BIG UNIVERSITY 2018

Technical Track 1

BIG UNIVERSITY 2018

Technical Track 1

SESSION 1

"Performing & Evaluating Penetration Tests"

Jason Beltrame (Cisco)

Today's Agenda

- The What and Why of penetration testing
- Steps to build a low-cost pentesting system
- Best practices of proper pentesting protocol
- How to evaluate your pentesting results

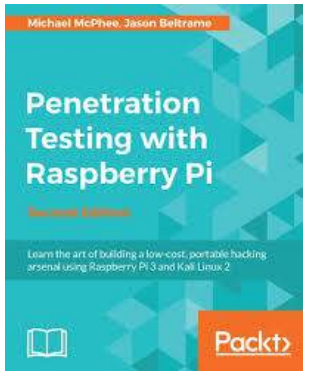
But first, a little about me….

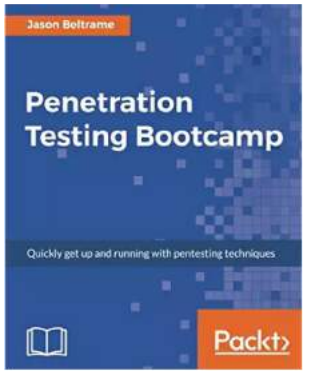
Background

- Fell into IT back in 1997, originally Architecture major
- Graduated from DeSales University
- First position was as a Network Admin
- Got into security because I was the “new” guy

DeSales University

Professional Experience

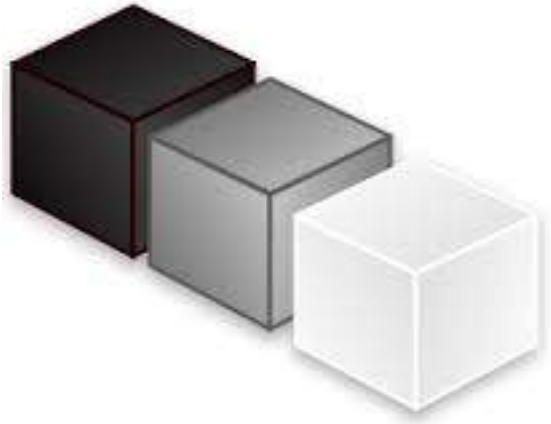




- Network Security Engineer for 16 years
- Had a lot of fun with compliance over the years
- Have been with Cisco now almost 4 years as Systems Engineer
- Author of “Penetration Testing Bootcamp”
- Co-author of “Penetration testing with a Raspberry Pi”

What is Penetration testing?

- Looking for security gaps within the environment
- Location
  - External Tests – eyes from outside environment
  - Internal Tests – eyes from within environment
- Types
  - White box – Full knowledge
  - Gray box – Partial knowledge
  - Black box – No knowledge



Why is Penetration testing important?

- Looking for security gaps within the environment
- Compliance Requirements
- Verifying current controls are working
- Documentation
- Finding 3rd party software/hardware bugs

Who can perform Penetration Tests

- Everyone Right?
  - Quick Answer, DEPENDS
- Approved Scanning Vendors (ASV)
  - Brought to us by PCI
- 3rd Party
- Internal Resources

How often do I perform tests?

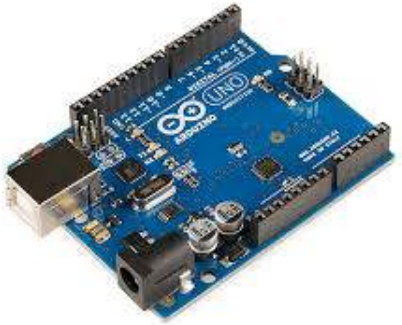
- Again, Depends
- Compliance will dictate some
  - PCI – Quarterly External Scans
  - PCI – Quarterly Internal Scans
- If no compliance regulations, at least bi-yearly
- After large changes to the environment

What do I test?

- Network access
  - Internal/External
- Web Application
- Social Engineering
- Vulnerability Scanning

Building a low-cost Penetration testing system

Research

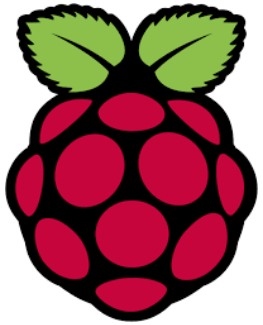


- Lots of options available
  - Arduino
  - Raspberry Pi
  - Joule
- Raspberry Pi is excellent option, but not in all cases.
- Hardware will ultimately depend on requirements

Picking the Right Raspberry Pi

- Multiple options available
- Requirements such as tools and locations will determine
- Most common models
  - Raspberry Pi 3
  - Raspberry Pi Zero

Raspberry Pi Provides



- Small footprint
- Powerful
- Wide community support
- Inexpensive
- Portable
- Flexible

Package/A la Carte

- The Raspberry Pi's can be purchased in bundles
- A la Carte option can be more affordable

Additional Hardware

- Additional Wifi adapter
- Additional Bluetooth adapter
- Command and Control server
  - Cloud based server
  - On-prem computer
  - Computer within Penetration Company network

Penetration Testing Best Practices

Perform all types of Testing

- Unless there is a good reason not too, test everything
- Each test is for a particular reason
  - Internal/External Network Access
  - Web Application
  - Social Engineering
  - Vulnerability Scanning

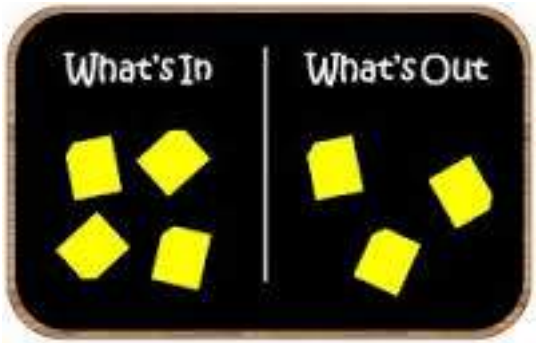
OpenVAS Open Vulnerability Assessment System

Nessus™

OWASP Open Web Application Security Project

Proper Scope

- PLAN, PLAN, PLAN!!!!
- Clearly Define the following
  - Scope
  - Time Frame
  - Desired Outcomes
  - Any specifics you desire



Get Management Buy-in

- Key to success
- Without there may be some limitation in place
  - Funding
  - Support
  - Remediation capabilities

Penetration Test Due Diligence

- Always check references when choosing penetration testing company
- Not all penetration testers are alike
- There are compliance organizations (PCI) that maintain lists, but still should be verified
- If possible, look at their report examples or sanitized customer reports

Provide Documentation

- Provide if you have it. Will help save time to provide
- Can be tested for accuracy during tests
- If there is none, one desired outcome could be documentation

Try not to fix issue during testing

- Can mess with results on both past and future tests
- Only adds complication
- Definitely consider it if extremely urgent finding is discovered.

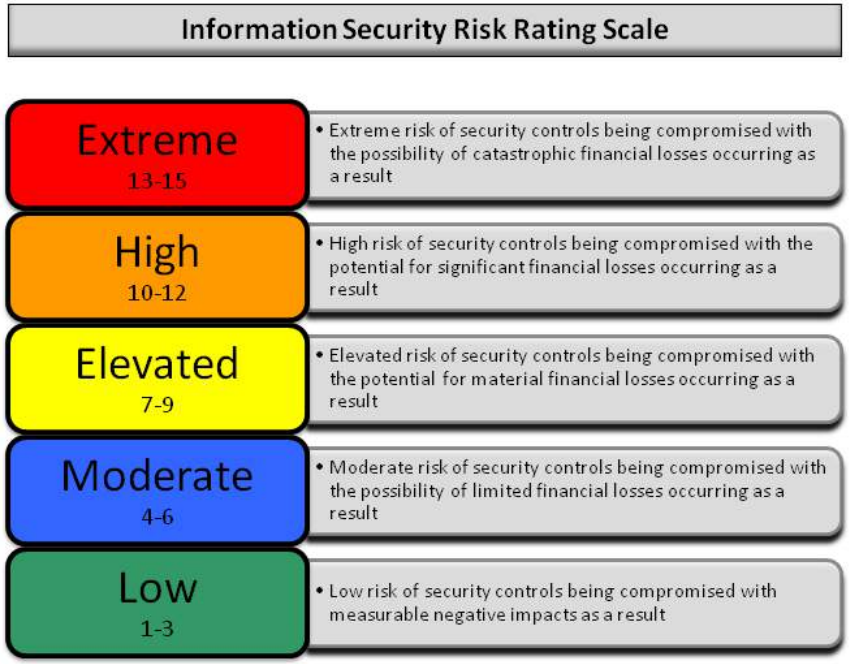
Reporting Etiquette

- Make sure reports are customized, and not just output form tool
- Make sure the information is in readable terms given the stakeholders
- Make sure reports show something meaningful, don’t just report on it to report on it.

How to evaluate the results!

Report should clearly lay everything out

- Include risk chart
- All findings should include:
  - Risk
  - Fix/Remediation
- Executive summary for upper mgmt
- Verify correct scope



Have plans in place for Remediation

- Schedule a business risk analysis meeting
  - Low hanging fruit
  - Architectural or larger infrastructure changes
  - Findings on unnecessary devices/services
  - Layout project plan and stick to it

Schedule next test

- After laying out your remediation plan, schedule the next test
  - Either during the normal rotation (Quarterly, Bi-yearly)
  - Test after any of the major changes.
- If you are sticking with the same company, try and request the same testers.

Thanks and happy pentesting!

Contact Information:

Jason Beltrame
Email: jabeltra@cisco.com
Twitter: @jmbeltrame

BIG UNIVERSITY 2018

Technical Track 1

SESSION 2

"How to Leverage DS as an Additional Layer of Security"

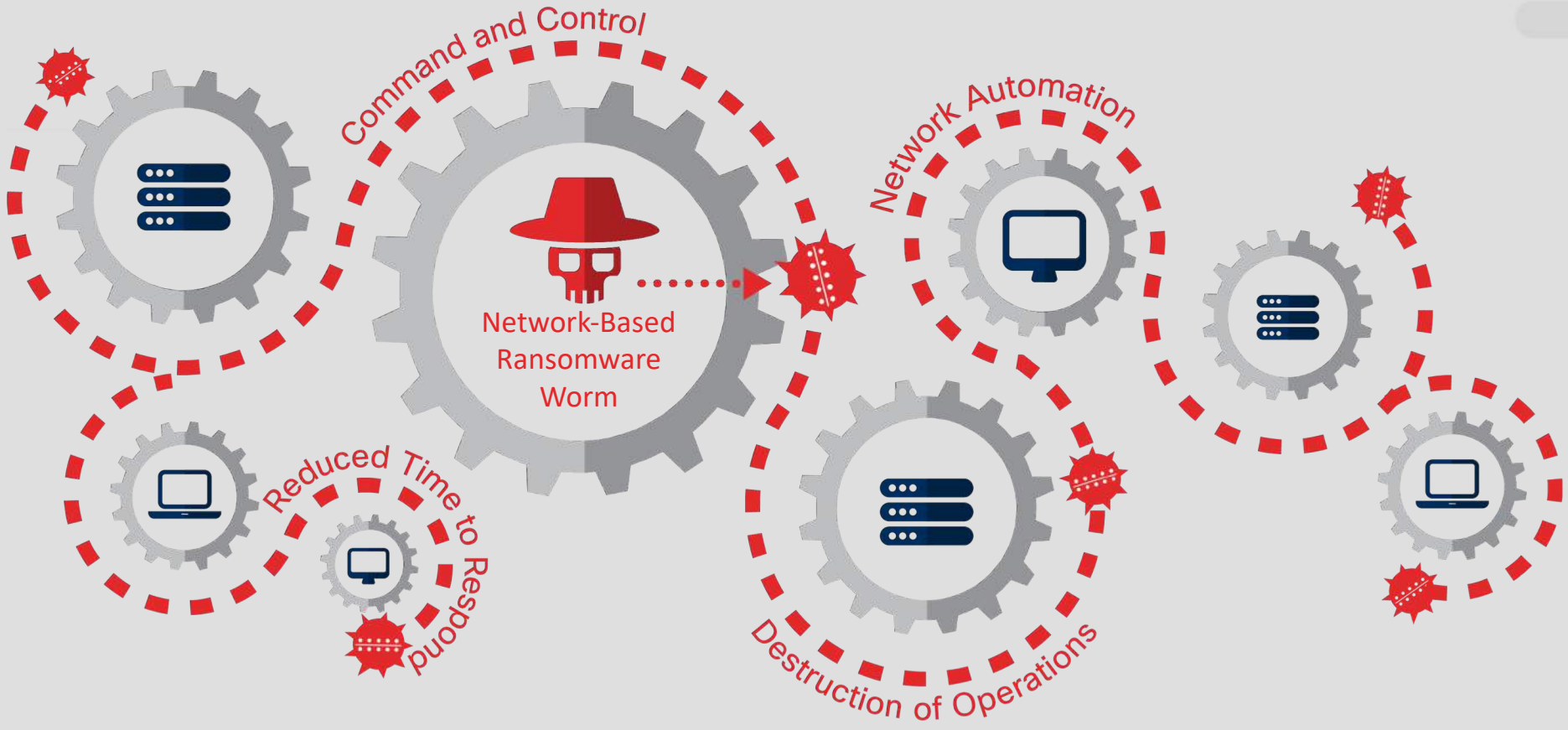
Nick Kelly (Cisco)

Security Defined

- Visibility + Policy + Enforcement = Security

Network-based Ransomware

WannaCry and Nyetya: rapid-moving, self-propagating network-based attacks



With active, unpatched machines, these automated worms will attack again. Have you secured your network?

The Cloud

Organizations increase reliance on the cloud

53%

manage over half of their infrastructure in the cloud

Appeal:

Better security (57%)

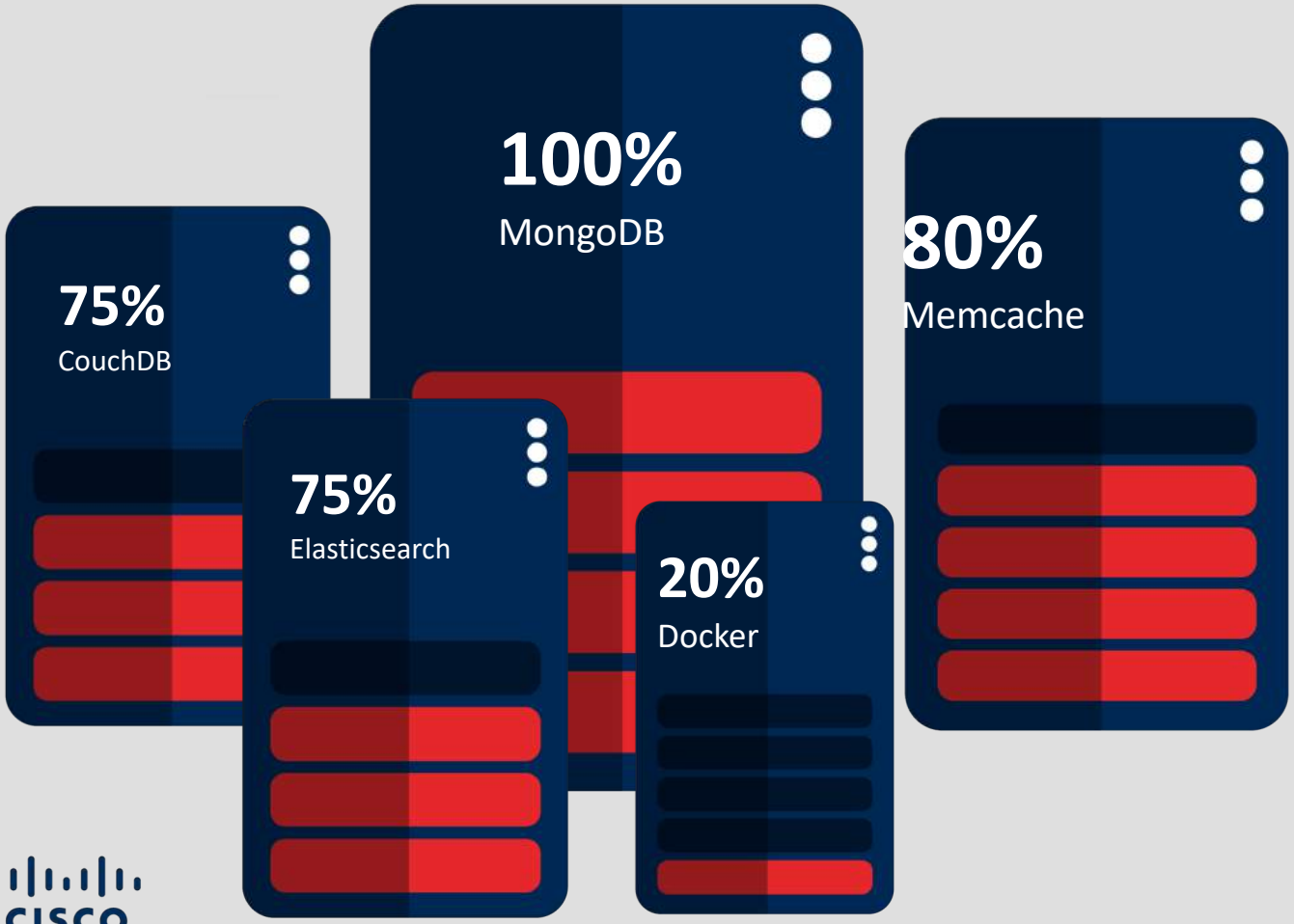
Scalability (48%)

Ease of use (46%)

Lack of internal workforce (41%)

Exposed Development Systems

Percentage of DevOps servers left WIDE OPEN is creating a huge ransomware risk



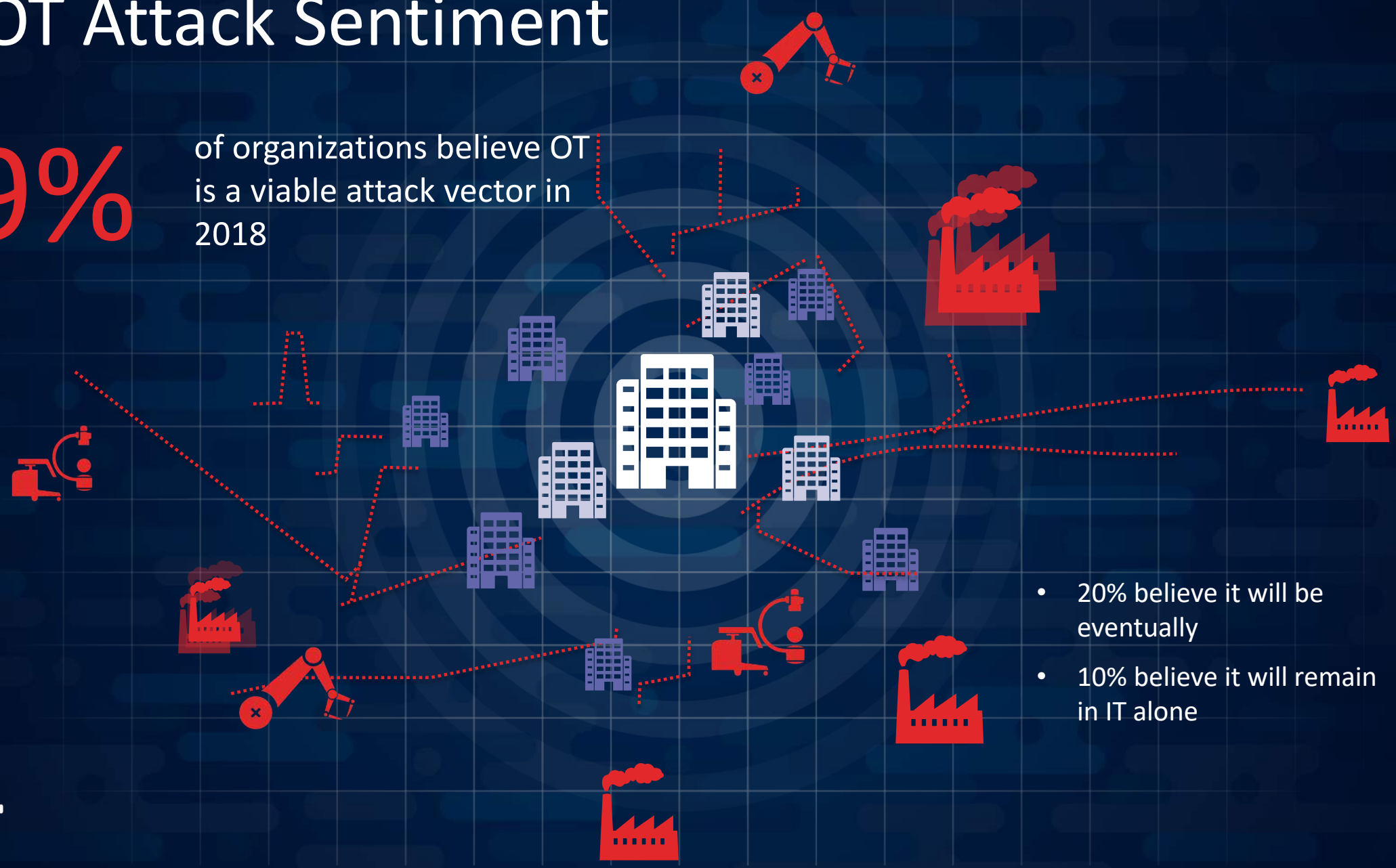
To reduce risk of exposure to DevOps ransomware attacks:

- Develop solid standards for secure deployment
- Maintain active awareness of the company's public infrastructure
- Keep DevOps technologies up to date and patched
- Conduct vulnerability scans

Source: Rapid7

IT/OT Attack Sentiment

69% of organizations believe OT is a viable attack vector in 2018

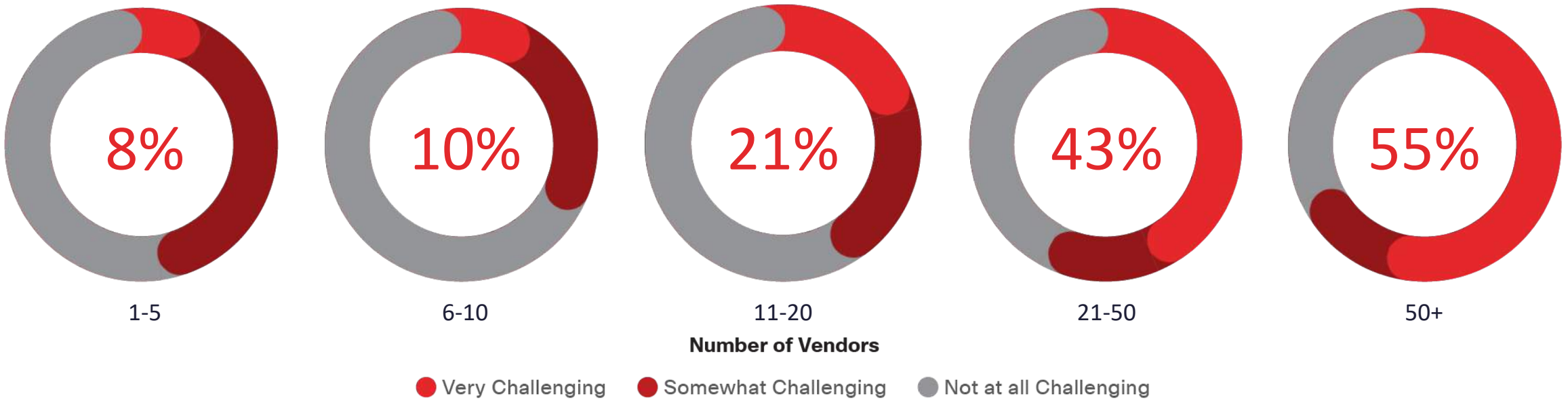


- 20% believe it will be eventually
- 10% believe it will remain in IT alone

cisco

Orchestration Challenges

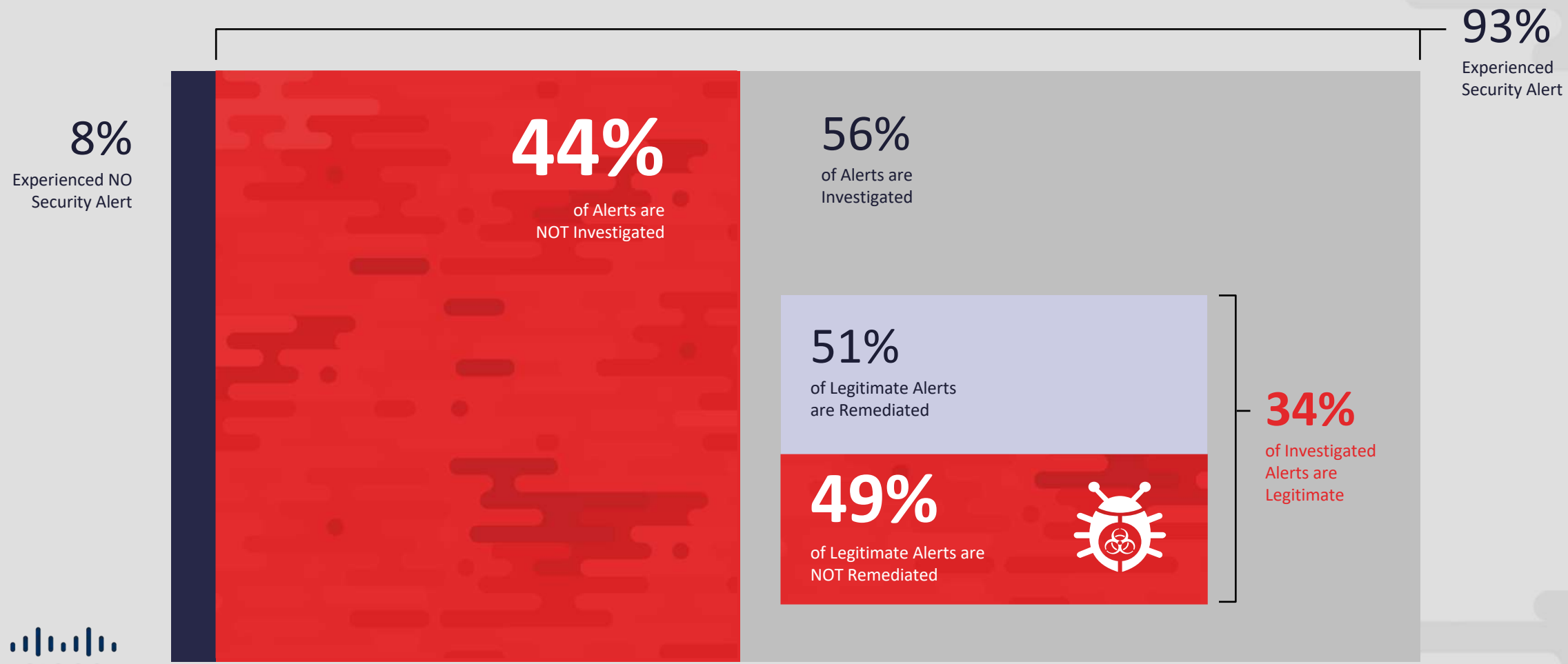
As the number of vendors increases, orchestration challenges grow



	Education	Financial Services	Government	Healthcare	Manufacturing	Pharma	Retail	Telecom	Transportation	Utility/ Energy
Very Challenging	17%	24%	16%	42%	14%	25%	19%	14%	12%	27%

Alerts

Uninvestigated alerts still create huge business risk



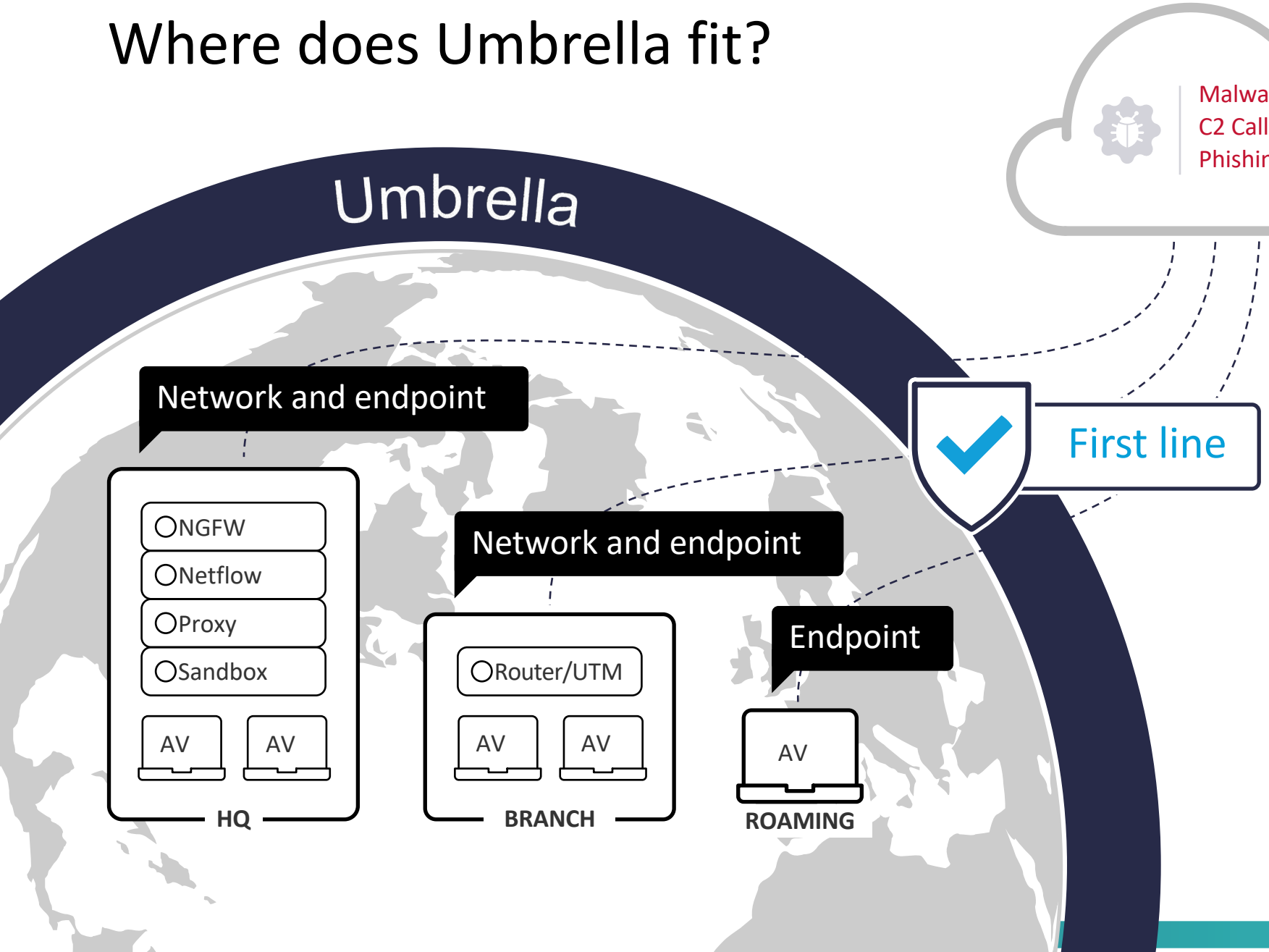
Users are the problem

- User is a four-letter word

Traditional Cisco Security

- ABC

Where does Umbrella fit?



It all starts with DNS

Precedes file execution and IP connection

Used by all devices

Port agnostic

An Added Layer of Breach Protection

UMBRELLA

Enforcement

Threat Prevention

Protects On & Off Network

Always Up to Date

No need for device to VPN back to an on-prem server for updates

Block by Domains, IPs & URLs for All Ports

Not just ports 80/443 or only IPs

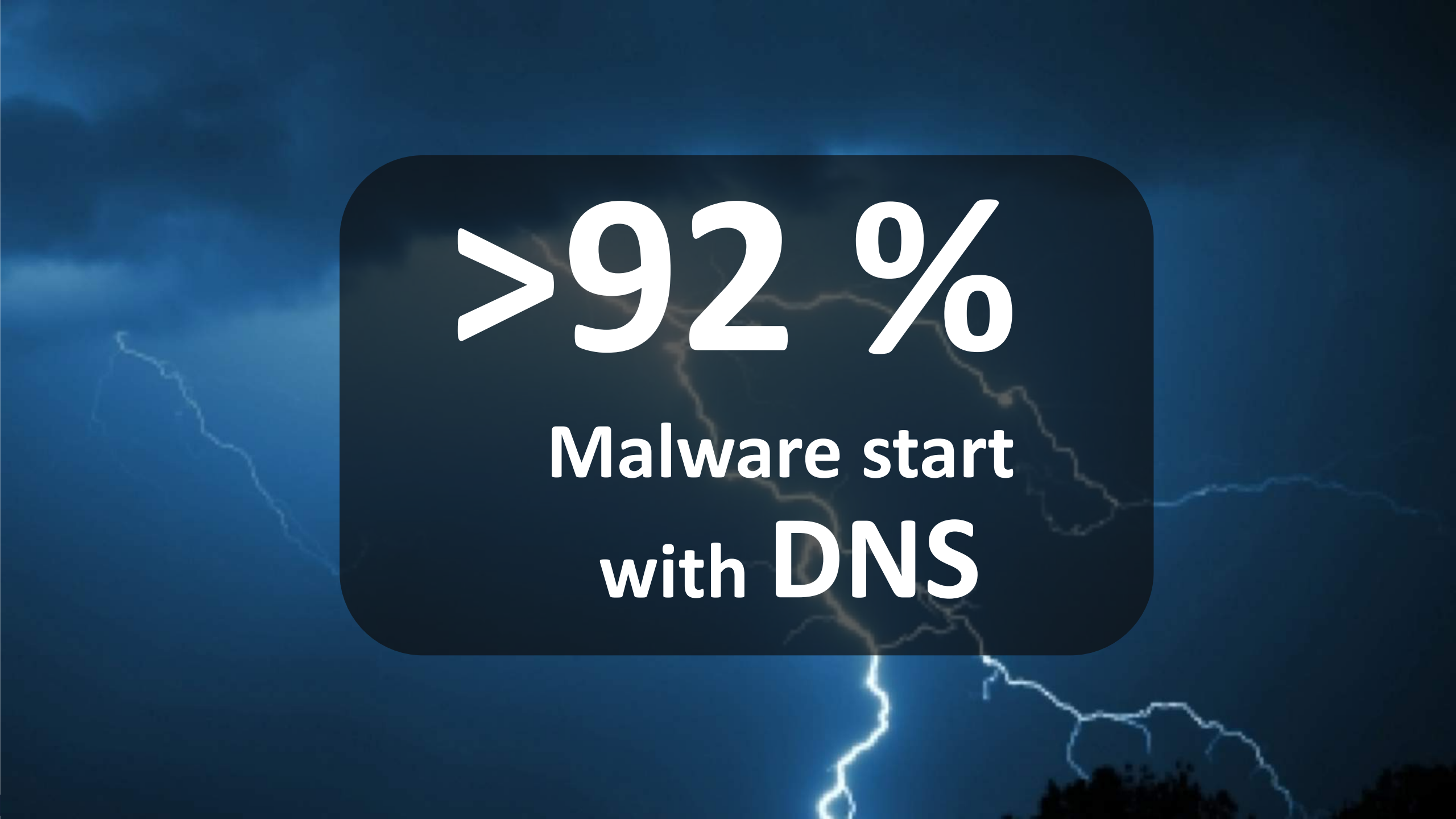
Turn-Key & Custom API-Based Integrations

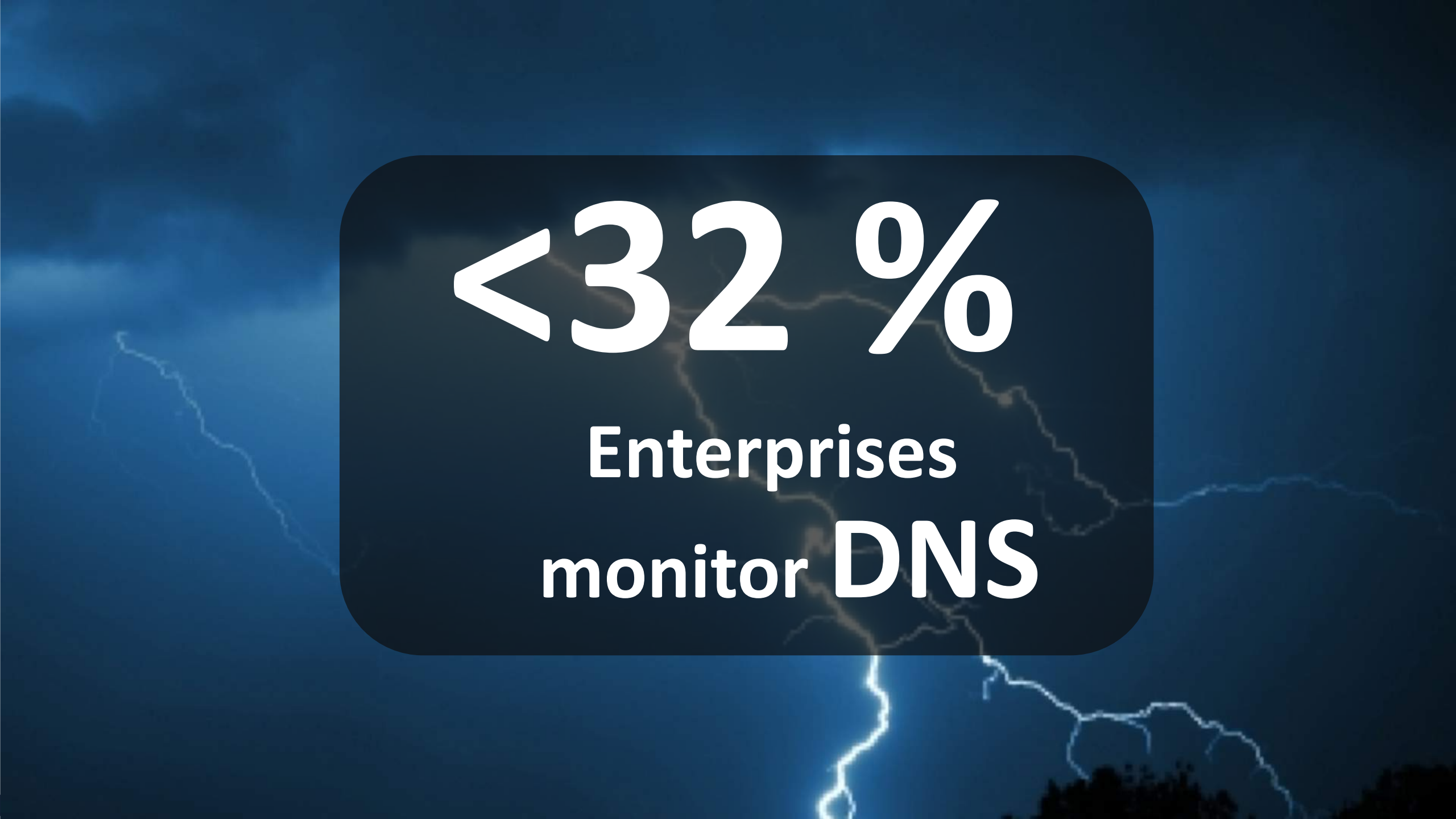
Leverage Existing Investment

- Nobody wants another agent
- Already invested in AnyConnect?
- VPN, Web Security, ISE, AMP, Umbrella, NetFlow (Stealthwatch)

Start With The Basics

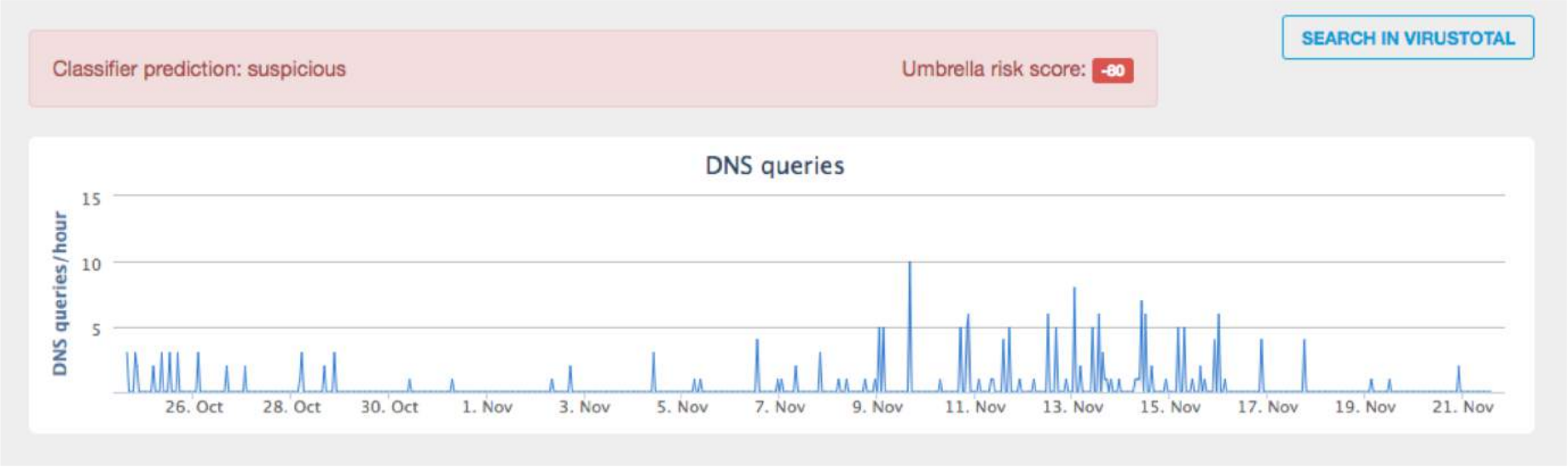
- **Patch Management**
- **Keep Software Updated**
- **Education On Ransomware**
- **Auto Update Security (Anti-Virus, Etc.)**
- **Control And Monitor Privileged Accounts**
- **Disable Macro Scripts from files transmitted over e-mail**
- **Backup Data Regularly**


>92 %
Malware start
with DNS


<32 %
Enterprises
monitor DNS

Where are you going?

- www.dell.com
- www.dell.com
- macafee.com
- symantex.com



Where are you going (part 2)?

Email Address	Associated Domains	Email Type	Last Observed
domains@hugedomains.com	Greater than 500 Total - At least 490 malicious	Administrative, Registrant, Technical	September 18, 2017

Nameserver	Associated Domains	Last Observed
nsg2.namebrightdns.com	Greater than 500 Total - At least 351 malicious	September 18, 2017
nsg1.namebrightdns.com	Greater than 500 Total - At least 359 malicious	September 18, 2017

I’m infected, now what?

Umbrella + AMP for Endpoints

Behavioral Indicators

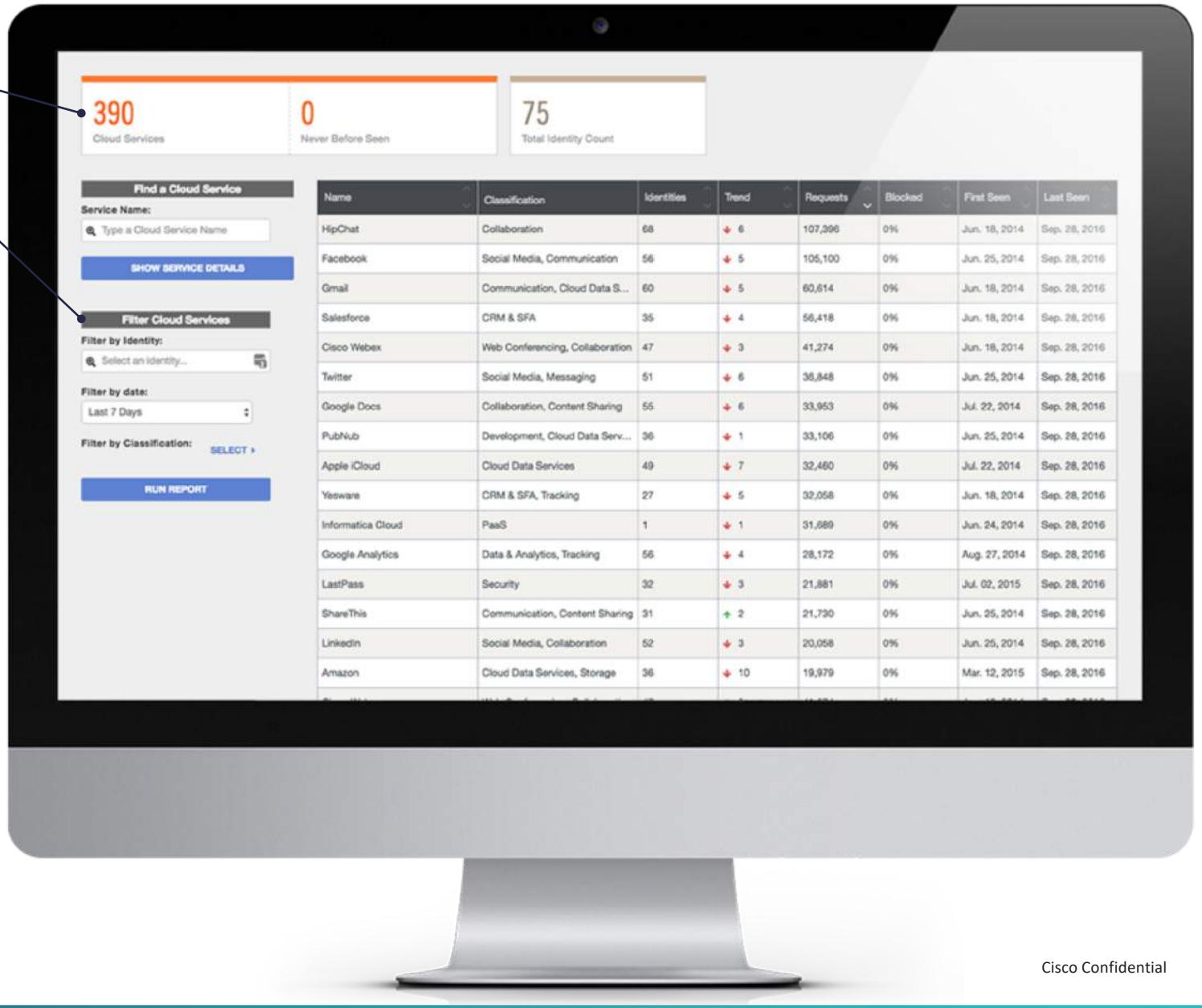
Potential TOR Connection	Severity: 100	Confidence: 100
Ransomware Backup Deletion Detected	Severity: 100	Confidence: 100
Shadow Copy Deletion Detected	Severity: 100	Confidence: 100
Artifact Flagged Malicious by Antivirus Service	Severity: 100	Confidence: 95
Process Modified Desktop Wallpaper	Severity: 100	Confidence: 95
Artifact Flagged as Known Trojan by Antivirus	Severity: 100	Confidence: 95

Total and newly seen cloud services

Cloud apps by classification and traffic volume

CLOUD SERVICES REPORT

Effectively combat shadow IT



Thank you.

BIG UNIVERSITY 2018

Technical Track 1

SESSION 3

"Analyzing Security Risks… Are You Really Protected?"

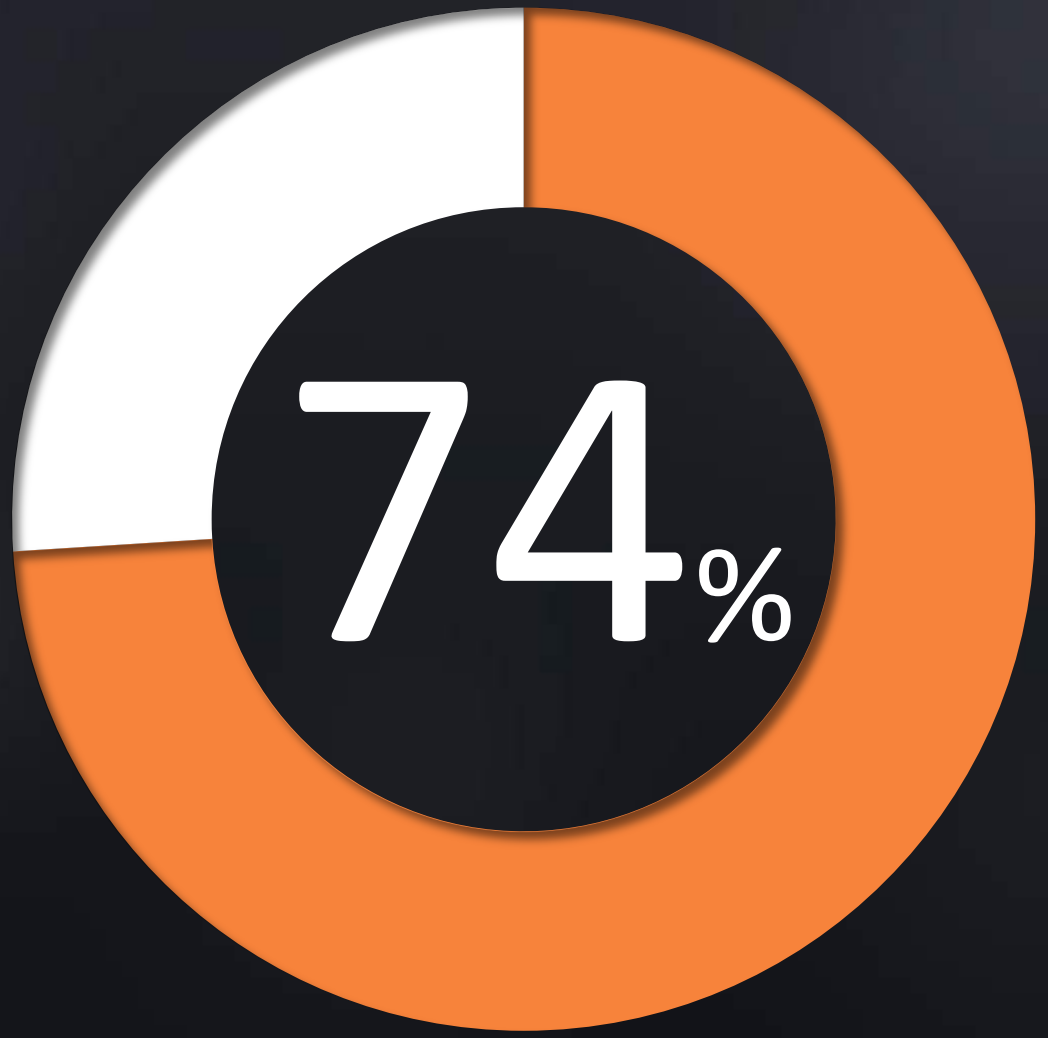
Joe Crehan (Barracuda)

Barracuda Email Protection

Version 1.1 | March 2018

Barracuda

Targeted Attacks Start with Email



2017 Threat Landscape Survey: Users on the Front Line - SANS Analyst Program

93% of phishing emails are now ransomware

FBI: $2.3 Billion Lost to CEO Email Scams

Advocate Health to pay largest HIPAA settlement

FBI Report: Ransomware and Phishing Scams Increasing

Of course, the number one cause of data loss, according to the FBI report, continues to be social engineering and email compromises. The reported losses associated with business email compromises in 2015 was $246,226,016.

Netflix Email Scam Targets Millions Of Subscribers

Russian Hackers Faked Gmail Password Form To Invade DNC Email System

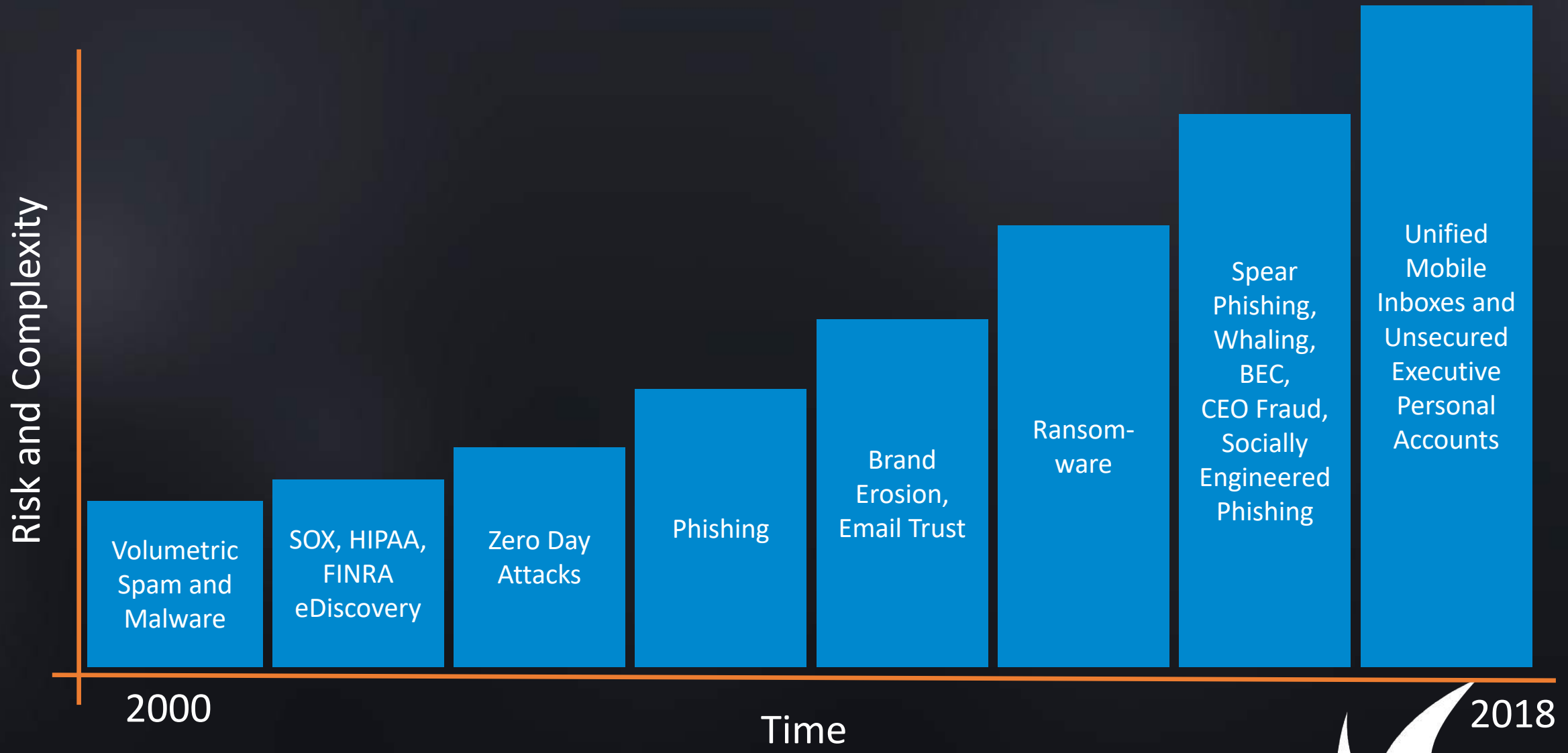
New online financial scam costs victims $130K per attack

- "Business-email compromise" scams target financial services firms and their clients through phishing.
- A successful attack nets an average $130,000 loss per scheme.
- Between 2013 and 2016, these schemes have resulted in a total dollar loss of $5.2 billion.

North Korean hackers target US electric companies with malicious email attack

Attackers Exploit 17-Year-Old Bug to Deliver Malware via Cobalt Strike

And it gets more complex every year

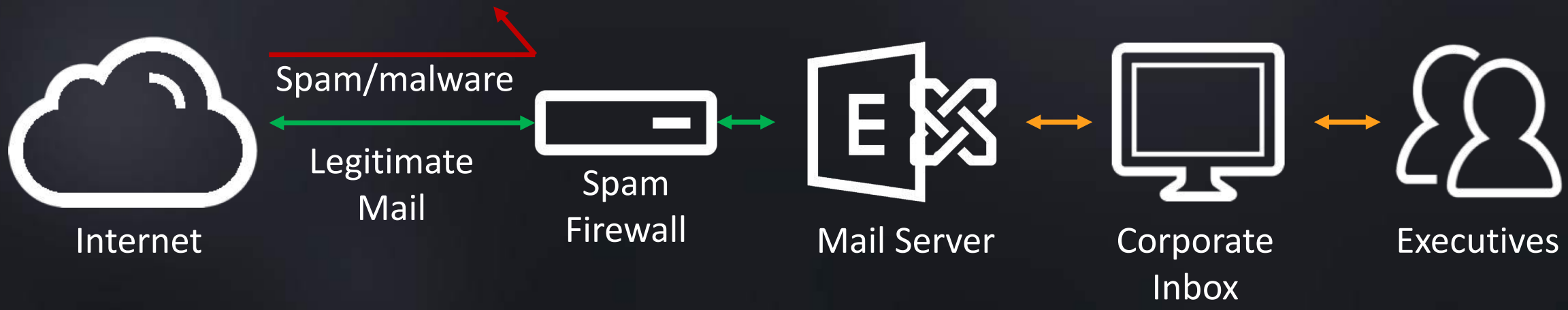


Barracuda Networks

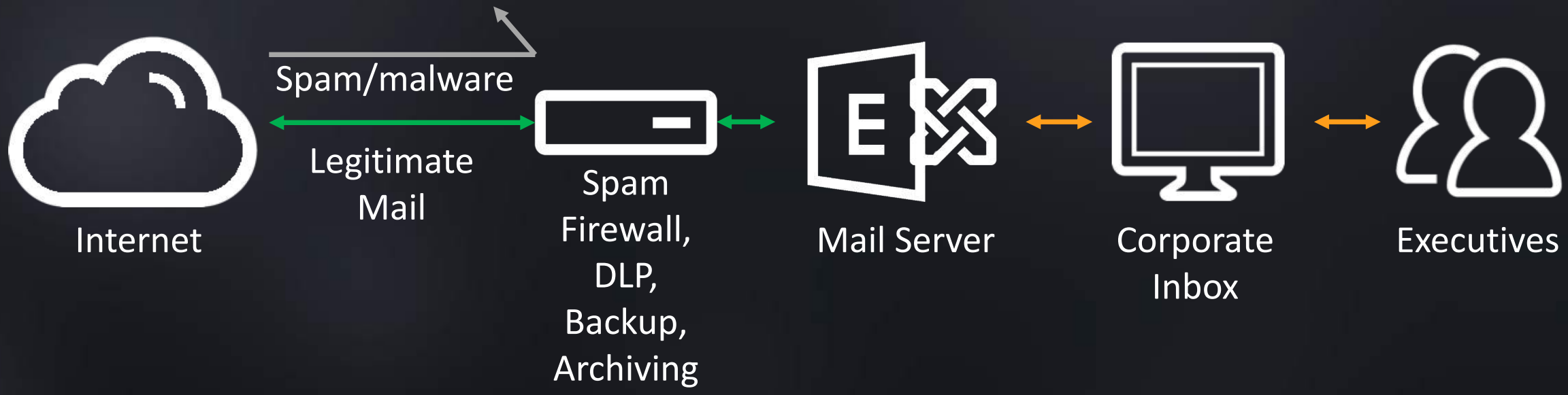
- Protecting and processing **1 billion** emails a day
- **Over 60,000** email protection customers
- Artificial Intelligence email threat defense engine trained on **2.5 million** emails
- **17 billion** messages archived
- Leader in spam and virus prevention **since 2003**

In the early days, it was simple

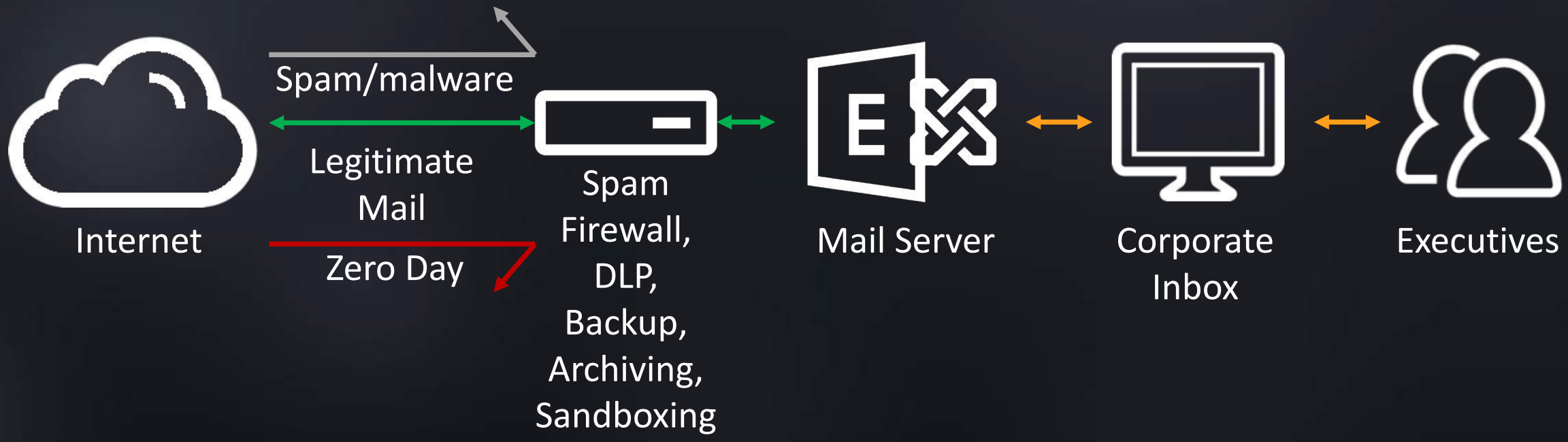
Spam firewalls kept bad things out



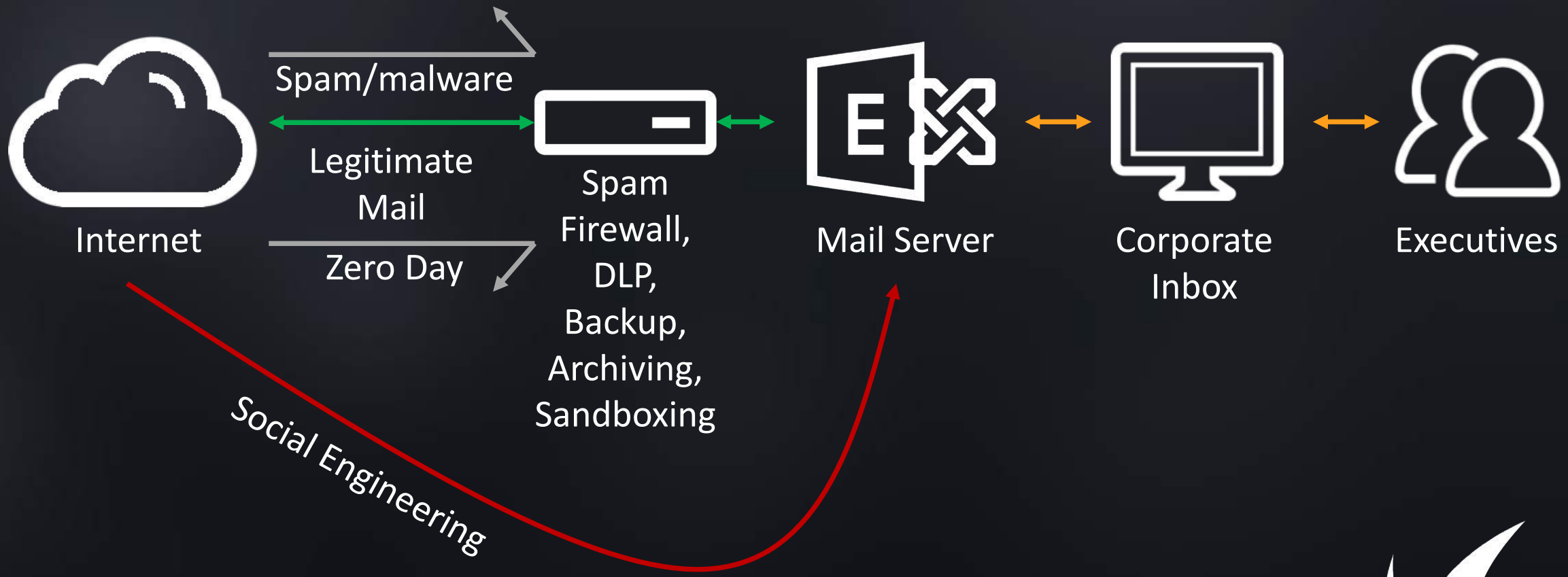
Over time, we built a better gateway



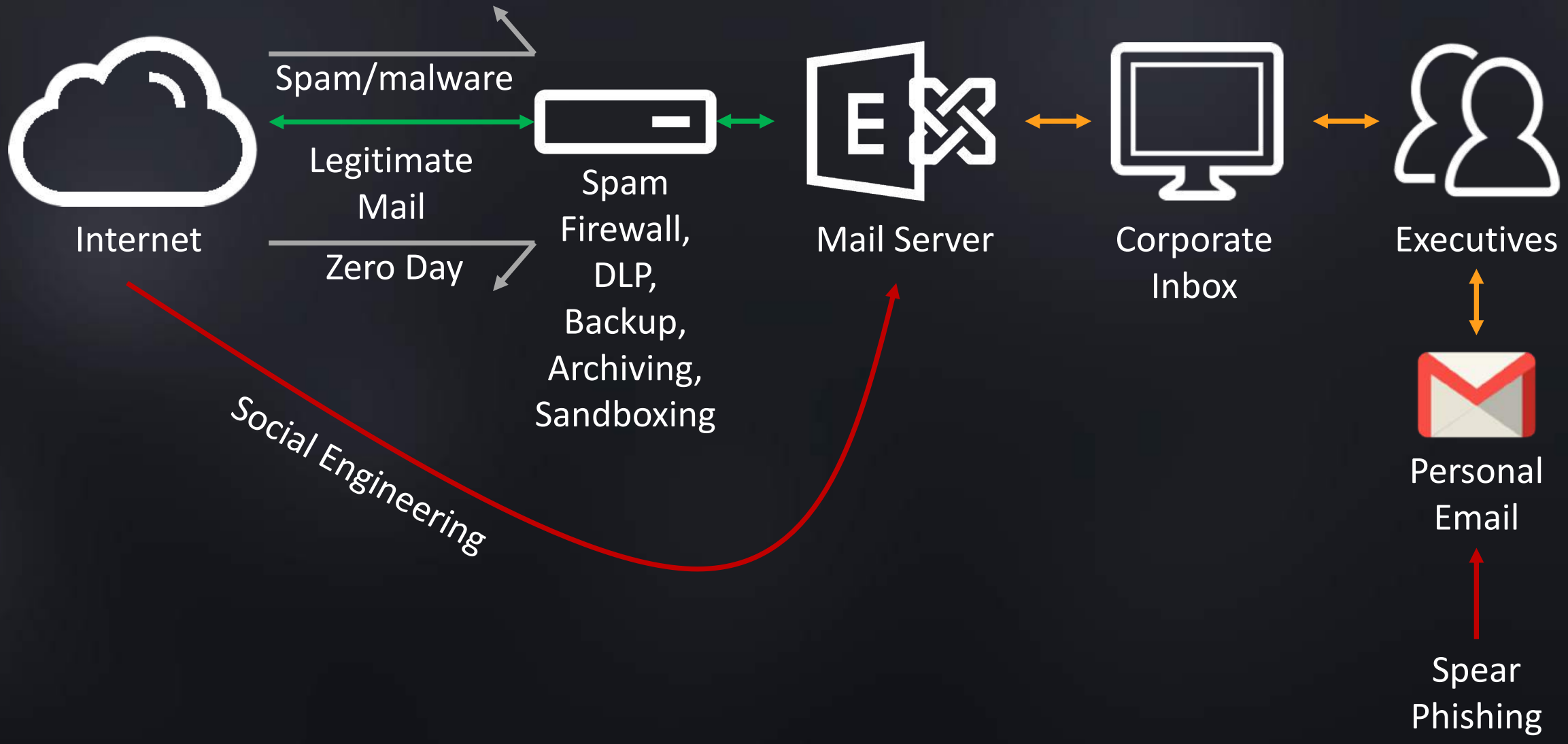
Sandboxing stopped zero day threats



But gateways are blind to social engineering

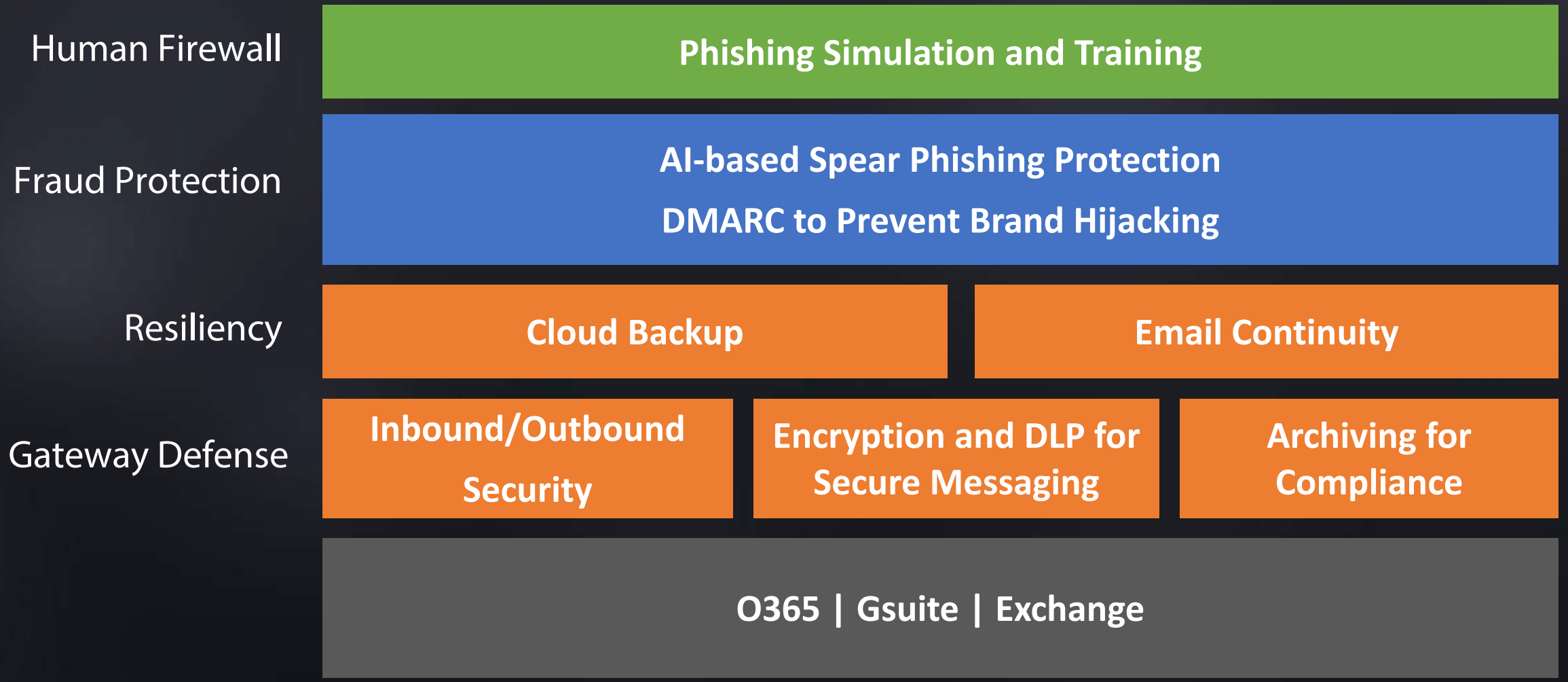


And attacks are coming in through the back door

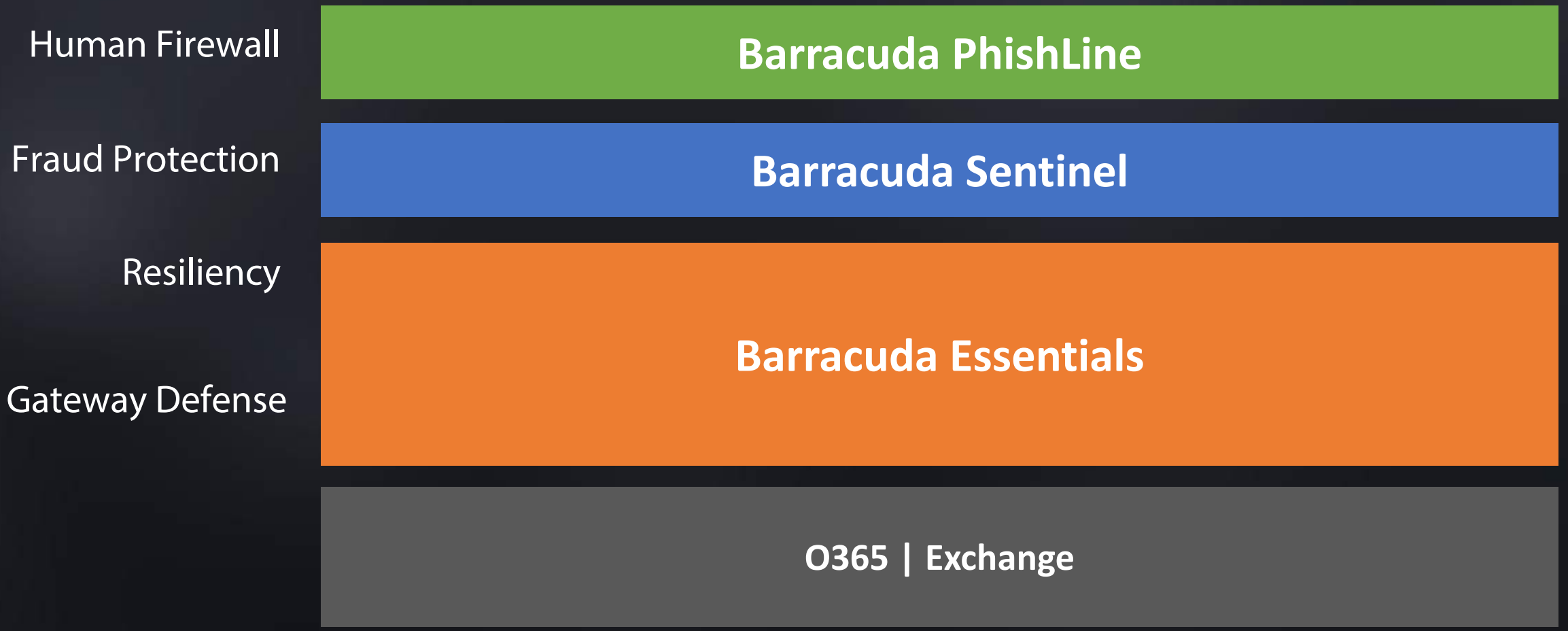


Securing the gateway is still **necessary**, but **no longer sufficient**

Next Generation Email Protection



Barracuda Email Protection



Gateway Defense
Barracuda Essentials

Barracuda PhishLine

Barracuda Sentinel

Barracuda Essentials

O365 | Exchange

Barracuda Essentials

Comprehensive security, archiving, and backup solution

- Office 365, on-premises and hybrid
- Simple quoting/bundling
- Per user licensing
- Web-based management

Advanced Email Security

Easy-to-Use, Cloud-Based Email Security

- Inbound/Outbound Scanning
- Email Continuity
- Secure Messaging (Encryption, DLP)

Prevent Advanced Threats

Barracuda Advanced Threat Protection

- Multi layered threat protection
- Optimized for speed and efficacy
- Global threat intelligence network

Compliance Archiving

Cloud-based archiving for compliance and eDiscovery

- Immutable journaled archiving
- eDiscovery search, hold, and export
- Mobile access

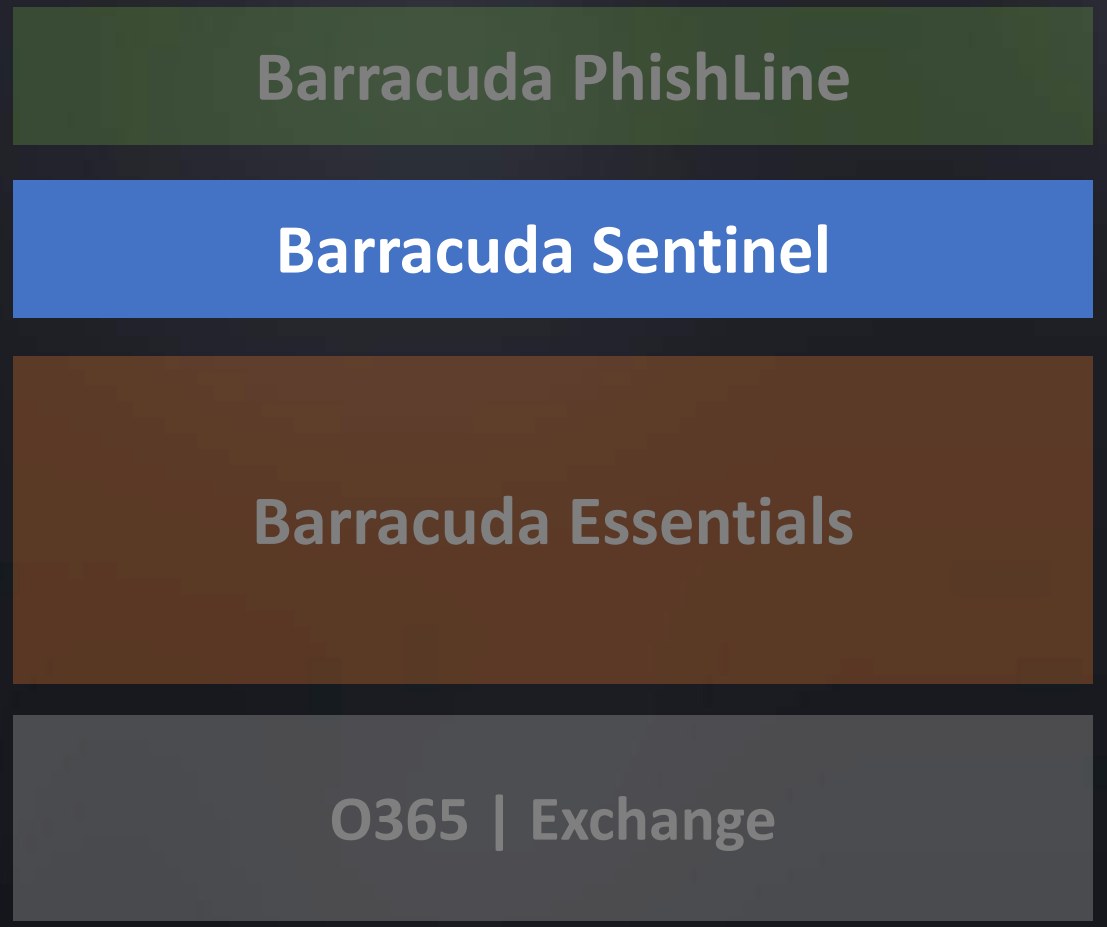
Cloud Backup

Protects Office 365 mailboxes, SharePoint, and OneDrive for Business

- Protect against accidental deletion
- Set custom retention policies
- Multi-selection restores
- Download files locally

Fraud Protection

Barracuda Sentinel



AI for Real-Time Spear Phishing Prevention

Machine learning protects against “zero payload” attacks

- Trained on 2.5 million mailboxes
- Analyzes 40 features
- <1:1,000,000 false positive rate
- Detects attacks gateways can’t see

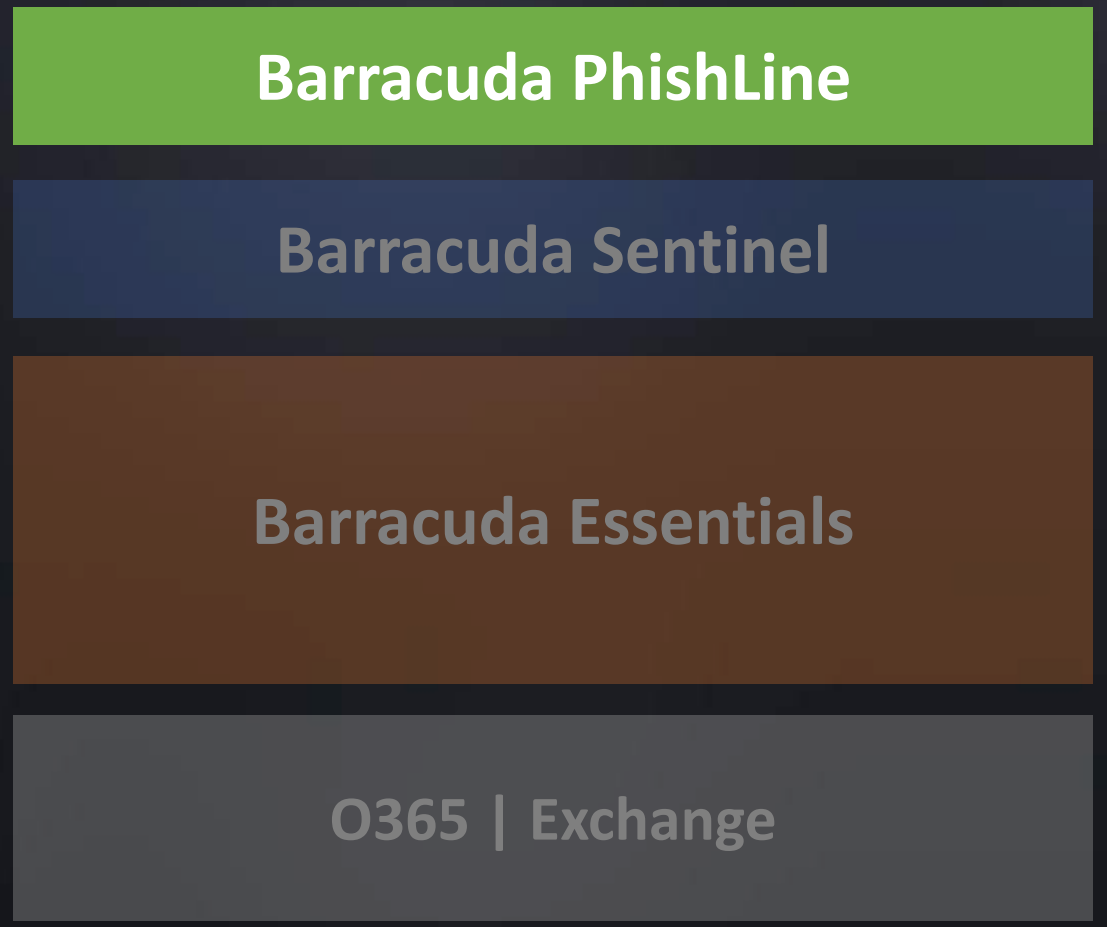
Brand Fraud Prevention with DMARC Reporting

Instant visibility into brand use and misuse

- Rich reporting into brand usage
- Allows rapid remediation of misuse
- Stops brand erosion
- Helps email deliverability and trust

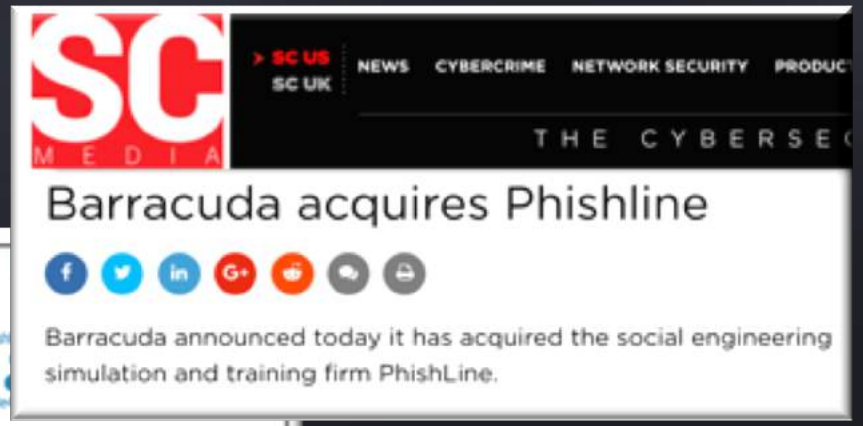
Human Firewall

Barracuda PhishLine



Barracuda PhishLine

- Acquired 12/2017
- Enterprise grade, Gartner visionary
- Unique, differentiated offering in Barracuda portfolio



Phishing Simulation

Test and train high risk users

- Turns users from liability to strength
- Pre-built templates for quick time to value
- Assess risk in a non-threatening manner

Phishing Training

Modular training courses

- Large inventory of turnkey content
- Continual updates stay fresh and relevant
- Gamification drives engagement

Proven Success

Worldwide Adoption

BEDFORD
BOROUGH COUNCIL

WELLINGTON
COLLEGE

Mid Cheshire Hospitals
NHS Foundation Trust
NHS

SKIWORLD

CRUISE AMERICA
RV RENTAL & SALES

WEST MIDLANDS FIRE SERVICE

BUFFALO WILD WINGS
GRILL & BAR

FARO®

FREEDOMPAY

Case Study – Regional Airline

Challenges: Spam and Account Compromise

- Employees inundated with spam
- Victim of crypto ransomware
- Account compromise via O365 login

Solution: Essentials and Sentinel

- Essentials - intuitive interface, granular control and, competitive pricing.
- Sentinel - growing capabilities every week

Results: Eliminated Spam and Account Compromise

- Enormous drop in the number of email attacks, virus and malware traffic
- Sentinel catching targeted spear phishing attacks
- Reduced stress in IT department

Case Study – Private Insurance Company

Property & Casualty Insurance Company
- IT Director joined in 2014
- Inherited outdated infrastructure
- Standardized on Office 365

Office 365 Exchange Online Protection (EOP)
- First 6 months – all was good
- Later, had significant CEO spoofing and spear phishing scares
- Didn’t have resources to “micro manage” EOP

Turned to Barracuda Essentials for Office 365
- Success with Barracuda Backup
- Enabled Email Security Service + Advanced Threat Protection
- Since activating - SPAM numbers and threat levels “dramatically down”

Case Study – Optometrist Retailer

Multi-state Eyeglasses & Optometrist Retailer

- 35 states/157 locations/650+ users
- Standardized on Office 365

Office 365 Compliance Did Not Satisfy Requirements

- In-Place preservation did not prevent deletion
- Needed cloud-based email archiving

Solution – Barracuda Cloud Archiving Service

- Easily generated audit logs for compliance
- Non-intrusive, “set it and forget it” operation

Next Steps

Leverage ETS solution
https://scan.barracuda.com

Start a 30 day trials

https://www.barracuda.com/essentials

Thank You

BIG UNIVERSITY 2018

Keynote Speaker

"Catch Me If You Can"
Frank Abagnale, Jr.

Thank you to our sponsors

Barley Snyder
ATTORNEYS AT LAW

Barracuda

CISCO

D&H

DUO

KnowBe4
Human error. Conquered.

McCONKEY & CO.
INSURANCE & BENEFITS
Innovative Solutions. Traditional Values.

VIEWPOINT

RADWIN

ydop
Near-user Marketing®