CISCO
SECURE

A Cloud Security Workshop

Zero Trust Architecture

Jan 2023

The bridge to possible

These last three years have transformed the nature of remote work and hybrid work

We are in a period of unprecedented uncertainty. Supply chain challenges, the war in Ukraine, rising costs

Small and Medium Businesses are scrambling to keep themselves safe

Proverb: "May You Live In Interesting Times"

Cyberattacks on businesses large and small are on the rise

For Cisco's customers this period is both a challenge and an opportunity

The scale and scope of Cisco's investment In security has never been greater.

And as a customer you can leverage that in service of your business

Objectives

- The Cybersecurity challenges businesses face
  - Through the story of an attack on a company called Code4U
- Cloud Security with Cisco Umbrella
- Zero Trust solutions and Cisco DUO
- Introduce you to two gentlemen who can assist you with your security needs

Into the Cloud

Jasmine C.
Head of IT – Code4U

- Code4U, a contract coding company, was recently hit with a ransomware attack.
- As a result of the attack, they are actively re-evaluating their entire security infrastructure.
- Code4U has three locations and the bulk of their applications are cloud based
- Due to their size, Code4U is working with Cisco Partner, Skyline-ATS

Into the Cloud

- Jose Mock is a rep with Cisco Partner, Skyline-ATS, who specializes in Cisco Security products.
- Skyline-ATS has a focus on Cisco Security products
- This is his 1st meeting with Jasmine.

Jose Mock
Skyline ATS

“Jasmine,
So sorry to hear about your recent ransomware attack.”

Jasmine C.
Head of IT – Code4U

“Thank you. We are re-evaluating everything.”

“Based on your experience we’re going to discuss the ransomware lifecycle. And how it applies to businesses like yours.”

And then we’ll discuss two simple products you can implement today – Umbrella and Duo

“You have my interest.”

Jose Mock
Skyline ATS

A proven networking and security innovator

2022 Overall Cloud Security (SASE) Market Leader
Dell'Oro

2021 WAN Edge
Gartner Magic Quadrant

2021 Best Security Company
SC Media

Securing **100%** of the Fortune 100

80% of the internet traffic through Cisco's infrastructure

Cisco = Comprehensive **End to End** Security

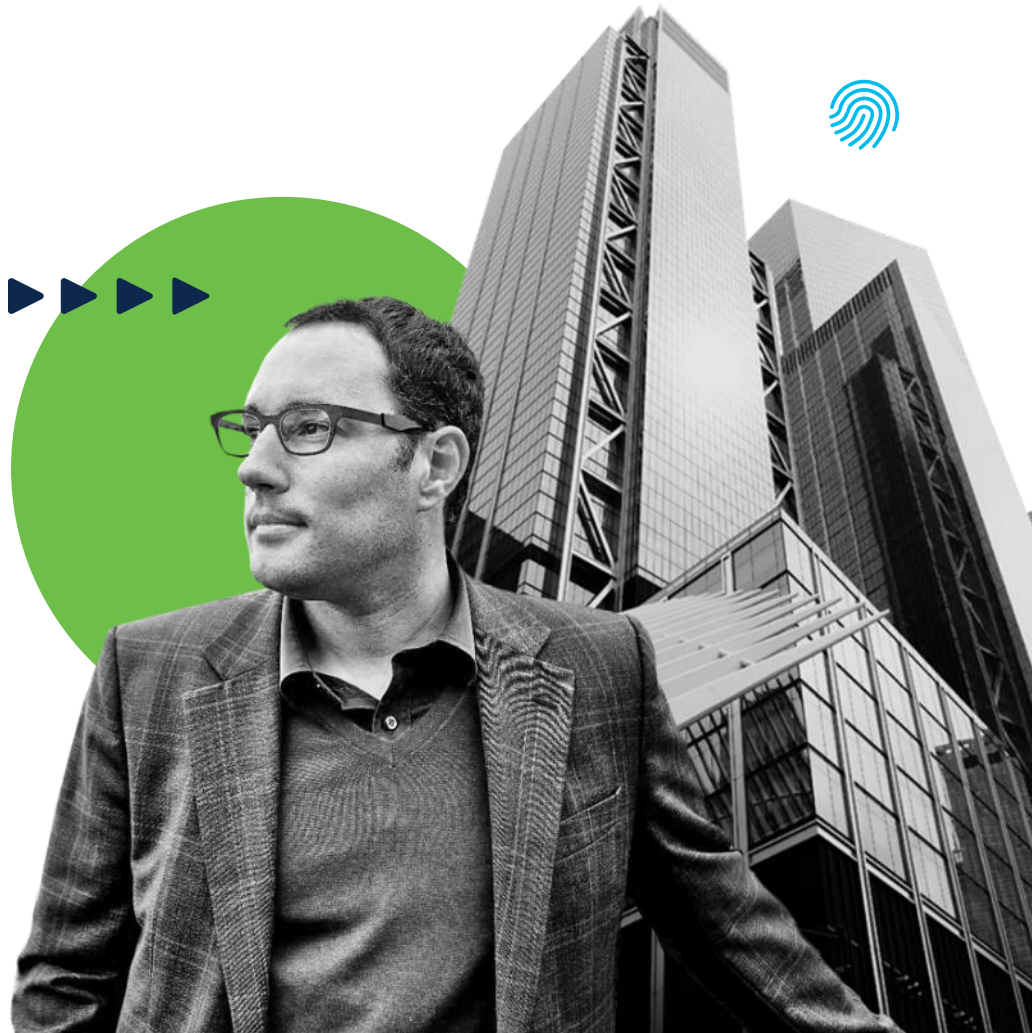
Over $1 Billion in Firewall sales

840k+ networks protected

40k+ WAN Edge customers

Backed by World-Class Talos Intelligence & Incident Response

Cyberattacks and Ransomware



Why Ransomware?

POLITICS

U.S. banks processed billion in ra

LIVE LOCAL

Growth in ransomware damage and costs worldwide

US$325 MILLION (2015)
US$5 BILLION (2017)
US$11.5 BILLION (2019)
US$20 BILLION (2021)

FinancesOnline REVIEWS FOR BUSINESS

Source: Cybersecurity Ventures

Yet ANO
a million
massive multi-state healthcare IT breach
delays and ambulance diversions

- Have YOU or anyone you know been impacted by these cyber-hacks?
- OakBend Medical Center said 500,000 individuals were aff
- Cybercrime group Daixin Team claimed responsi
- They claimed to have over a million pati
- The hospital group is being sued b

lion to end
ecord

s reported the previous year.

pected Russian cyber

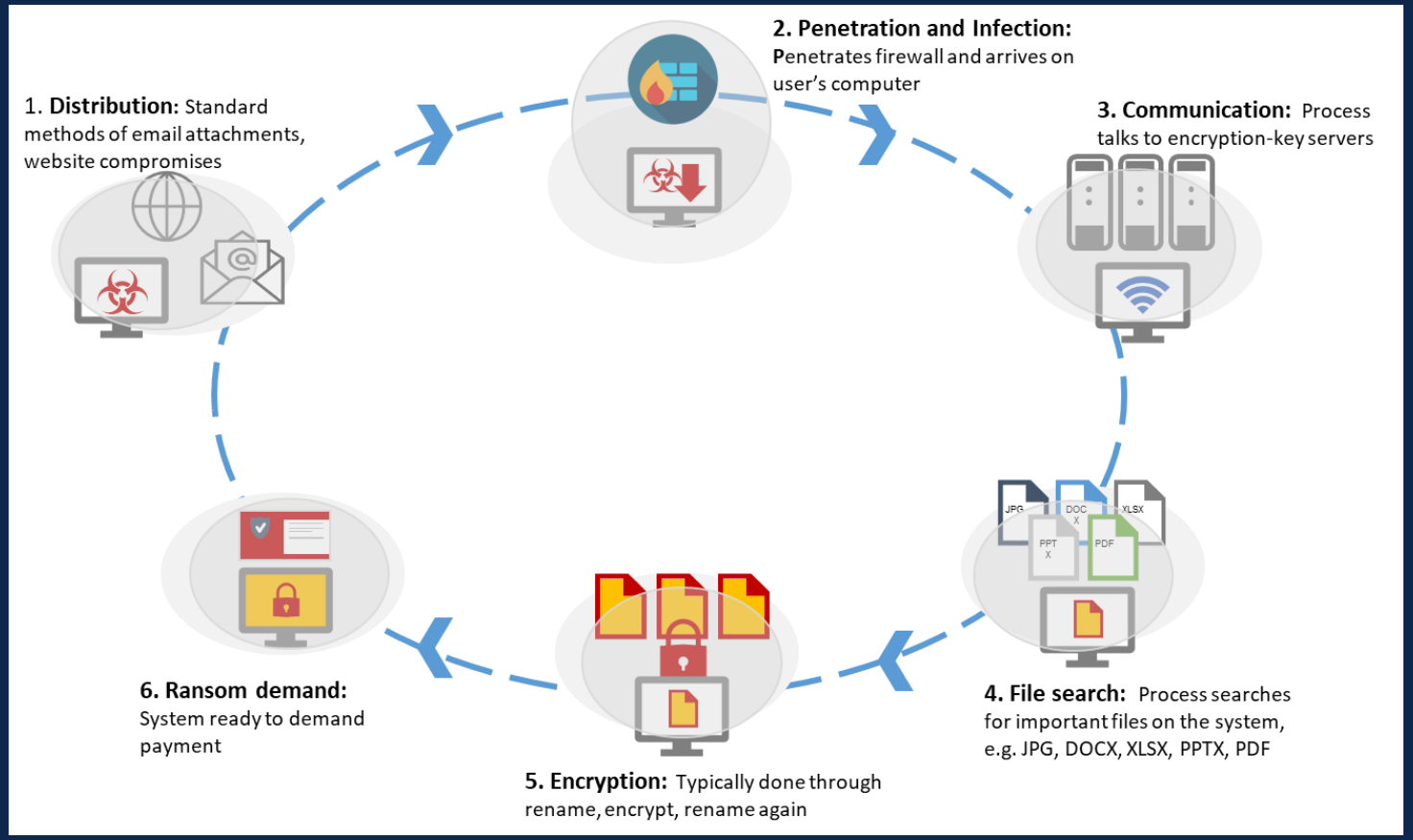
comparitech

Ransomware attacks on US schools and colleges cost $3.56bn in 2021

Ransomware Lifecycle

Six Steps of a Ransomware Attack

- Distribution
- Penetration/Infection
- Communication
- File Search
- Encryption
- Ransom Demand



Ransomware Sequence

Six Steps of a Ransomware Attack

Distribution

- Email is the primary attack vector
- Malware docs (pdfs, word doc, attachments)
- URLs. Click on a URL and you are accessing malware
- Compromised login credentials

Ransomware Sequence

Six Steps of a Ransomware Attack

Penetration/Infection

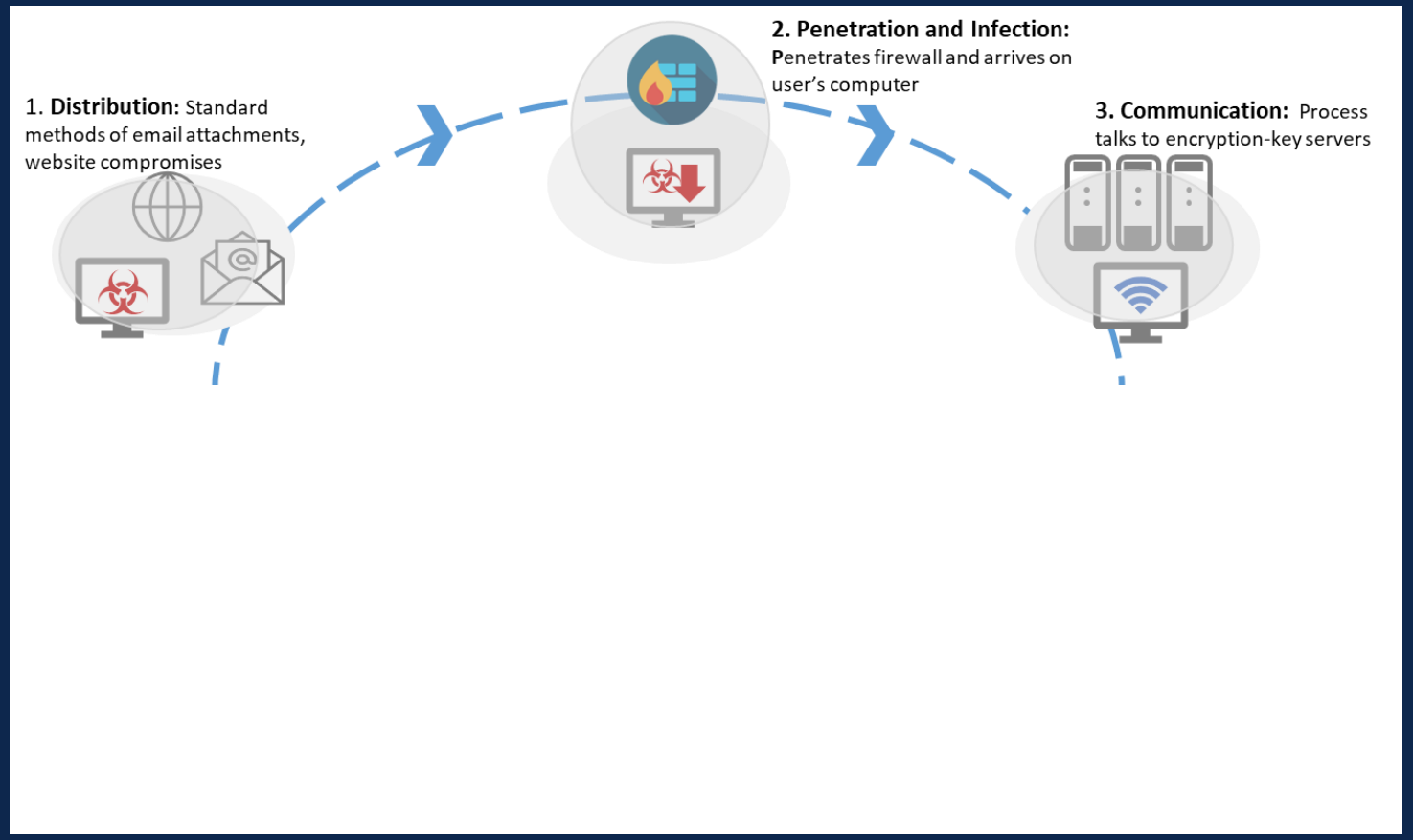
- The malware passes through the firewall and is introduced onto the target device (laptop, desktop, server)
- The firewall does not recognize the malware as malware
- Some standard anti-virus software may be able to stop some infections
- Typically, more sophisticated Malware Detection is needed

Ransomware Sequence

Six Steps of a Ransomware Attack

Communication

- Once malware is on the machine, it will then connect out to command and control (C2) servers to download additional malware and an encryption key
- DNS (Domain Name Server) protection would be able to block the process

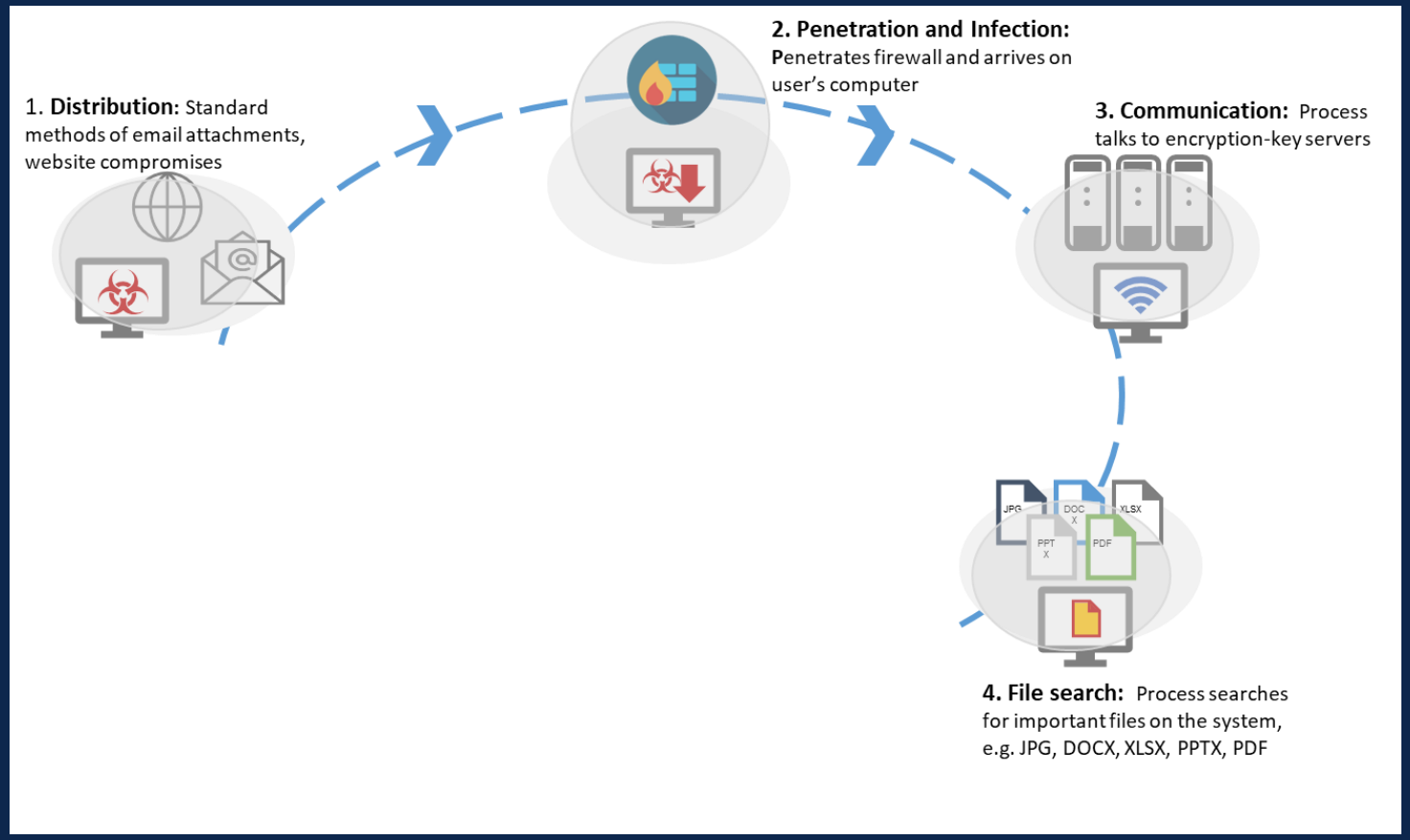


Ransomware Sequence

Six Steps of a Ransomware Attack

File Search

- The malware will attempt to escalate privilege
- The malware will then move through the network laterally and gather any and all sensitive data that can be used to blackmail the organization or individual
- The data will then be exfiltrated to the command and control (C2) server

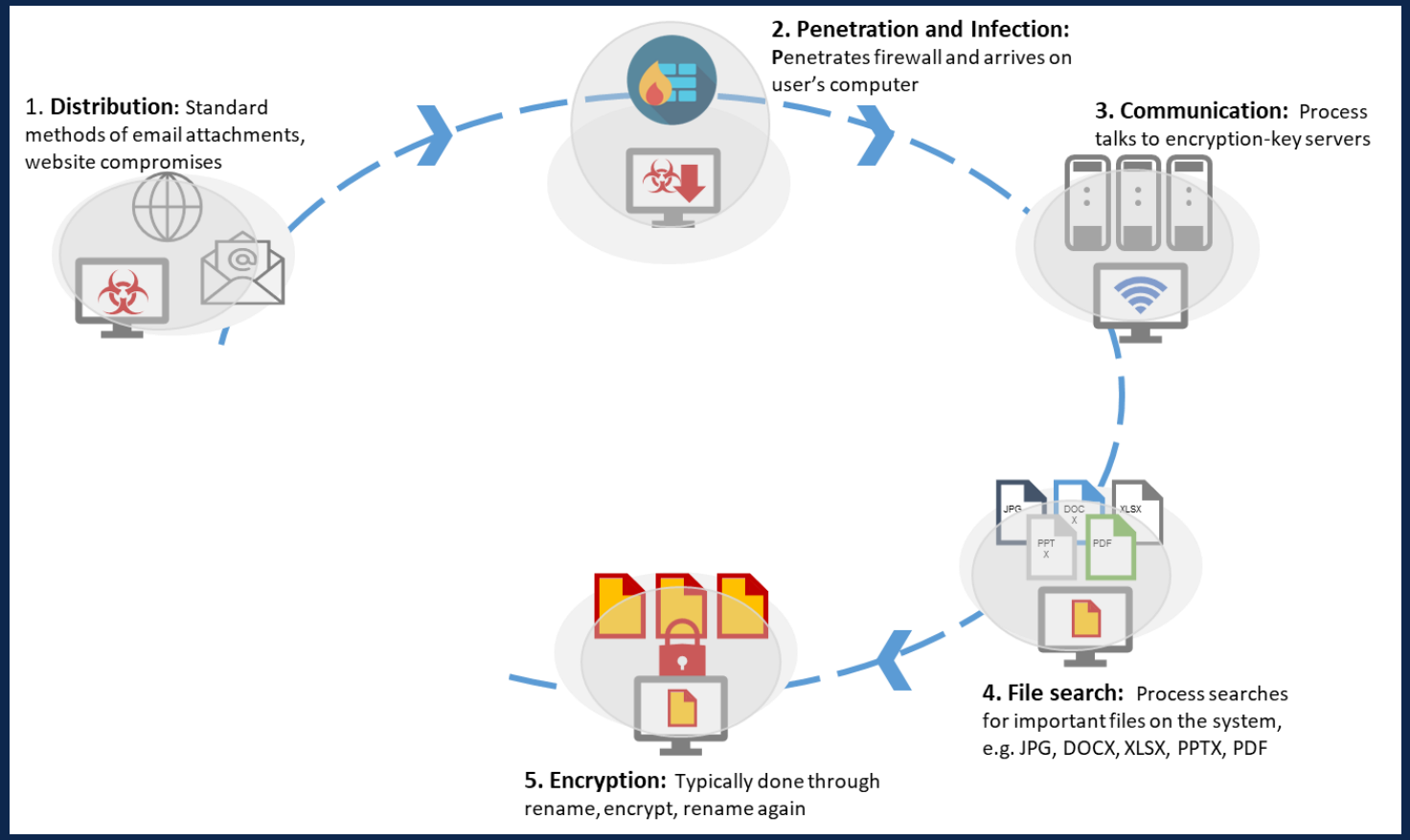


Ransomware Sequence

Six Steps of a Ransomware Attack

Encryption

- After sensitive data has been exfiltrated, the malware will then activate the encryption keys downloaded from the command and control (C2) server

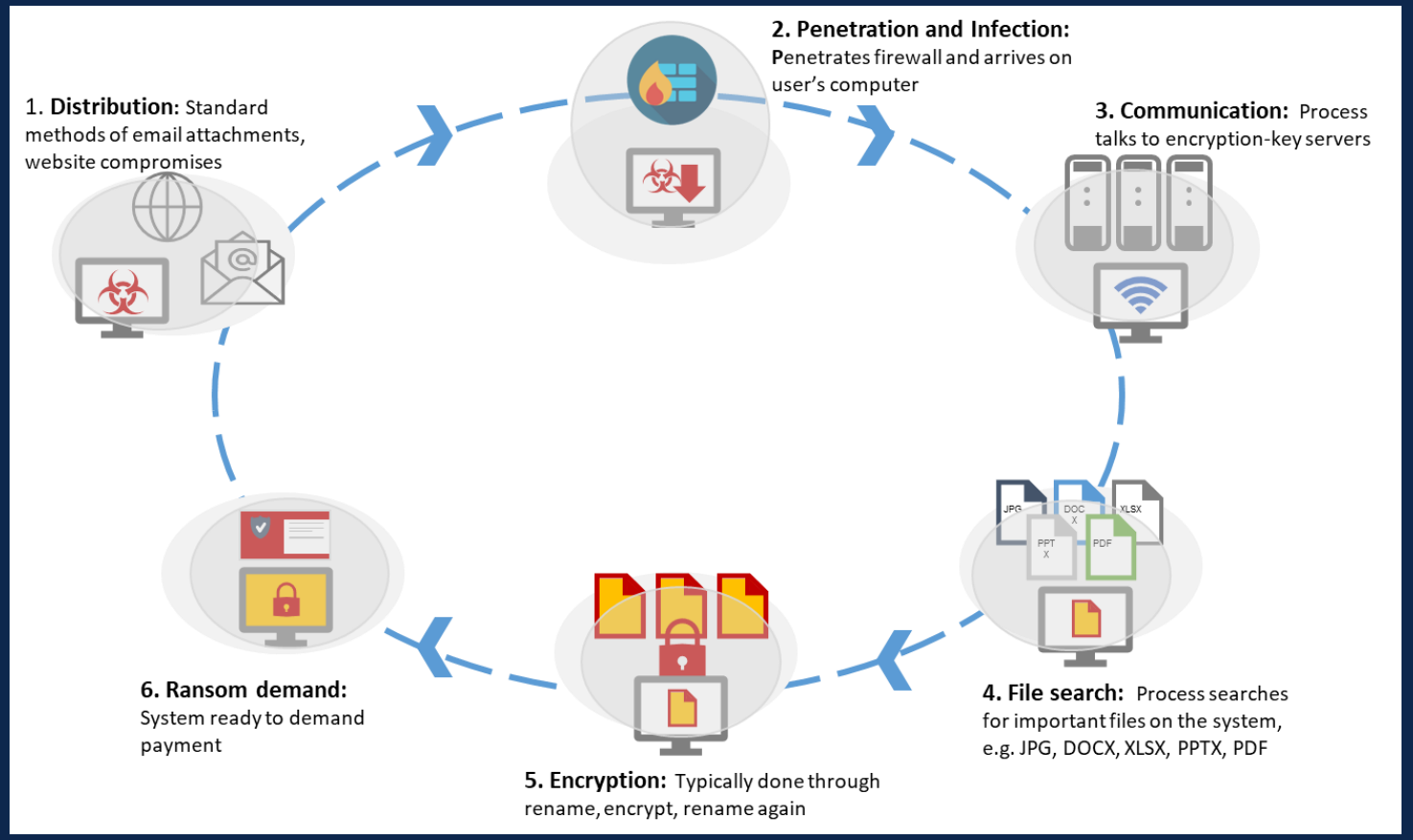


Ransomware Sequence

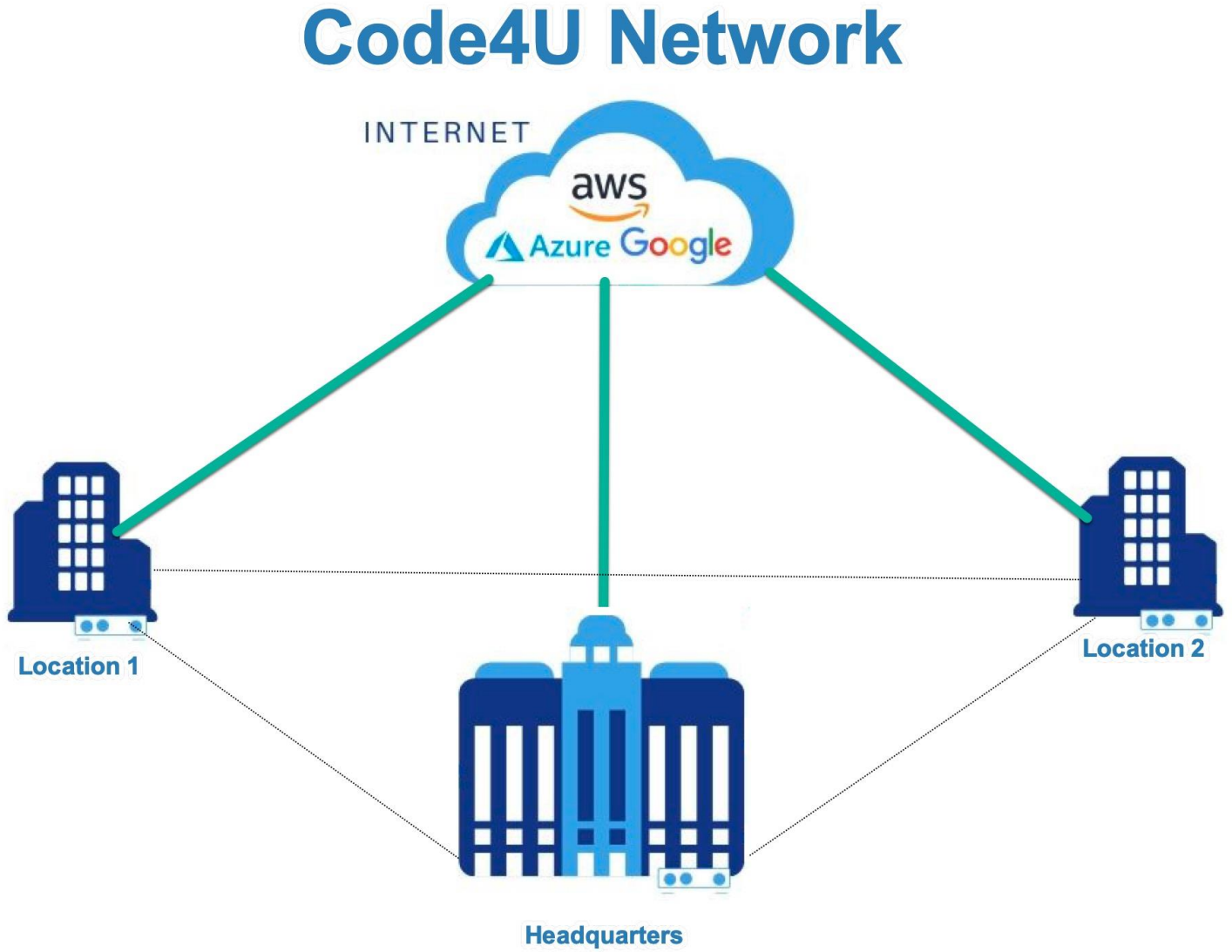
Six Steps of a Ransomware Attack

Ransom Demand

- At this point, the hackers demand a ransom to unlock the encrypted files and systems
- As insurance, hackers will threaten to release the exfiltrated data



- 3 Locations
- Each location connects directly to the internet
- In addition, 55 contract and remote workers spread throughout the region



Issue #1

The data and resources are in the cloud.

The people are everywhere. How to access safely?

Issue #2

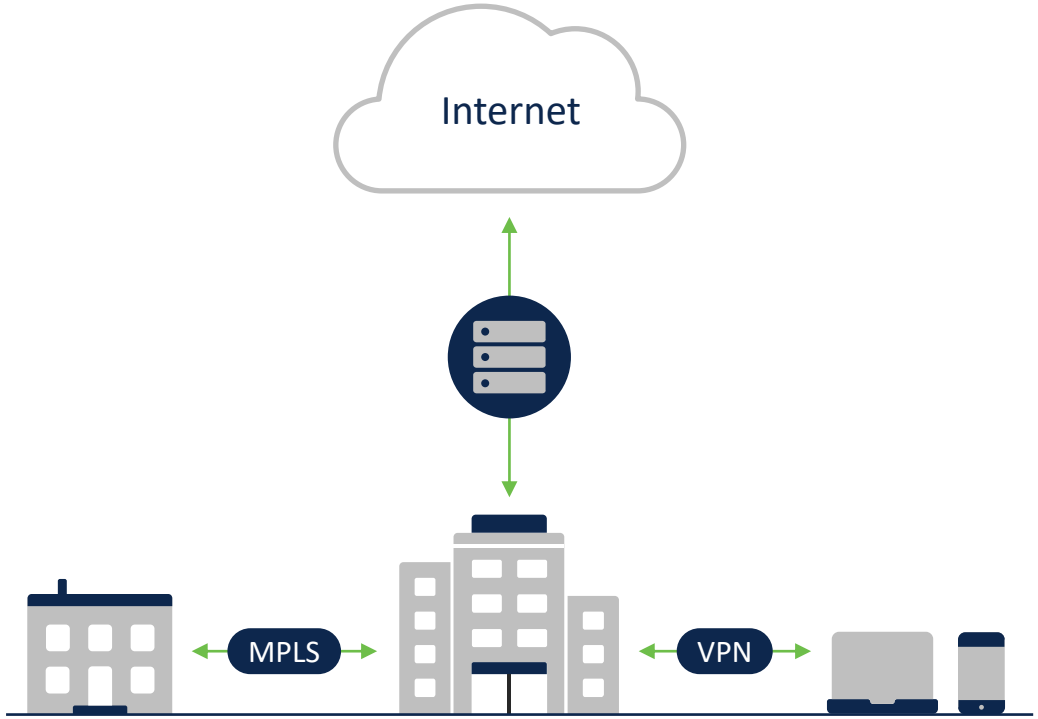
How to provide firewall type inspection of incoming and outgoing traffic when the users are no longer centralized?

Issue #3

Even "safe" websites may contain links that connect to malware. How do we allow employees to browse with confidence?

Network transformation

Before



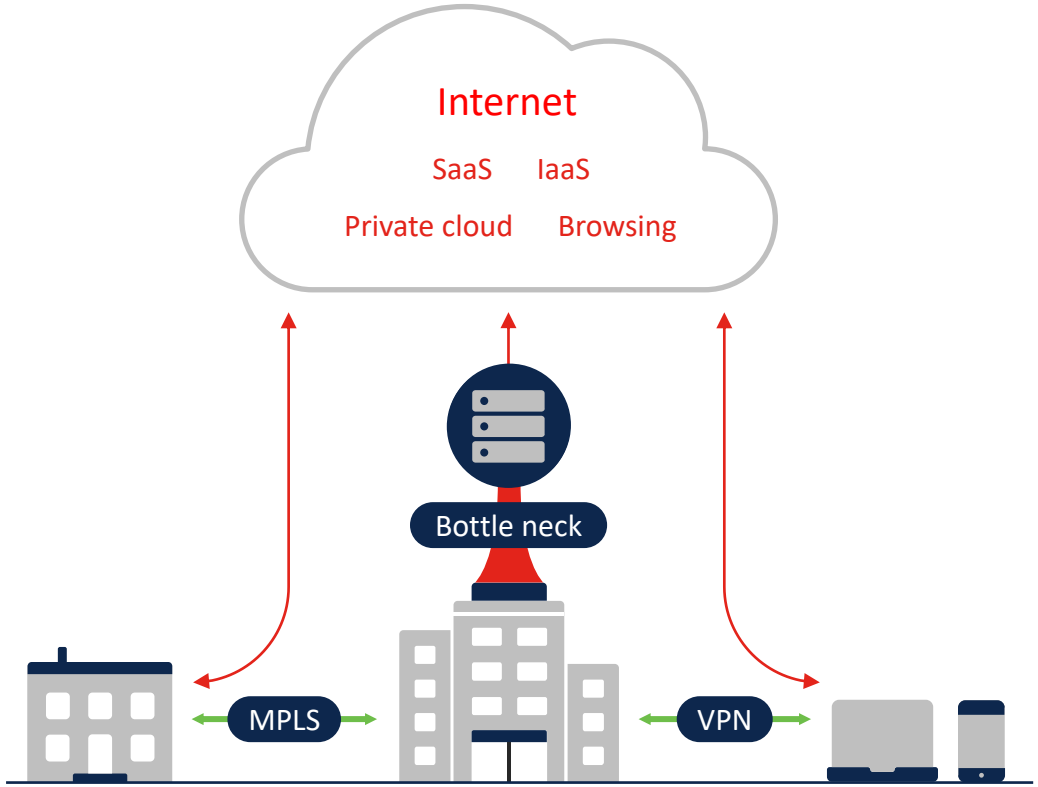
Apps: Hosted in datacenter

Users: Connected to corporate network to work

Network: Centralized

Security: On-premises security stack

What's changed



Apps: More hosted in the cloud

Users: More work done off-network

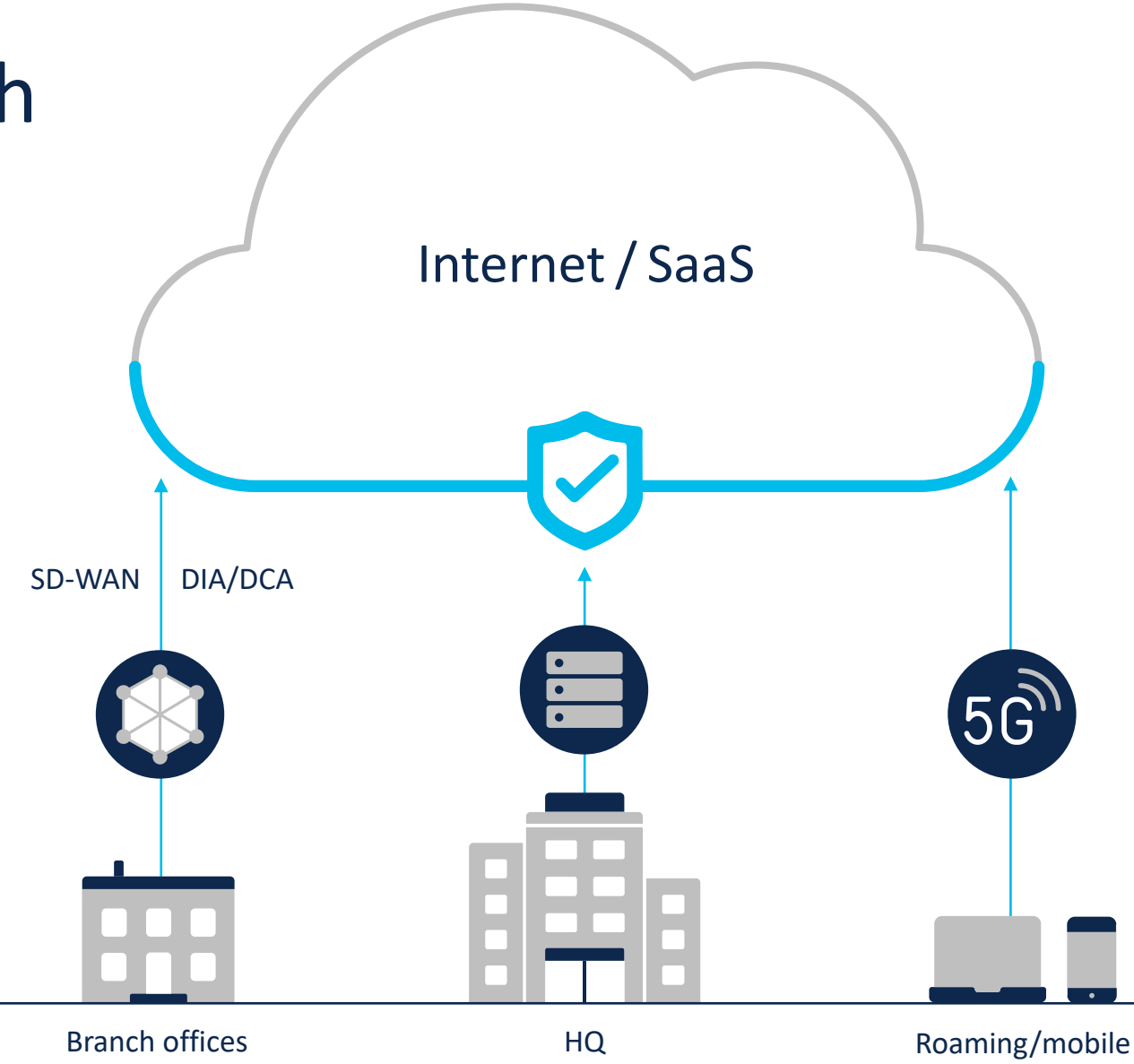
Network: De-centralized

Security: Gaps in protection

A more modern approach

Security:
Enforced at the cloud edge

Network:
Optimized routing from anywhere to the cloud

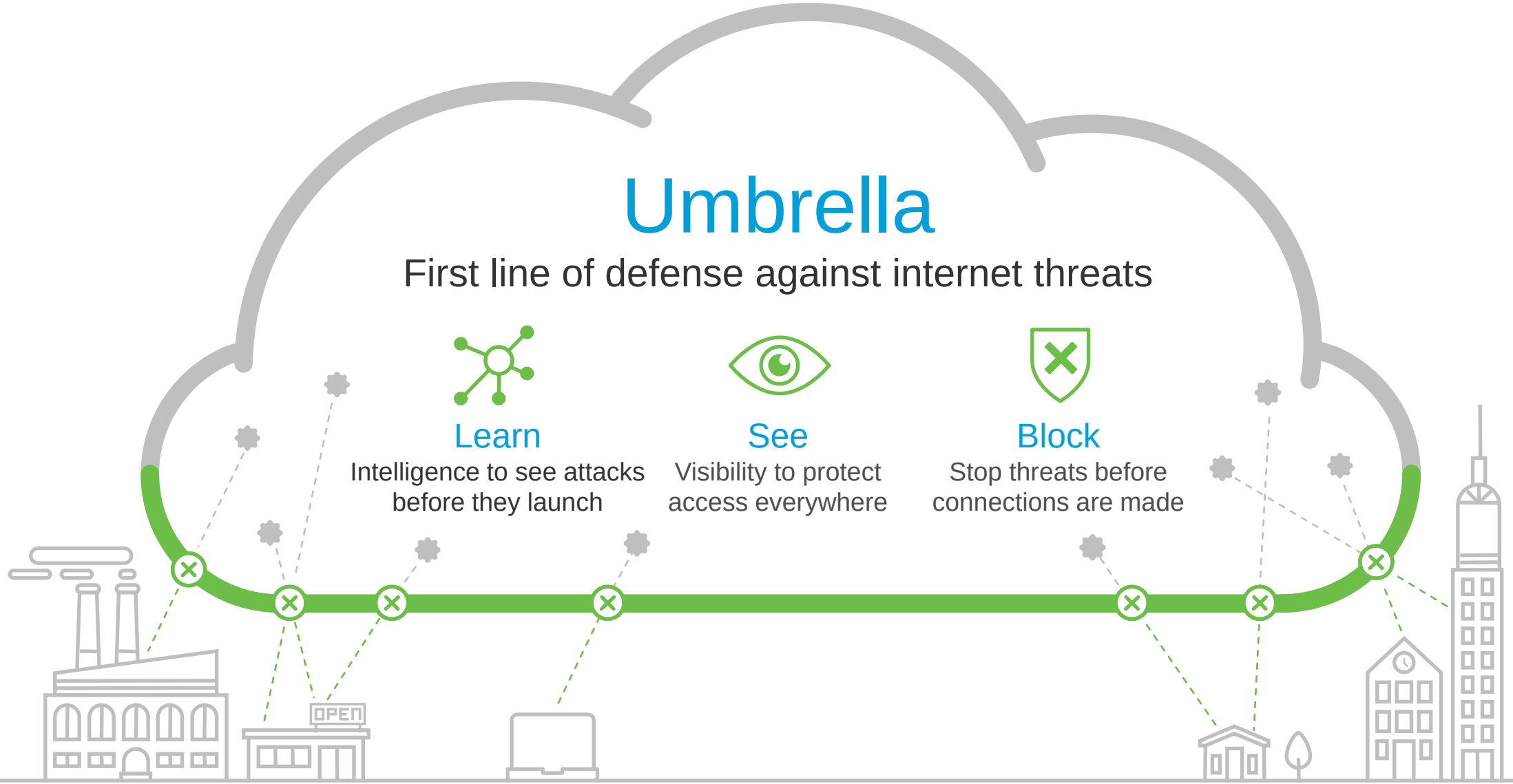


Cisco Umbrella

Secure access to the internet

Umbrella

First line of defense against internet threats



Learn

Intelligence to see attacks before they launch

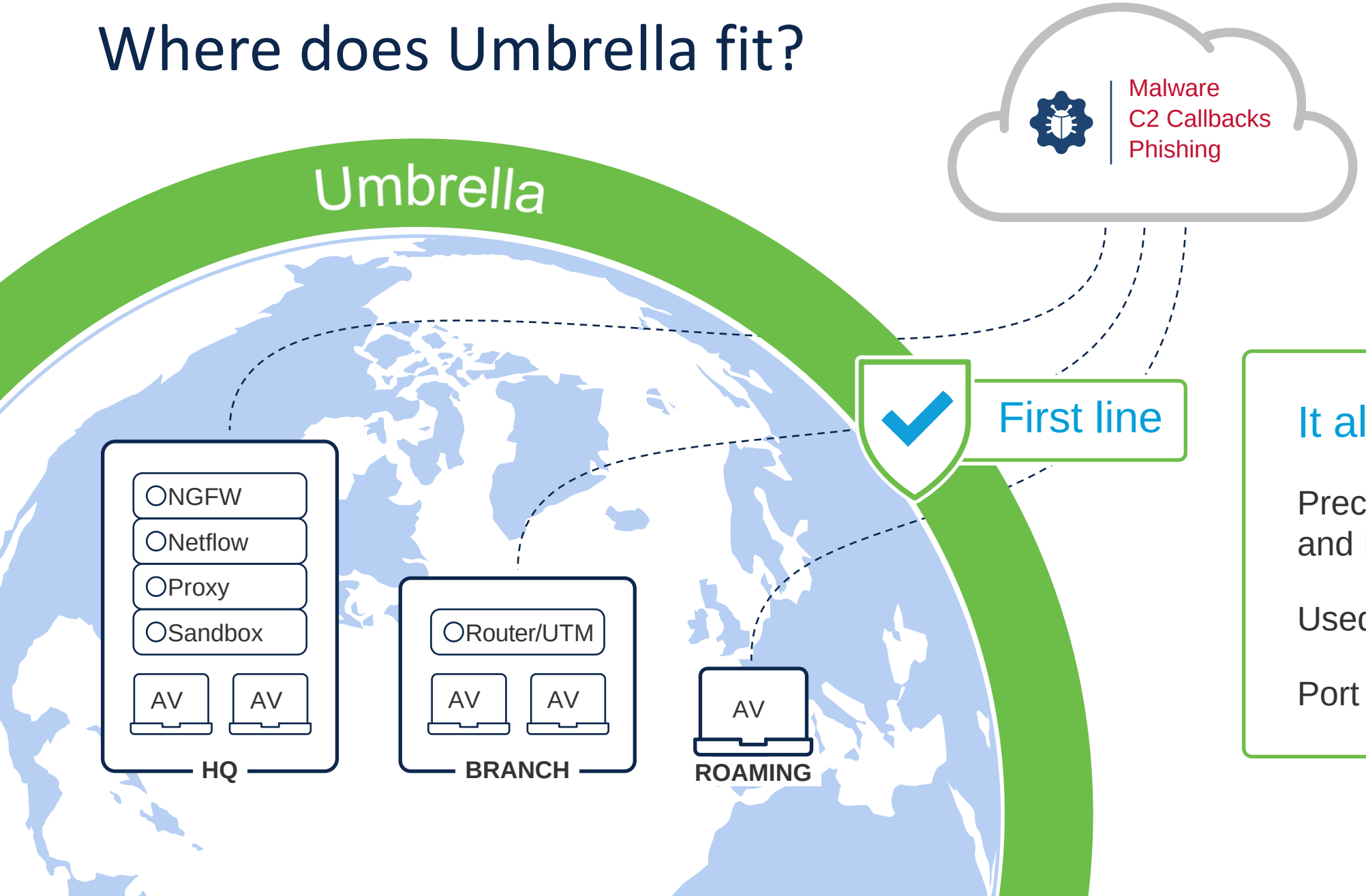
See

Visibility to protect access everywhere

Block

Stop threats before connections are made

Where does Umbrella fit?



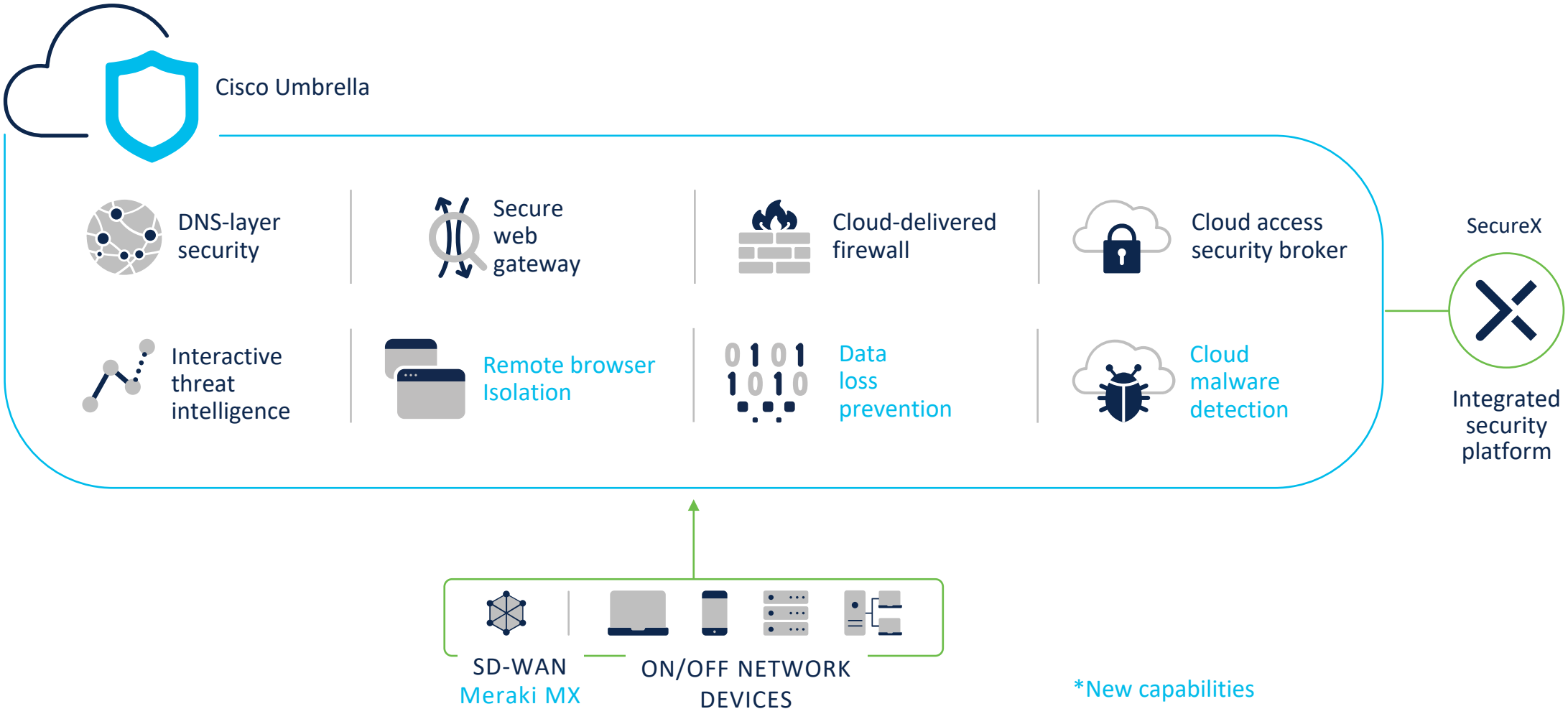
It all starts with DNS

Precedes file execution and IP connection

Used by all devices

Port agnostic

Cisco Umbrella



*New capabilities

Umbrella cloud-delivered firewall

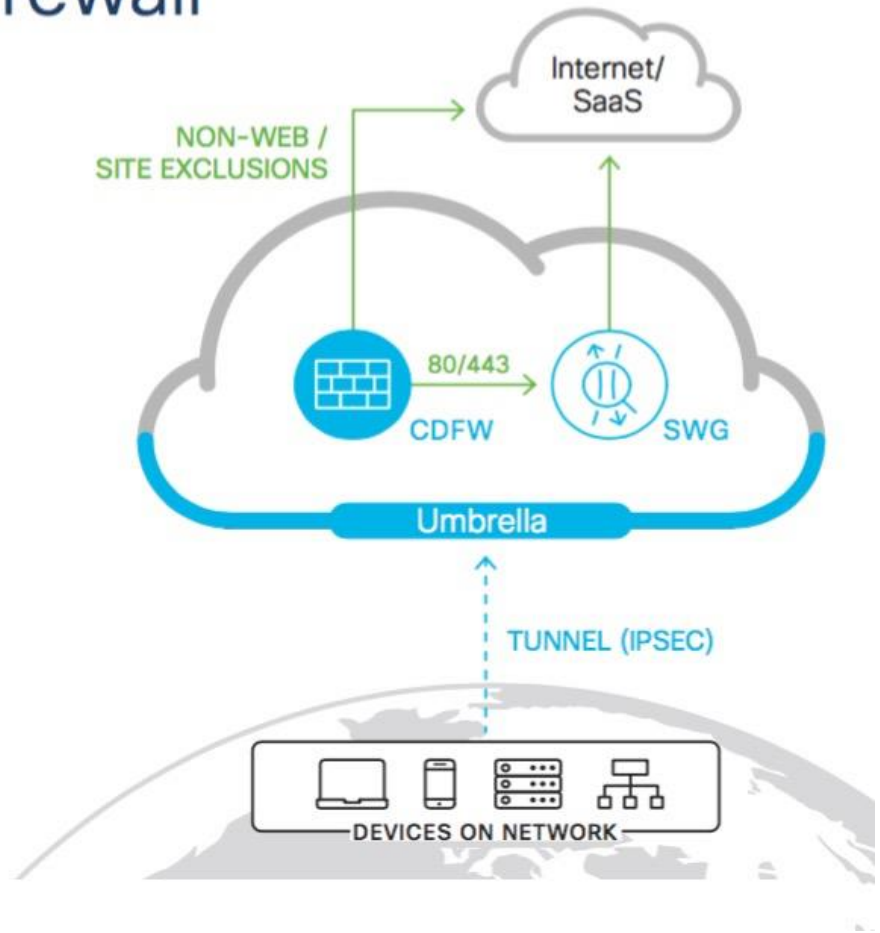
Layer 7 Application Visibility and Control

Block high risk, non-web applications and protocols (Layer 7 application visibility and control / AVC)*

Centrally manage IP, port, and protocol rules (Layer 3 / 4 and 7)

Tunnel all outbound traffic to Umbrella

Transparently forward web traffic on ports 80/443 to secure web gateway



Application visibility and control

Extends across enforcement points

DNS-layer security

- Visibility into cloud apps used in organization
- Identify potential risk and block specific apps (16K apps discoverable)

Secure web gateway

Granular control of web apps over HTTP/S (ports 80/443):

- Block uploads to cloud storage apps
- Block posts/shares to social media apps
- Block attachments to webmail apps
- Tenant restrictions

Cloud-delivered firewall

- Layer 7 Application Visibility and Control *
- Extends visibility, protection, control to:
  - Non-web (non-HTTP/S) traffic
  - Apps not performing DNS lookup
  - Apps that use hard-coded IP addresses and do not perform DNS lookup
  - Apps where signature-based detection (not based on IP, domain, URL) is required to detect and block

*Limited availability

Data loss prevention

Challenge

More cloud application usage leads to higher risk of malicious or inadvertent sensitive data loss

Data loss prevention

Capabilities

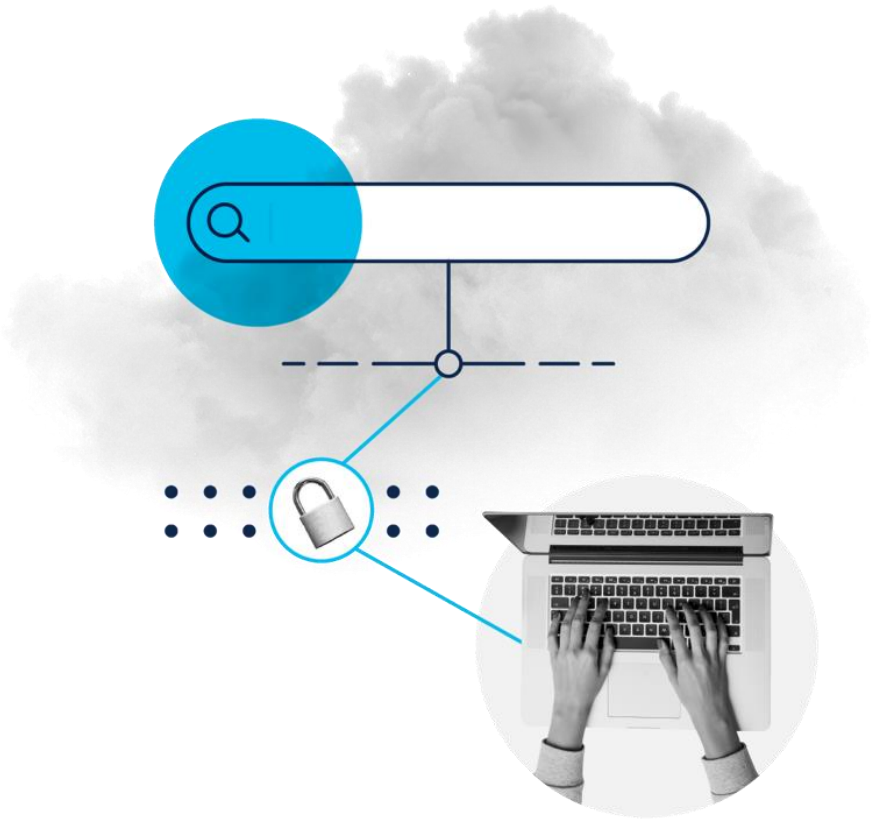
- Monitor and enforce in real time
- Inspect data in-line with full SSL inspection
- Create flexible policies with 80+ pre-built dictionaries (customizable)
- Provides detailed incident reporting

Results

- ✔ Discover and block sensitive data being transmitted to unwanted destinations
- ✔ Prevent data exfiltration
- ✔ Support compliance mandates

Limited Availability

cisco SECURE



Remote browser isolation

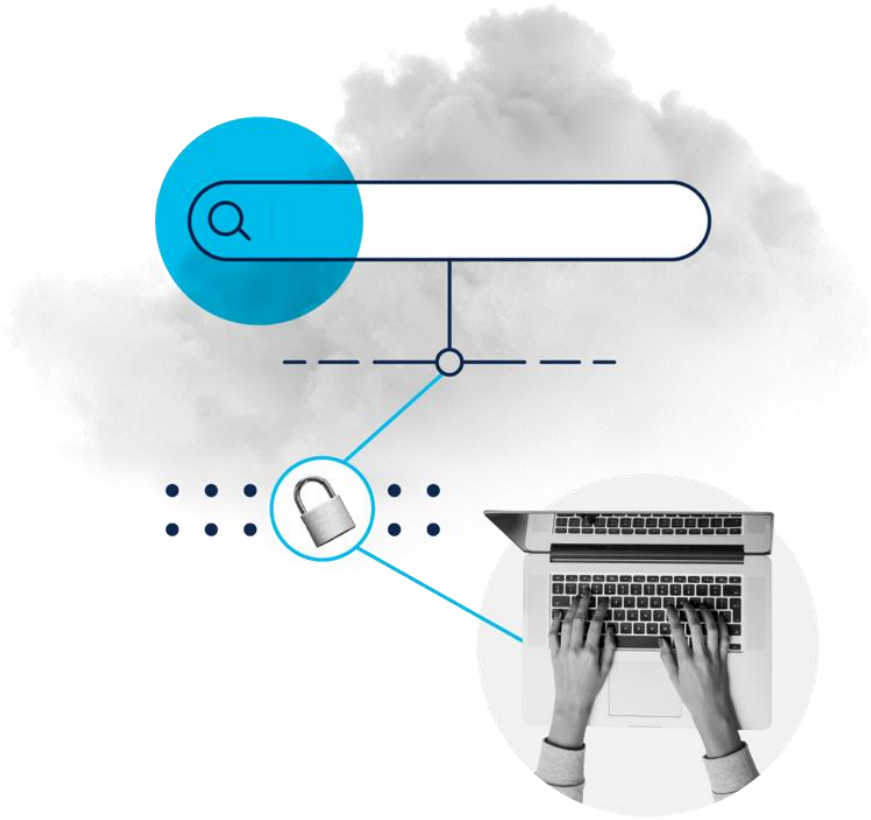
Challenge

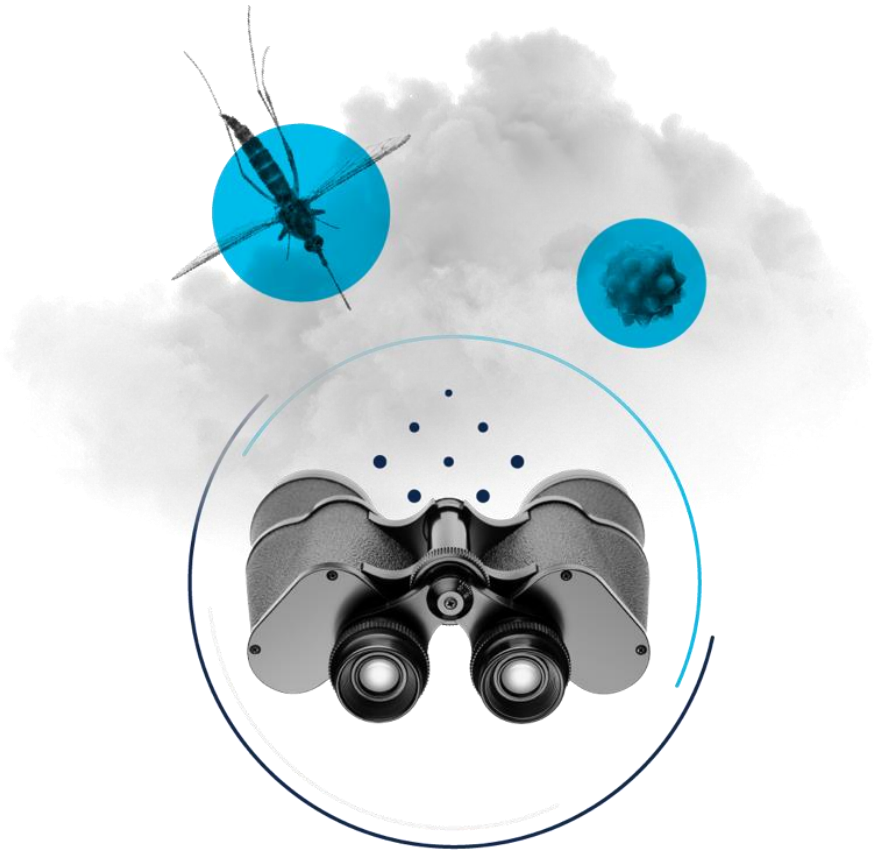
Deliver a secure browsing experience with protection from zero-day threats

Umbrella remote browser isolation (RBI)

Optional add-on provides more protection for risky destinations & users

- Provide air gap between user, device and browser-based threats
- Deploy rapidly without changing existing configuration
- Deliver a secure browsing experience with protection from zero-day threats
- Boost productivity by expanding safe access to risky destinations and protecting high risk users





Cloud malware detection

Challenge

Greater use of cloud storage applications increases the potential for malware infections

Cloud malware detection

Capabilities

- Scan cloud file storage repositories
- Detect cloud malware
- Automatically delete or quarantine malicious files

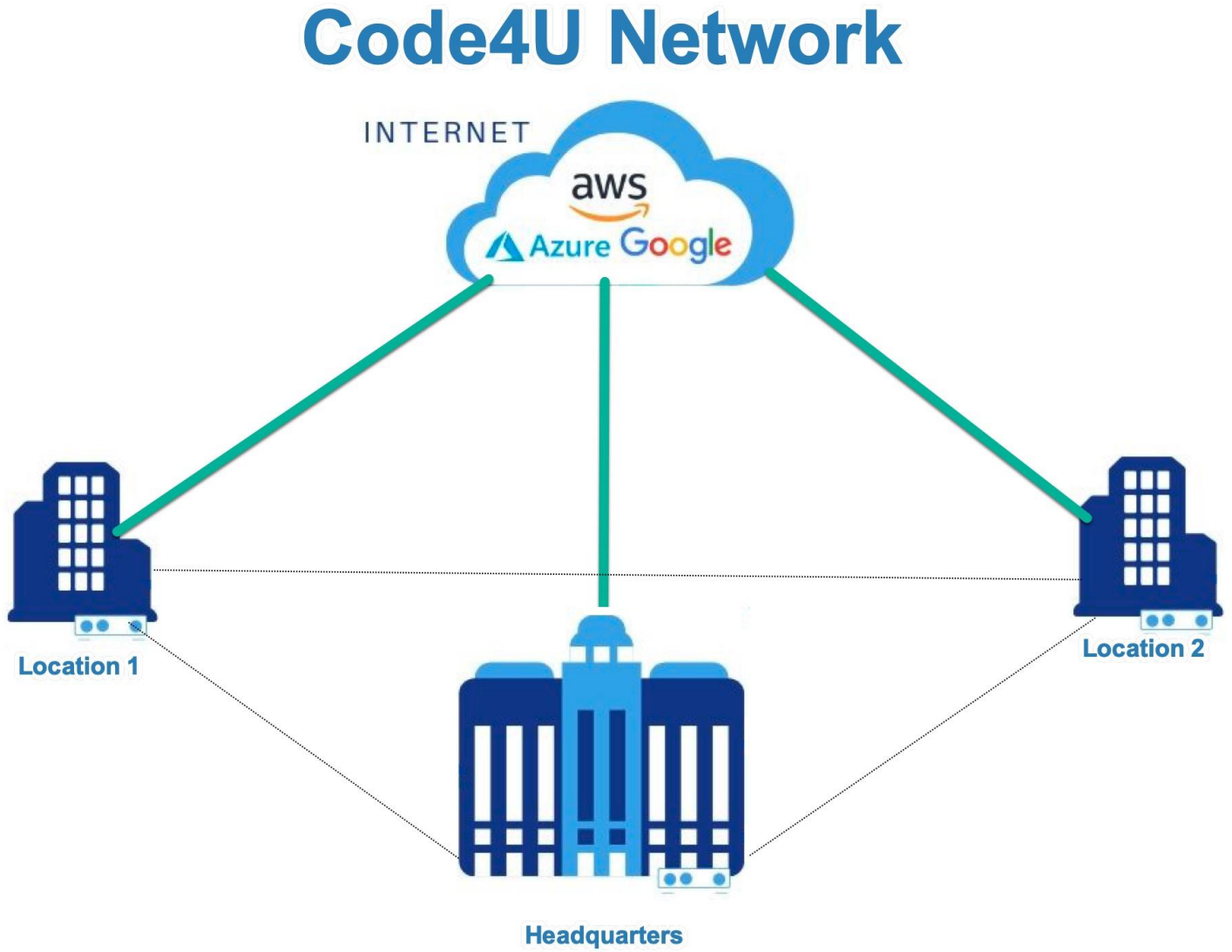
Results

- ✔ Safely move critical applications to the cloud
- ✔ Prevent malware infections from third-party cloud applications
- ✔ Prevent the spread of cloud malware infections

Limited Availability

cisco SECURE

- 3 Locations
- Each location connects directly to the internet
- In addition, 55 contract and remote workers spread throughout the region



Issue #1

The data and resourc cloud.

The people are How to access safely?

Umbrella = Cloud Security

Issue #2

How to provide firew ction of incoming and outg hen the users are no longer centrali

Umbrella w/ Cloud Delivered Firewall

Issue #3

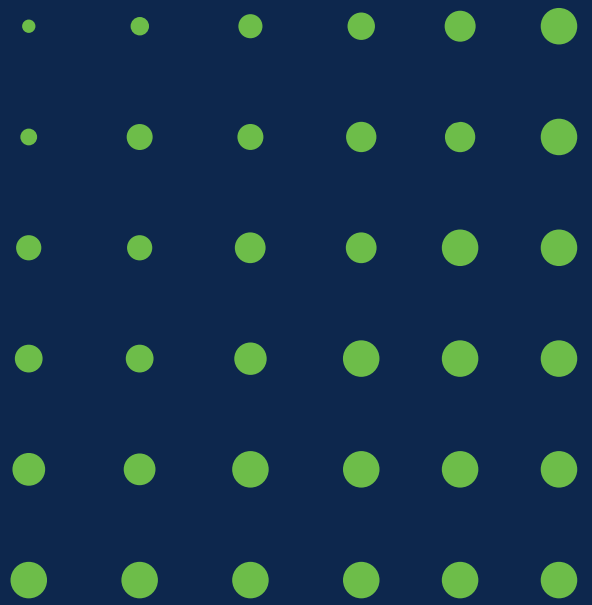
Even "safe" websit… …ks that connect to malw… …llow employees to … …ence?

Umbrella w/ Remote Browser Isolation

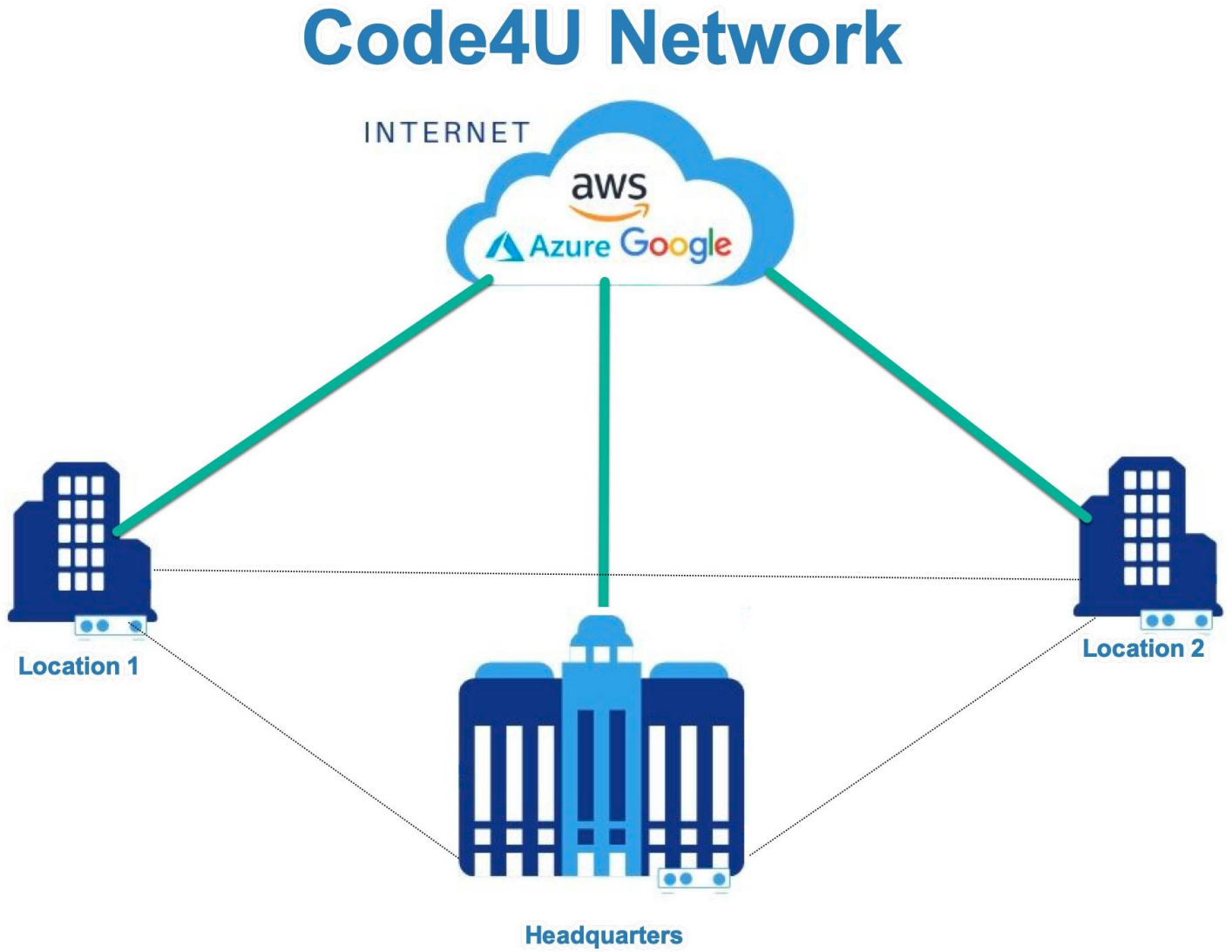
Cisco Umbrella Package Comparison

	DNS Essentials	DNS Advantage	SIG Essentials	SIG Advantage
	Block threats at the DNS layer across your enterprise in minutes without added latency	Get DNS protection plus additional web security and threat insights to speed up investigations	Deploy advanced security functions and simplify management with the most effective security in the industry	Unlock the highest levels of protection and control with advanced security functions like layer 7 firewall with IPS, DLP, and more
Licencing	By # of users	By # of users	By # of users	By # of users
Security & Controls				
DNS-layer security				
Block domains for malware, phishing, botnet, and other high risk	●	●	●	●
Block domains from Cisco SecureX, direct integrations (Splunk, Anomali, & others) and custom lists using enforcement API	●	●	●	●
Block direct-to-IP traffic for C2 callbacks that bypass DNS[1]		●	●	●
Secure web gateway (SWG)				
Proxy web traffic for inspection		Traffic associated with risky domains via selective proxy	All web traffic	All web traffic
Decrypt and inspect SSL (HTTPS) traffic		With selective proxy	●	●
Enable web filtering	By domain or domain category	By domain or domain category	By domain, URL, or category	By domain, URL, or category
Create custom block/allow lists	Of domains	Of domains	Of URLs	Of URLs
Block URLs based on Cisco Talos and other feeds; block files based on AV Engine and malware defense		With selective proxy	●	●
Use malware analytics (sandbox) on suspicious files			500 samples/day	Unlimited samples
Use retrospective security to identify previously-benign files that became malicious			●	●

Cisco DUO: Establish user trust with MFA



- 3 Locations
- Each location connects directly to the internet
- In addition, 55 contract and remote workers spread throughout the region



Scenario #1

I gain the username and password of one of your employees and attempt to log into your network.

Am I successful?

Scenario #2

I am an employee of your organization. My laptop is running an outdated operating system with known vulnerabilities.

Am I able to access corporate resources?

Scenario #3

I am a hacker and I have penetrated your network. I am now attempting to access your most sensitive applications.

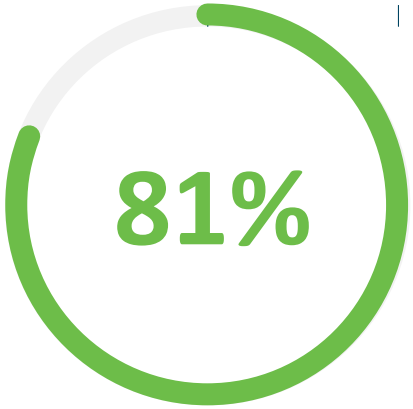
What controls are in place to stop me?

Shift in IT Landscape

Users, devices and apps are everywhere

Threats Today, As a Result

A new approach to security is needed – zero trust – to address identity, app & network threats.



Targeting Identity

81% of breaches involved compromised credentials

Targeting Apps

54% of web app vulnerabilities have a public exploit available

Targeting Devices

300% increase in malware variants targeting IoT devices

Colonial Pipeline Ransomware Attack

Timeline/Details:

Prior to May 6: Eastern European hacker group DarkSide infiltrates Colonial Pipeline's network and steals 100s of gigabits of data

May 6: Hackers Launch Ransomware Attack on Colonial Pipeline – Largest Pipeline in the US. Colonial Pipeline shuts down the pipeline.

May 7: Colonial Pipeline pays near $4.4 million (USD) Ransom

May 10: FBI confirms DarkSide Ransomware is responsible for the attack.

May 12: Over 1000 fuel stations run out of gas amid "panic buying"

May 12: Colonial Pipeline restarts operations

Result

The largest cyberattack on an oil infrastructure target in the history of the United States

Costs in the the tens of millions

And the source of the breach...

“

A single compromised password

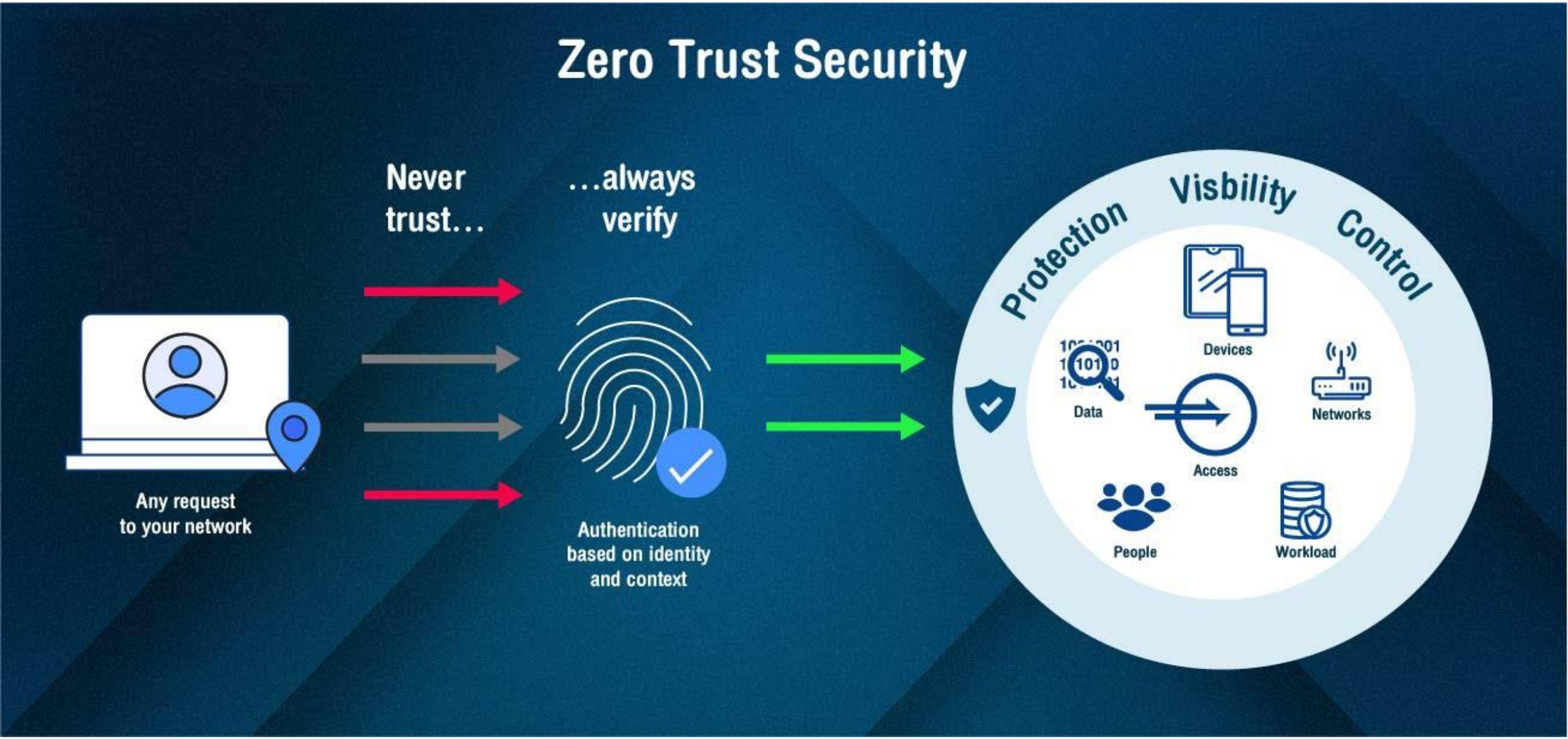
“The hack that took down the largest fuel pipeline in the U.S. and led to shortages across the East Coast was the result of a single compromised password.

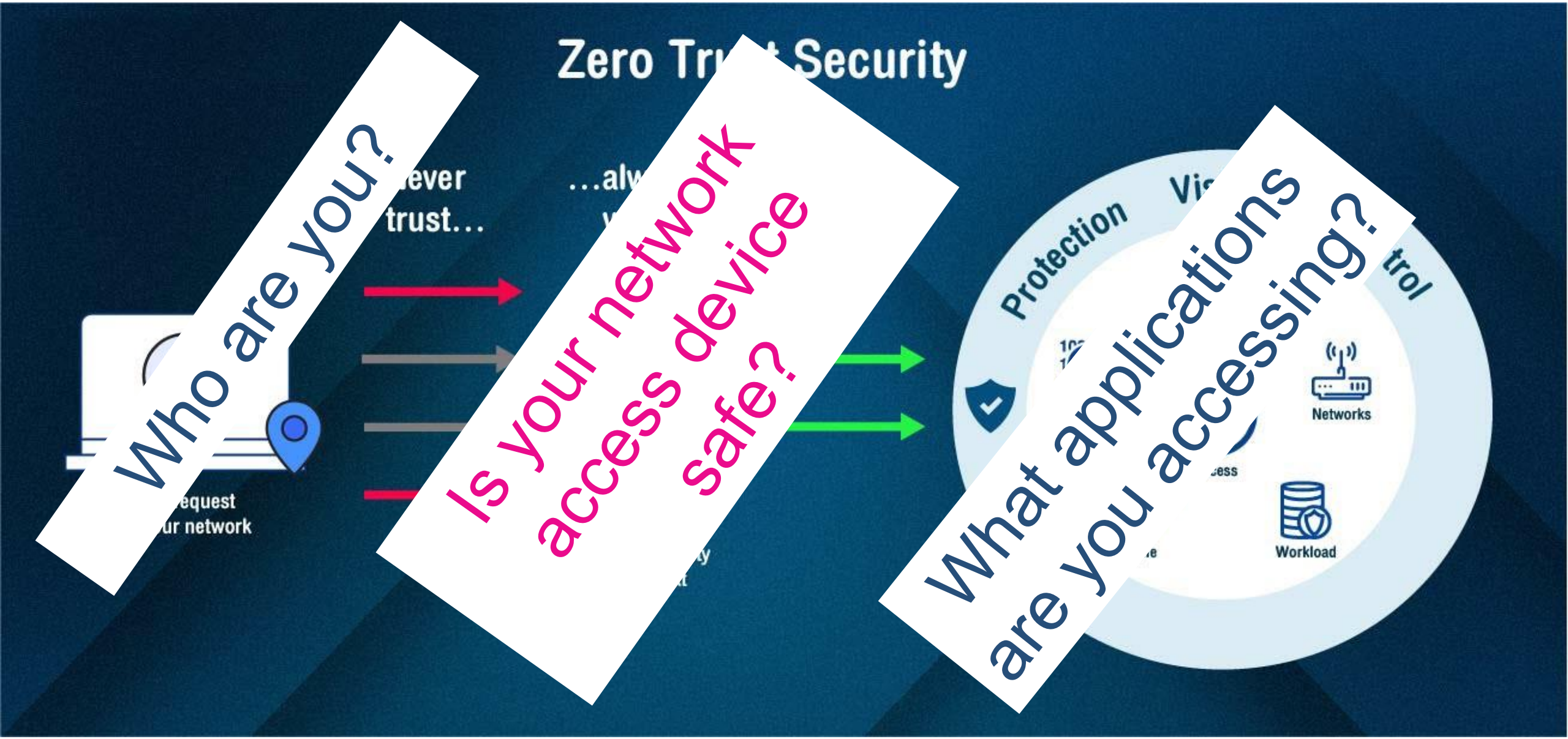
Hackers gained entry into the networks on April 29 through a VPN account. The account was no longer in use at the time of the attack but could still be used to access Colonial’s network.

The VPN account, which has since been deactivated, didn’t use ***multifactor authentication (MFA)****, a basic cybersecurity tool, allowing the hackers to breach Colonial’s network using just a compromised username and password.”*

Bloomberg 6.4.21

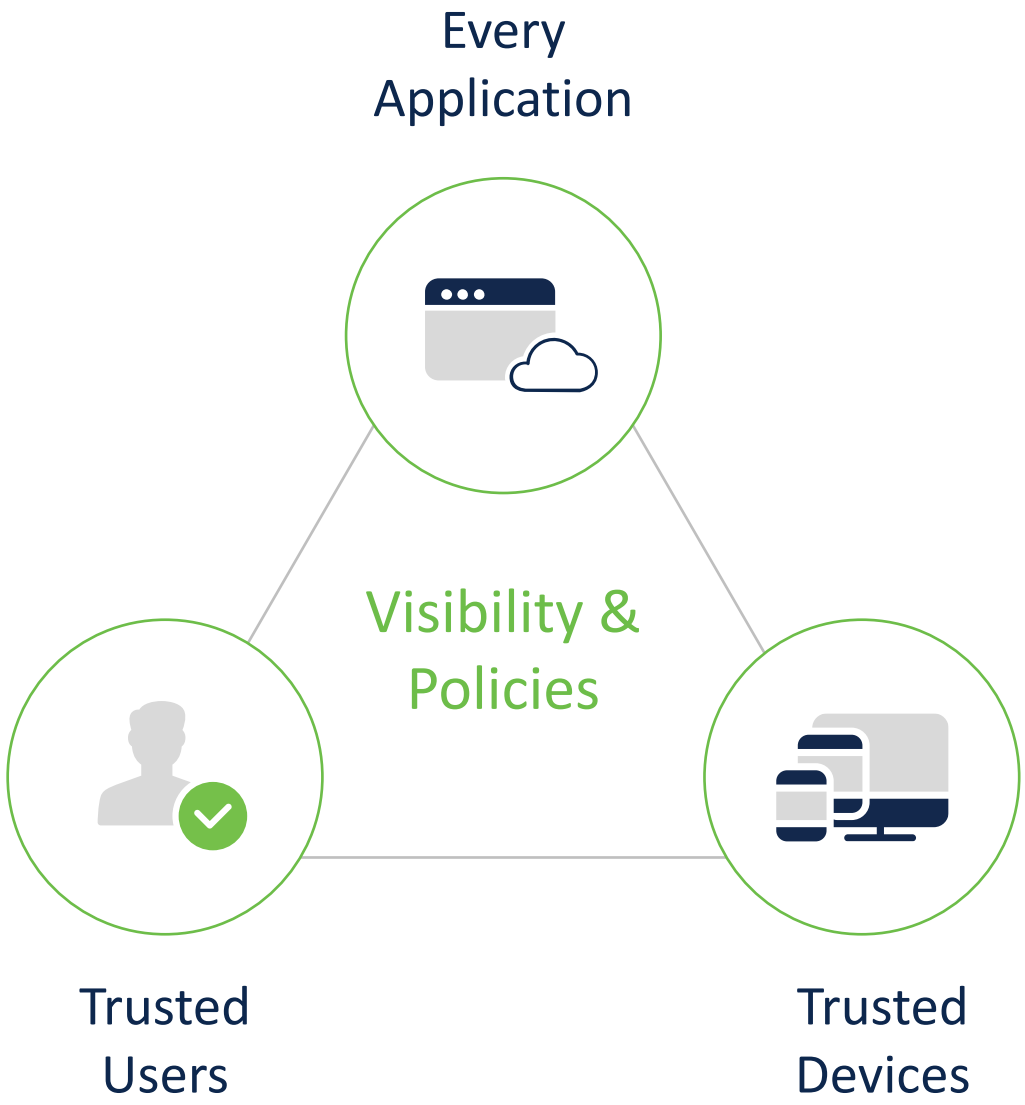
Zero Trust Security




Zero Tr t Security
ever
trust...
...alw
Who are you?
Is your network access device safe?
What applications are you accessing?
Protection
Networks
Workload

Cisco Duo delivers Zero Trust for your Workforce

by verifying the identity of users
and the health of their devices before
connecting to the applications they need



cisco DUO

The scope of Cisco DUO

900M

Authentications
Per month

37 Bill

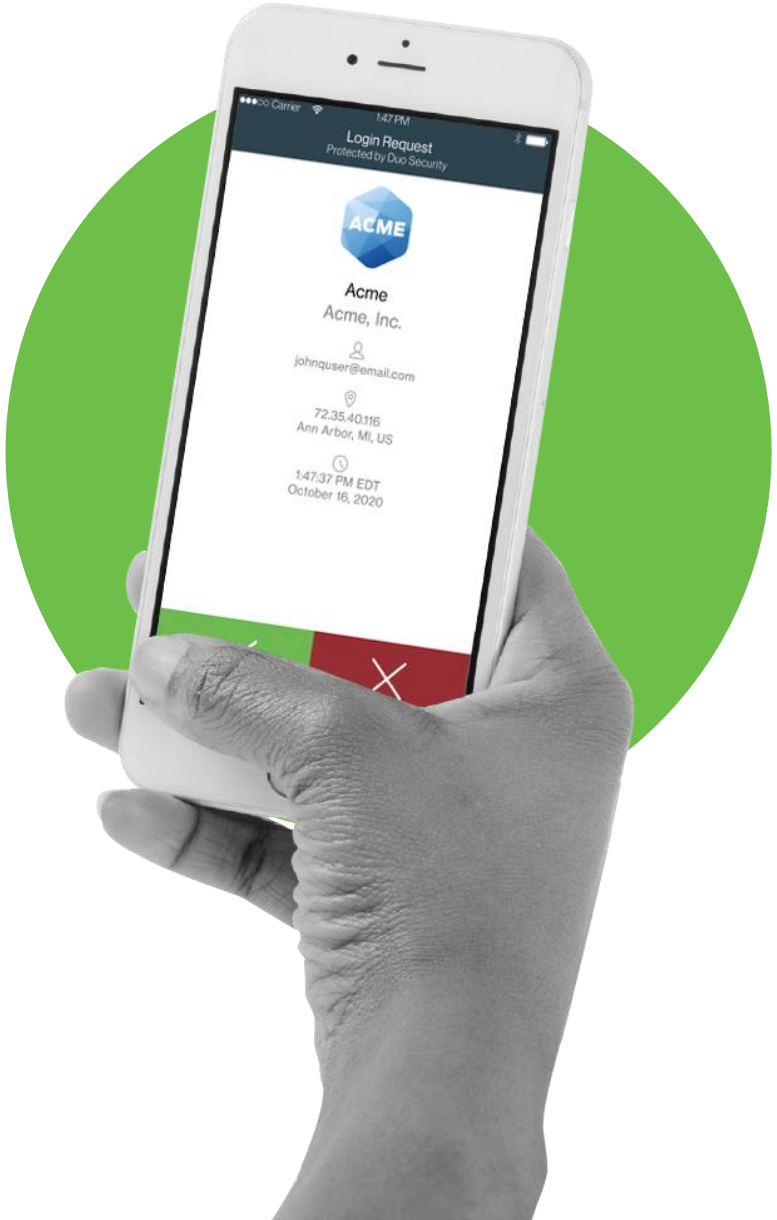
Devices Protected

436K

Unique Applications

World's Easiest and Most Secure MFA

- Instantly integrates with all apps
- Users self-enroll in minutes
- Users authenticate in seconds; no codes to enter



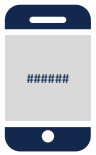
Broadest Range of Multi-Factor Authentication (MFA) Options

- Configure authentication options for each application or group of users
- Enable multiple option for users for ease of use and flexibility


Wearables


Push


Phone Call



Soft Token


Biometrics


U2F


Hardware Tokens


SMS

Meet Compliance Requirements

Every security best practices guide and regulation asks for MFA and device visibility

Meet MFA requirements outlined in PCI-DSS 3.2 Section 8.3

Helps meet NIST 800-63 and 800-171 access security requirements

Meet DEA's EPCS requirements when approving e-prescriptions

Aligned with GDPR data protection laws in Europe

Meet FFIEC requirements for financial applications

Get visibility into personal devices used to access PHI

Customer Story

Facebook

Challenge

- Protect developers as they access internal networks
- Ease of Use

Solution

- DUO with Yubico keys
- Multiple authentication methods
- Initially deployed on Linux servers and then spread through organization.

facebook.

Duo grew organically at Facebook, from protecting 300 to more than 10,000 users.

Facebook uses Duo's solution to reduce friction and make security easy for their internal team.

> Facebook is a very fast-paced environment and we needed technologies that would allow us to maintain that pace. Because of the ease of use of Duo, we have seen minimal support and overhead costs. Other technologies didn't fully support our need to allow multiple and rapid logins to SSH sessions."
>
> - John Flynn – Information Security Manager

Cisco DUO -Device Trust

Assess the health and security posture of
any device

Compromised Devices Can Access Your Data

- Admins lack time to patch all corporate (managed) devices
- End users access data with personal (unmanaged) devices
- End users don’t want admins to take control of personal devices

of vulnerabilities exploited will be ones known by security team for at least one year (through 2021)

Source: Gartner, Dale Gardner, 2018 Security Summit

Deep visibility into laptops and desktops

- Laptop / desktop security health
- Check devices before they login
- Corporate managed and BYO devices
- Supports web-based applications
- Windows 10 and MacOS

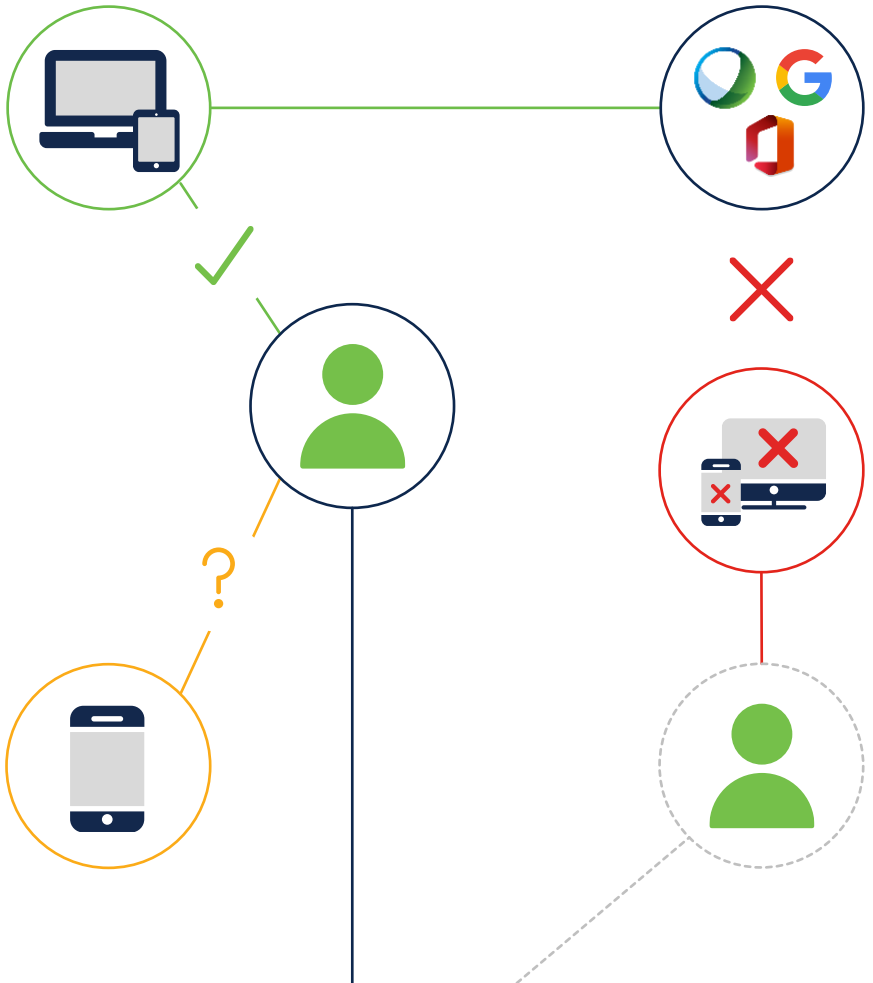
Protect Every Application

Manage and control who is allowed to access applications

cisco SECURE

Enforce Adaptive Policies

- Create customizable security policies
- Enforce Global, App & Group Level controls
- Establish a level of trust based on users and devices



Secure Any Corporate Application

Proprietary Apps (APIs)

C# Java python node Ruby

Microsoft Environments

Forefront Windows Office 365 Microsoft Active Directory Outlook

Cloud Services

Active Directory Federation Services Centrify onelogin okta PingIdentity

Unix Devices (SSH Sessions)

FreeBSD Linux redhat ubuntu

Internal Applications (VPNs)

OPENVPN paloalto Array Check Point Barracuda f5 FORTINET CISCO JUNIPER

Cloud Applications

Dropbox salesforce Google Apps workday amazon web services box Office 365 Cisco webex slack

Web Applications

splunk> Drupal Confluence WordPress JIRA Shibboleth

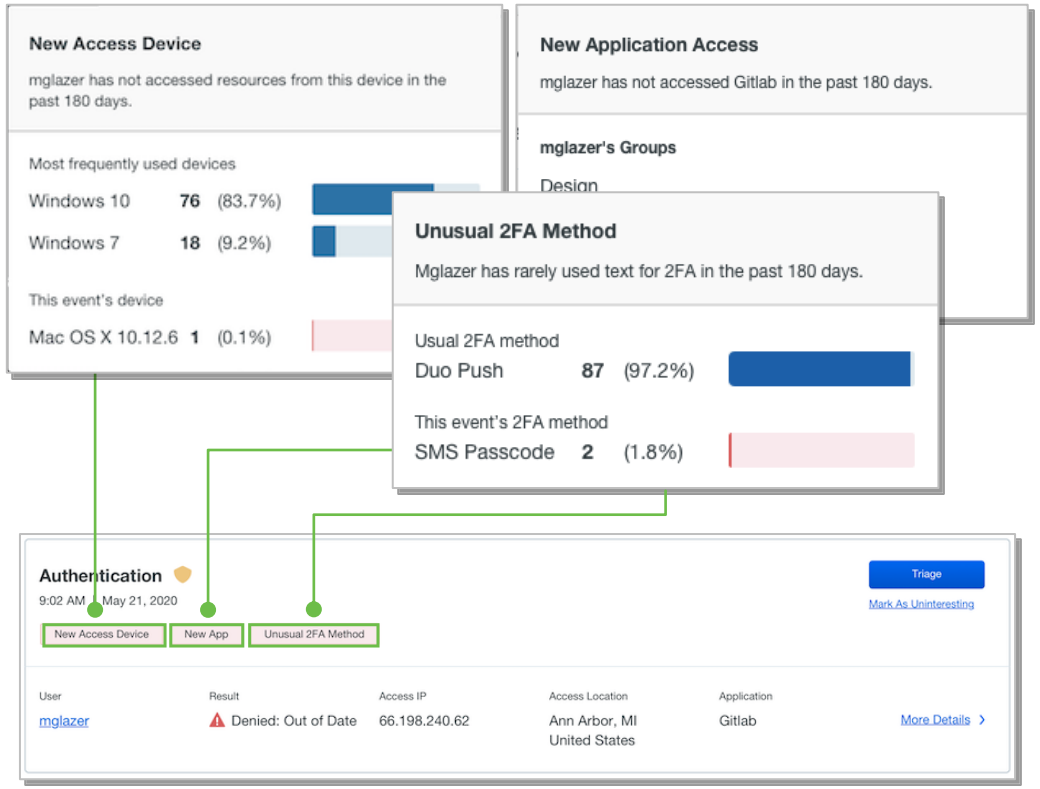
SAML 2.0 Applications

Google Apps amazon web services Office 365 salesforce box

Integration documents are available at duo.com/docs

Monitor Access Risk

- Analytics engine evaluates historical & contextual access patterns
- Duo Trust Monitor then surfaces risky and atypical login attempts
- Leverage anomalies to update policy or remediate compromised credentials



Scenario #1

I gain the username and pass one of your employees and attempt to l our network.

Am I successful?

Scenario #2

I am an employee of you… My laptop is running an outdated o… …n with known vulnerabilities.

Am I able to acce… …esources?

No. DUO – Device Posture Checks

Scenario #3

I am a hacker and I have ur network. I am now attempting to acce sensitive applications.

W hat controls ar top me?

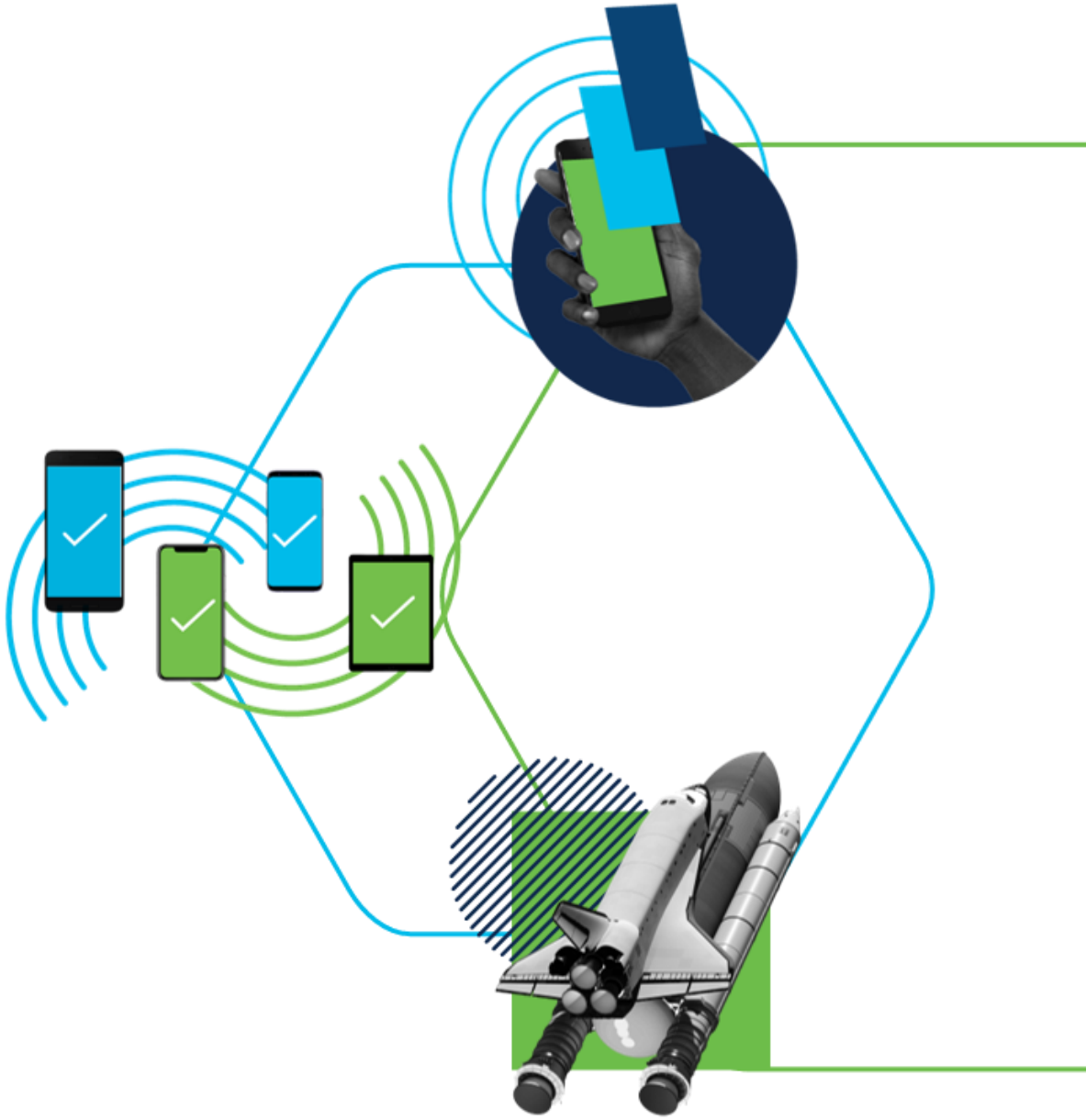
Answer: DUO Application Visibility

Packaging

Duo MFA
Basic MFA & SSO for unlimited applications

Duo Access
Adaptive MFA policies based on user and device risks

Duo Beyond
Granular device policies based on device trust



Feature Highlights

Duo MFA

- Multi-Factor Authentication
- Single Sign-On (SSO)
- Protect Any Application
- Protect Federated Cloud Apps

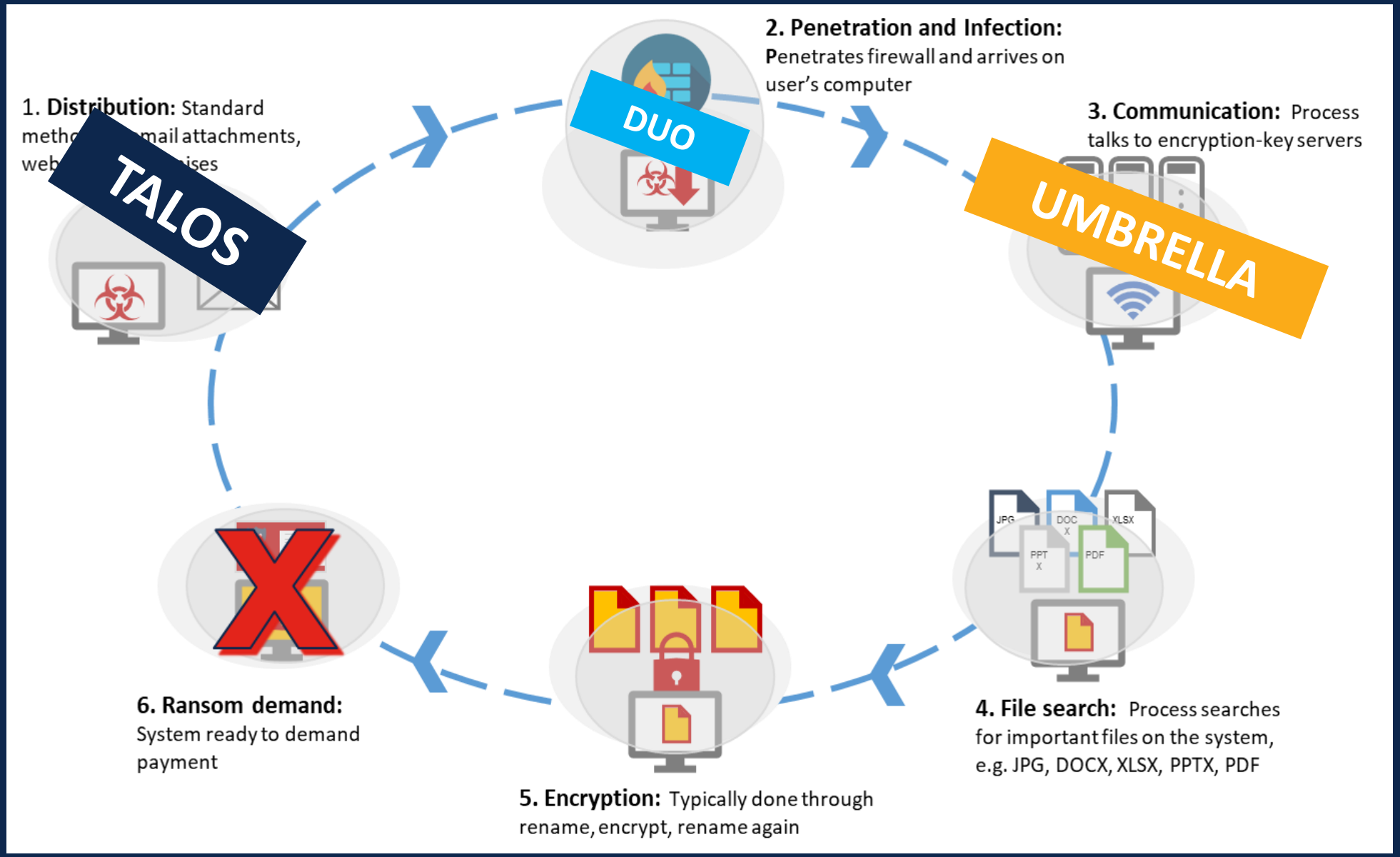
Duo Access

- Duo MFA +
- Adaptive Groups Based Policy Controls
- User Based Policy
- Device Visibility
- Device Health Checks
- Device Based Policy

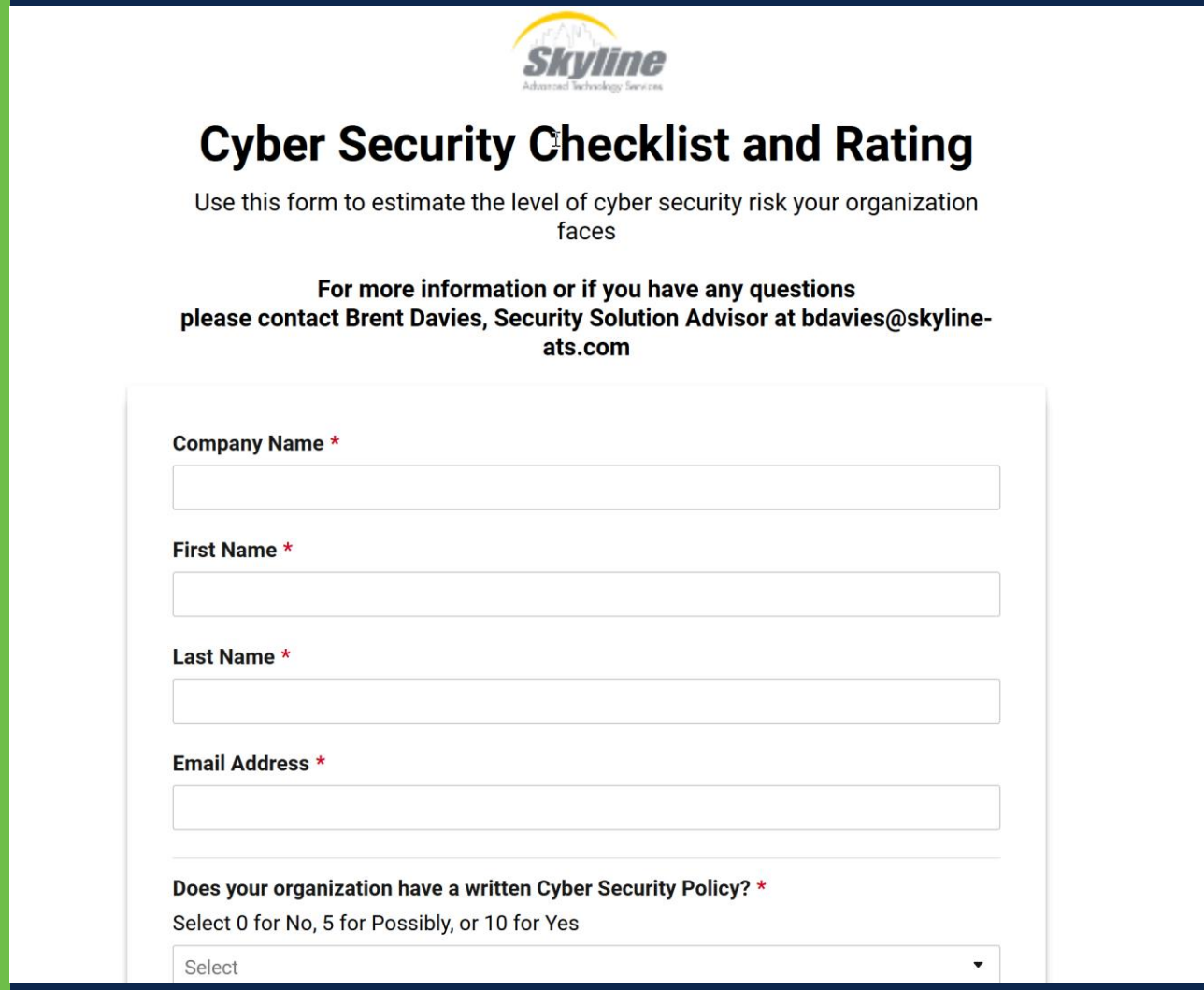
Duo Beyond

- Duo MFA and Access +
- 3rd Party Agent Verification
- Trusted Endpoints
- Secure Remote Access
- Duo Mobile as Trusted

Full Capabilities: https://duo.com/pricing



Next Steps….



Skyline
Advanced Technology Services

Cyber Security Checklist and Rating

Use this form to estimate the level of cyber security risk your organization faces

For more information or if you have any questions please contact Brent Davies, Security Solution Advisor at bdavies@skyline-ats.com

Company Name *

First Name *

Last Name *

Email Address *

Does your organization have a written Cyber Security Policy? *

Select 0 for No, 5 for Possibly, or 10 for Yes

Select

Thank you for attending.

To continue the conversation about your security please contact:

Security Solution Advisors:

Jose Mock jmock@skyline-ats.com

Brent Davies bdavies@skyline-ats.com

Skyline Advanced Technology Services

Questions