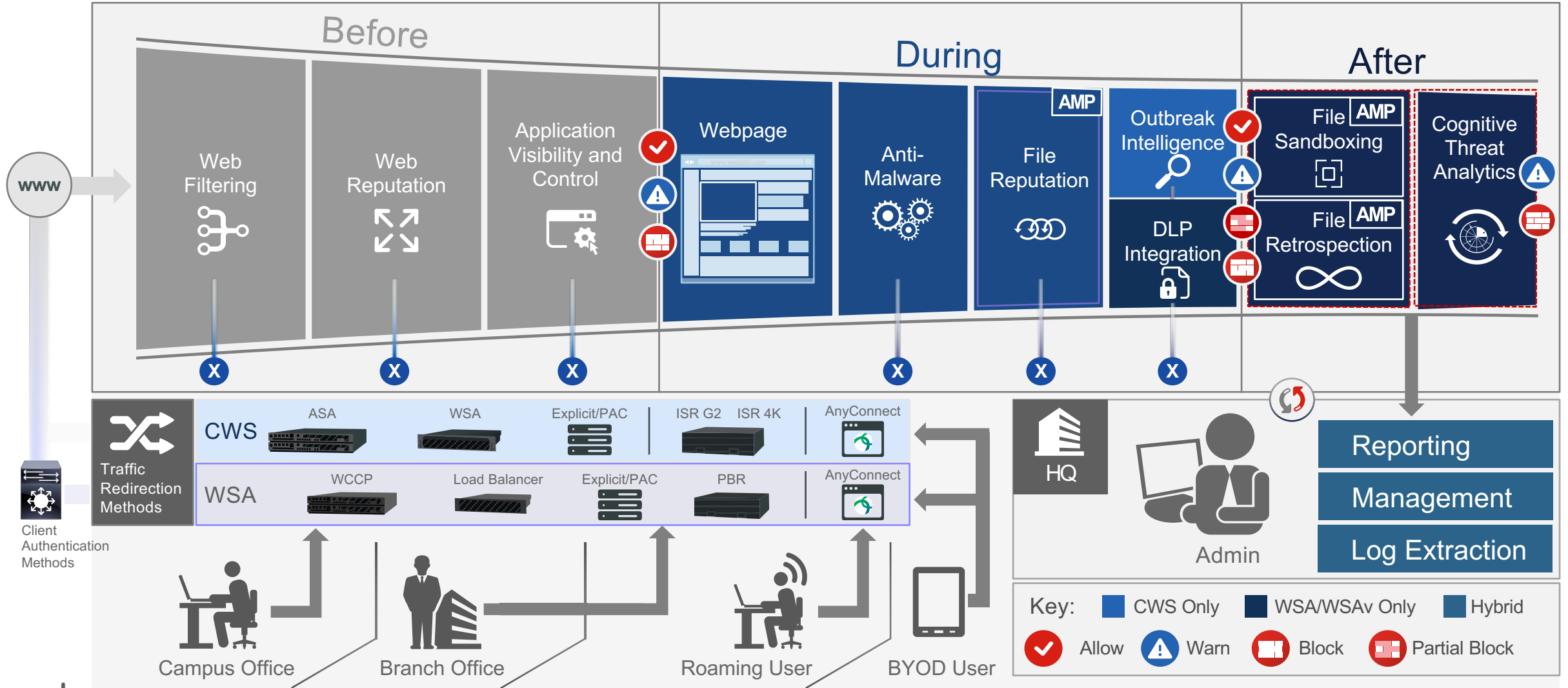
Superior
Flexibility



Cisco Web Security Appliance (WSA)



Cisco Cloud Web Security (CWS)





It Starts with Usage Control and Active Defense



Web Filtering

Block over 50 million known malicious sites



Web Reputation

Restrict access to sites based on assigned reputation score



Dynamic Content Analysis

Categorize webpage content and block sites automatically



Outbreak Intelligence

Identify unknown malware and zero-hour outbreaks in real time



Application Visibility and Control

Regulate access to website components and apps



DLP Integration

Prevent confidential information from leaving your network



Time and Bandwidth Quotas

Set controls for users in terms of time on social media sites as well as bandwidth usage



Roaming User Protection

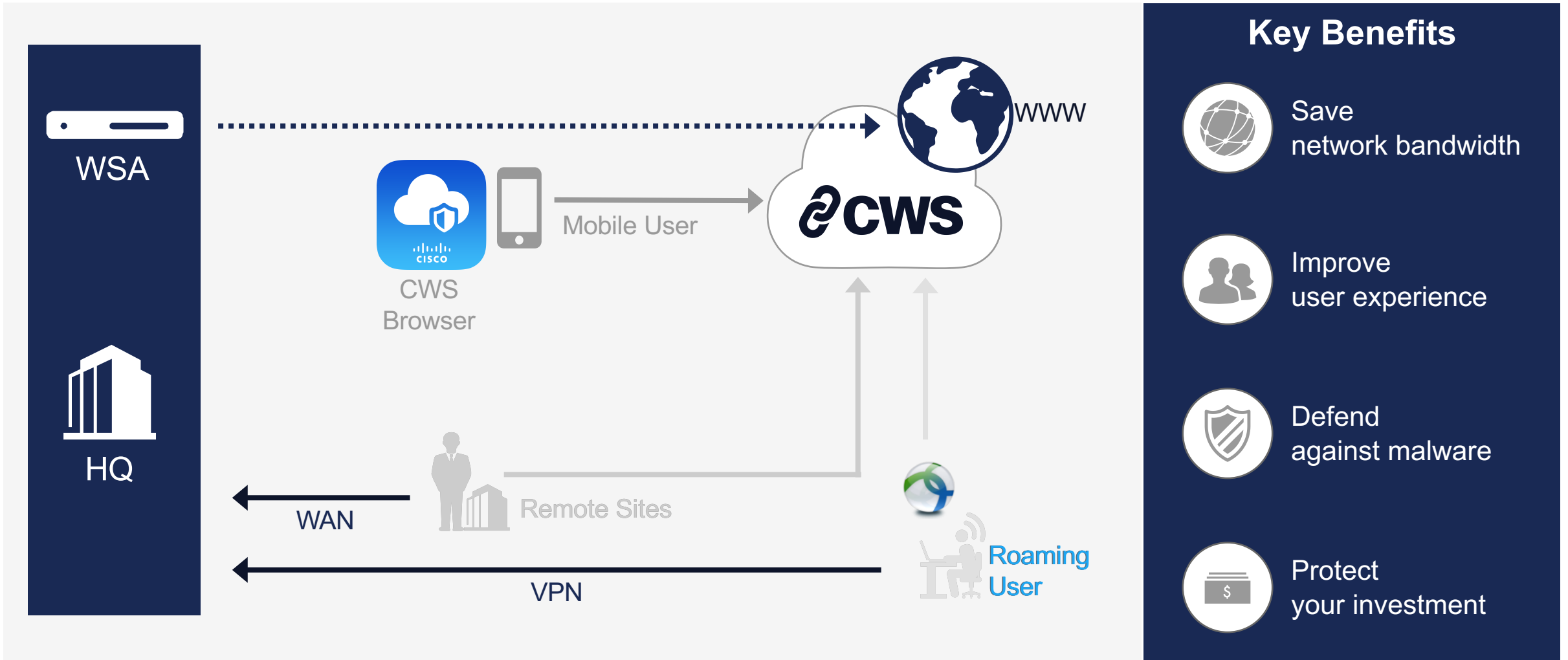
Protect users while away from the corporate network

● Available only on WSA/WSAv

● Available only on CWS



Extending Protection Beyond the Network



Key Benefits

-  Save network bandwidth
-  Improve user experience
-  Defend against malware
-  Protect your investment



And Extending User Identity and Context



ISE Integration

Acquires important context and identity from the network

Monitors and provides visibility into unauthorized access

Provides differentiated access to the network

Cisco TrustSec® provides segmentation throughout the network

Cisco Web Security Appliance provides web security and policy enforcement

● Available only on WSA



Cisco Web Security Combats Evolving Threats

Cisco Advanced Malware Protection (AMP)

File Reputation



Increase the accuracy of threat detection by examining every aspect of a file

File Sandboxing



Determine the malicious intent of a file before it enters the network

File Retrospection



Identify a breach faster by tracking a file's disposition over time

Updating Security to Meet Tomorrow's Challenges



Talos

Security Intelligence
and Research Group

Get industry-specific threat intelligence
tailored to your business

Catch advanced threats endpoints miss with
Cisco's reverse engineers and threat analysts

Stay protected against the latest threats with
regular updates pushed automatically

Threat Intelligence



Research Response



Multi-tiered defense



600+ Researchers

Industry-leading research



Identifying Unnamed Threats and Breaches

Continuous Capabilities with Cisco® Cognitive Threat Analytics (CTA)

000 0100010111011 10010001101 010 001 001101 00111 0100 111001 1001 11 111 0 01000 01010 1110  0111100 011
 1010011101011101001110100011101010
 01000 01000111 0100 1110101001 1101 111 0011 101001 110011 100 01111 001101 00111 0100 00 011 1010011101 01001110 001101 00111 0100 0001
 110001100
 100 011101001 110011 100 01111 01100 011 1010011101 100101001 110011 10  0 0111010011101 10001110 10011 101 010011101 1100001110001110 1000111011
 01000 0100 0111 0100 11101 100 00111011010101110101001 110011 100 01111 010011101 10001110 10011101 1100001 1100 011101001110100010100100010001111



Anomaly Detection

Detect infections faster by automatically scanning for symptoms of an attack



Behavioral Analysis

Identify unknown breaches by analyzing a user's behavior over time

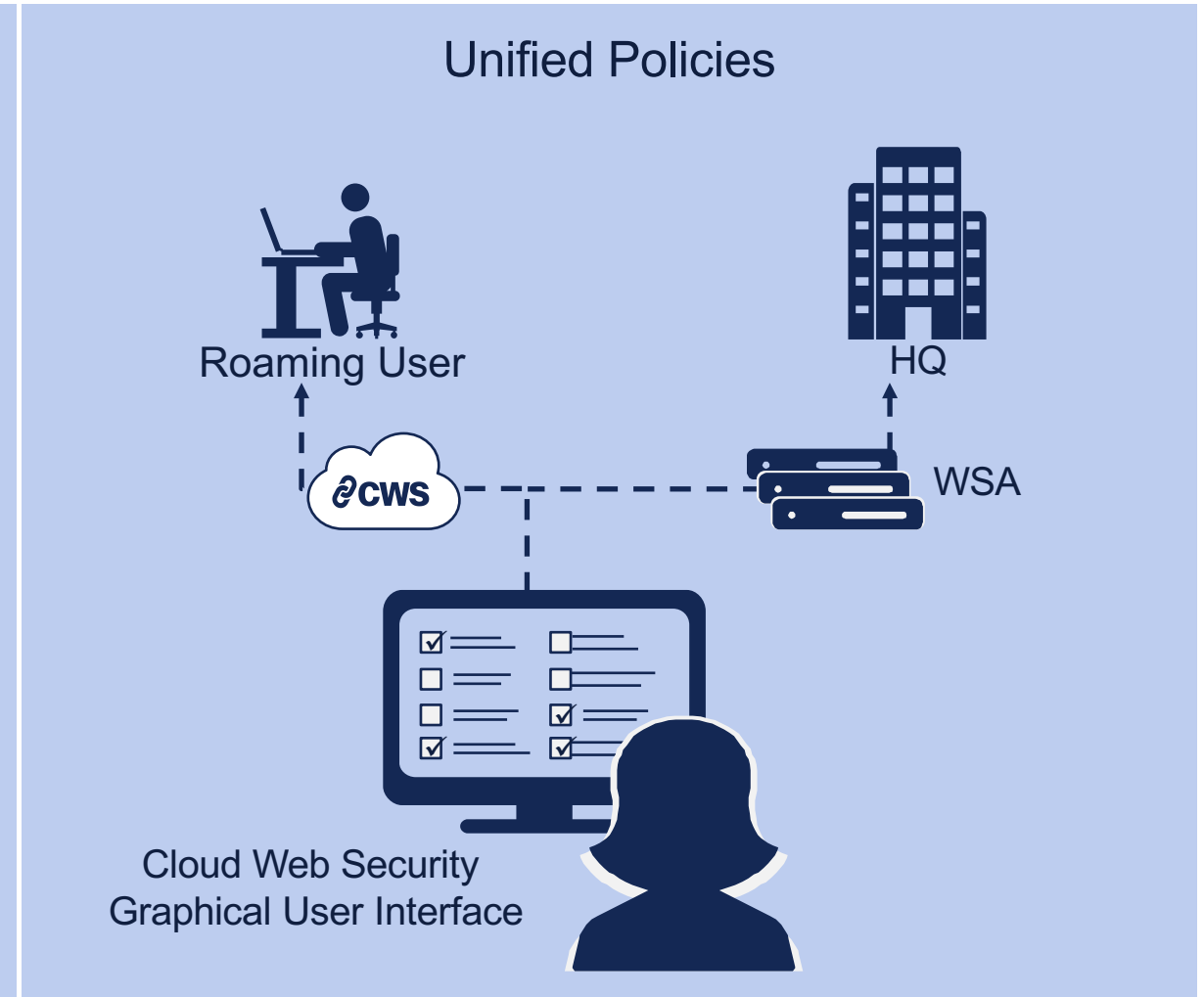
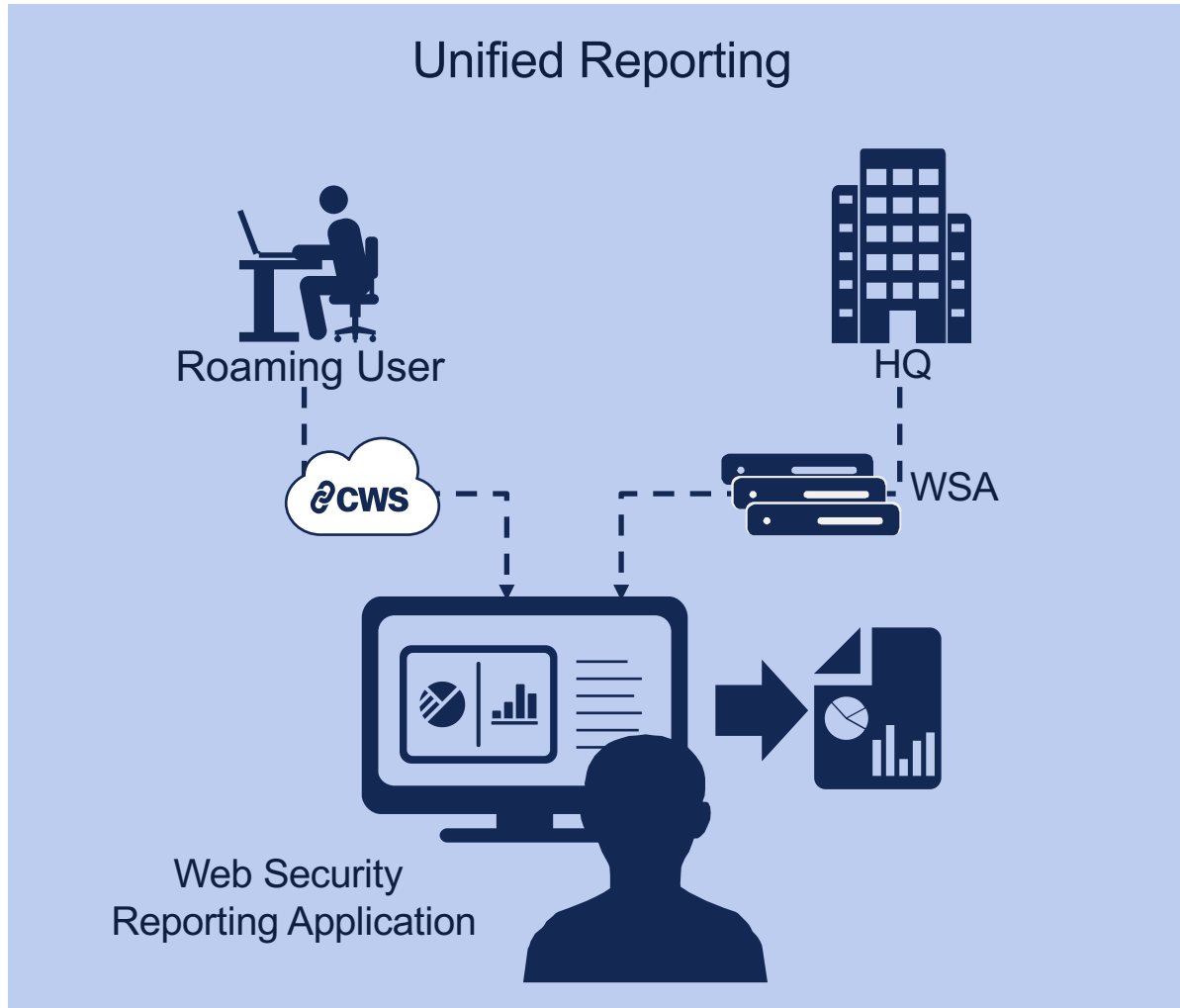


Machine Learning

Automatically learn and adapt to threats with big-data algorithms



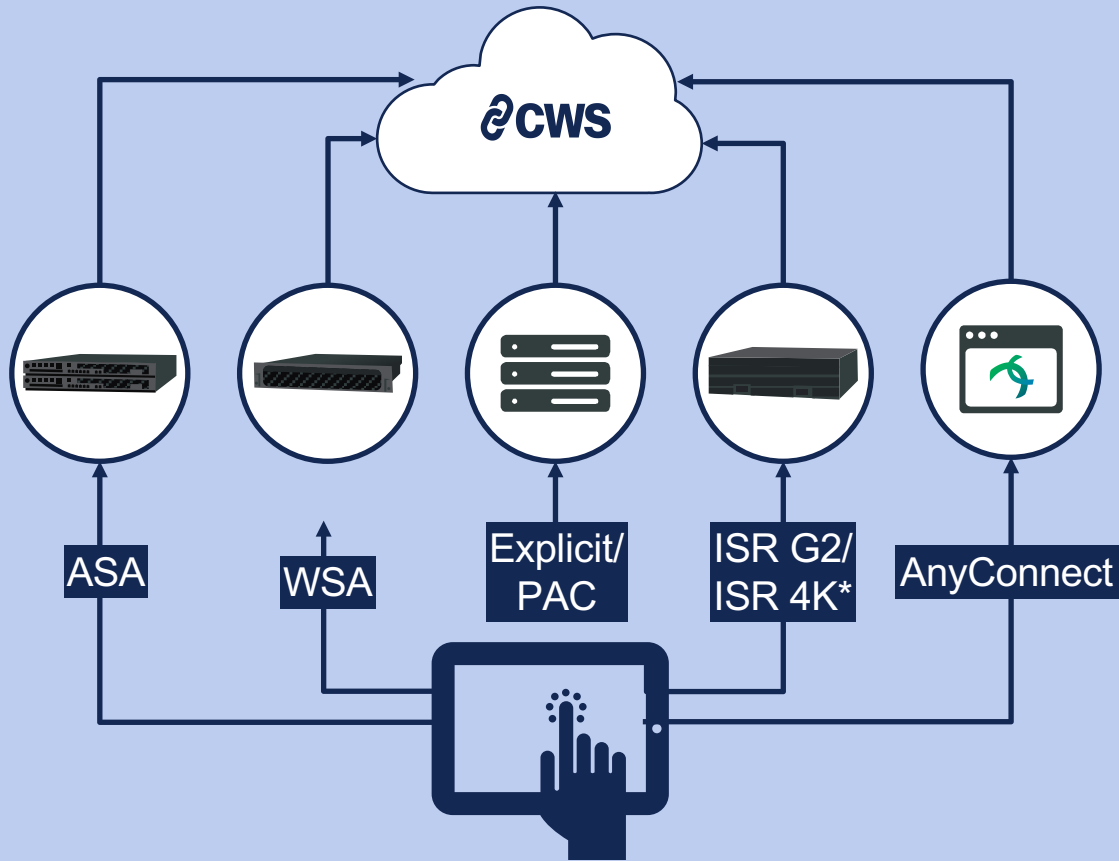
With Unified Reporting and Policy Management





And Work with Your Existing Environment

CWS Traffic Redirectors



WSA Models

Physical Appliance

Perfect for small
business branches



WSA-S190

Perfect for
mid-size offices



WSA-S390

Perfect for large
enterprises



WSA-S690

Virtual Appliance (WSAv)

Respond instantly to traffic spikes and eliminate
capacity planning by never shipping or installing
a physical appliance

*GRE over IPsec

Only Cisco Offers Web Security with Advanced Threat Protection





Thank you

