The Modern Threat Landscape

HOW TO MANAGE CYBERSECURITY RISK

Marius Baczynski

Head of CyberSecurity Sales

EMEAR-CENTRAL

CISCO

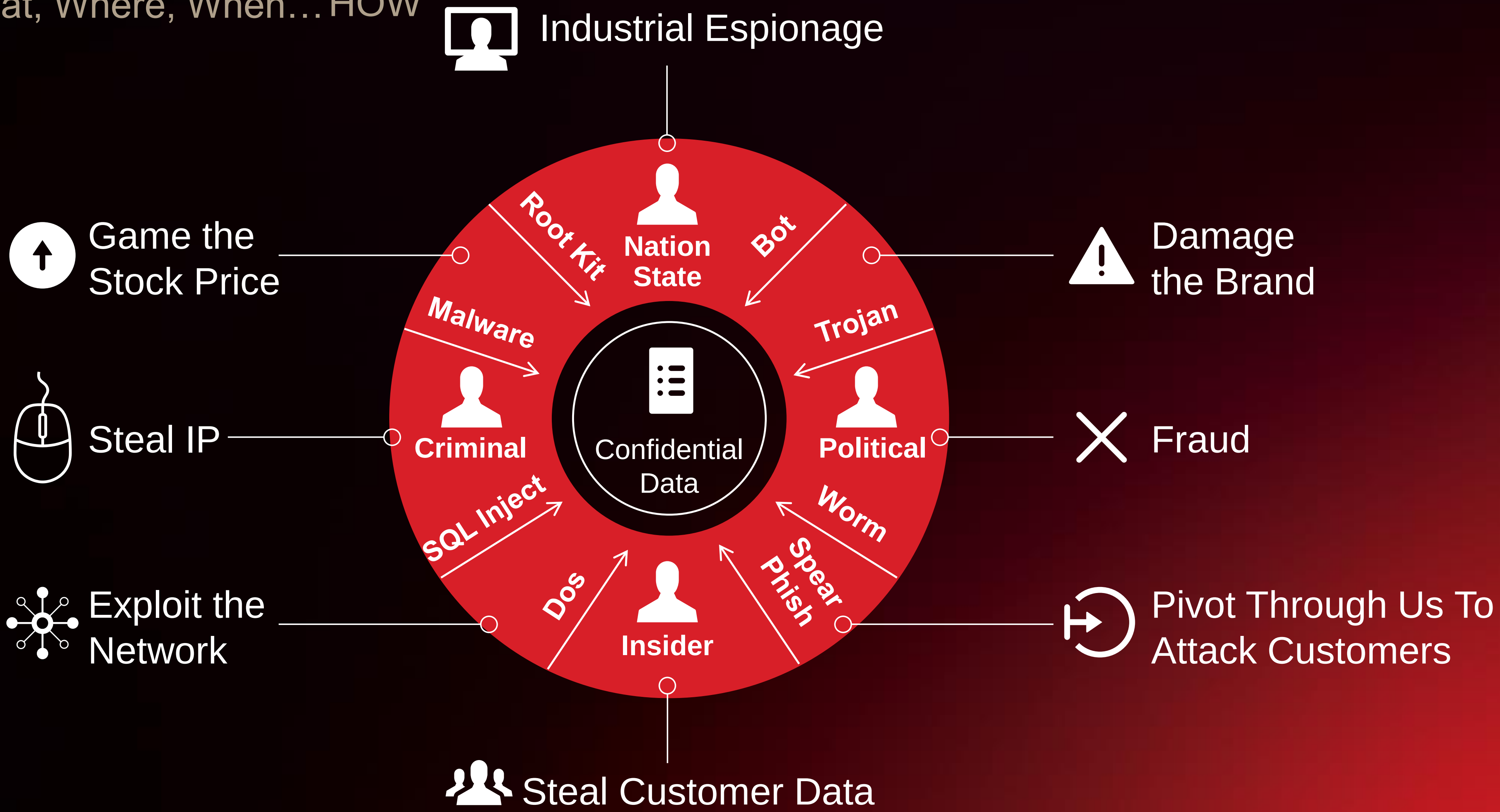
Bratislava, 1/03/2016

“In the world there are two types of organisations: those, who have been hacked and those, who don’t know about it”

John Chambers

A Security Executives’ business challenges

Who, What, Where, When…HOW



Industrial Espionage

Game the Stock Price

Damage the Brand

Steal IP

Fraud

Exploit the Network

Pivot Through Us To Attack Customers

Steal Customer Data

Nation State

Criminal

Political

Insider

Root Kit

Bot

Malware

Trojan

SQL Inject

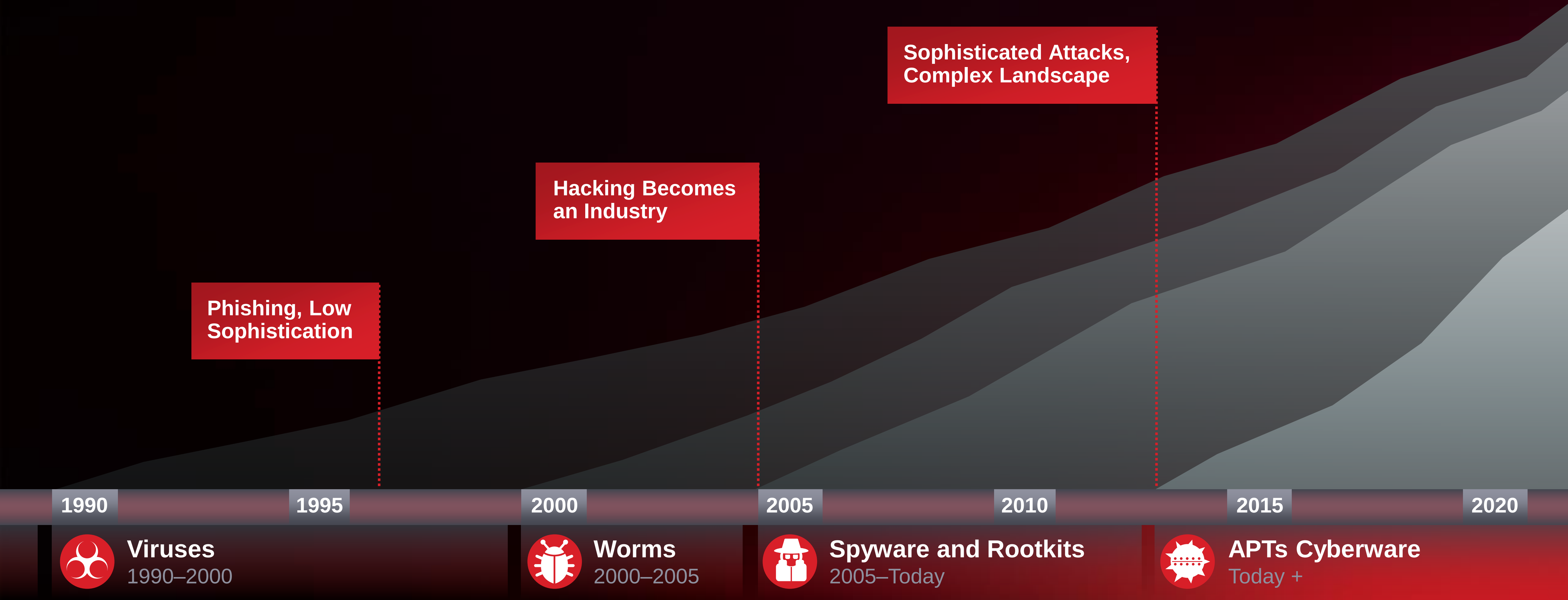
Worm

Dos

Spear Phish

Confidential Data

The Industrialization of Hacking



Phishing, Low Sophistication

Hacking Becomes an Industry

Sophisticated Attacks, Complex Landscape

Viruses
1990–2000

Worms
2000–2005

Spyware and Rootkits
2005–Today

APTs Cyberware
Today +

Welcome to the Hackers’ Economy

There is a multi-billion dollar global industry targeting your prized assets

$450 Billion
to
$1 Trillion

Malware Development
$2500 (commercial malware)

Social Security
$1

Exploits
$1000-$300K

Credit Card Data
$0.25-$60

DDoS

DDoS as A Service
~$7/hour

Bank Account Info
>$1000 depending on account type and balance

Facebook Accounts
$1 for an account with 15 friends

Mobile Malware
$150

Medical Records
>$50

Spam
$50/500K emails

Direct Attacks Generate Big Profits

More efficient and more lucrative

$300 X **317.18** X **365** = **$34M**

average ransom

ransoms paid per day

days in a year

gross yearly income for ransomware per campaign

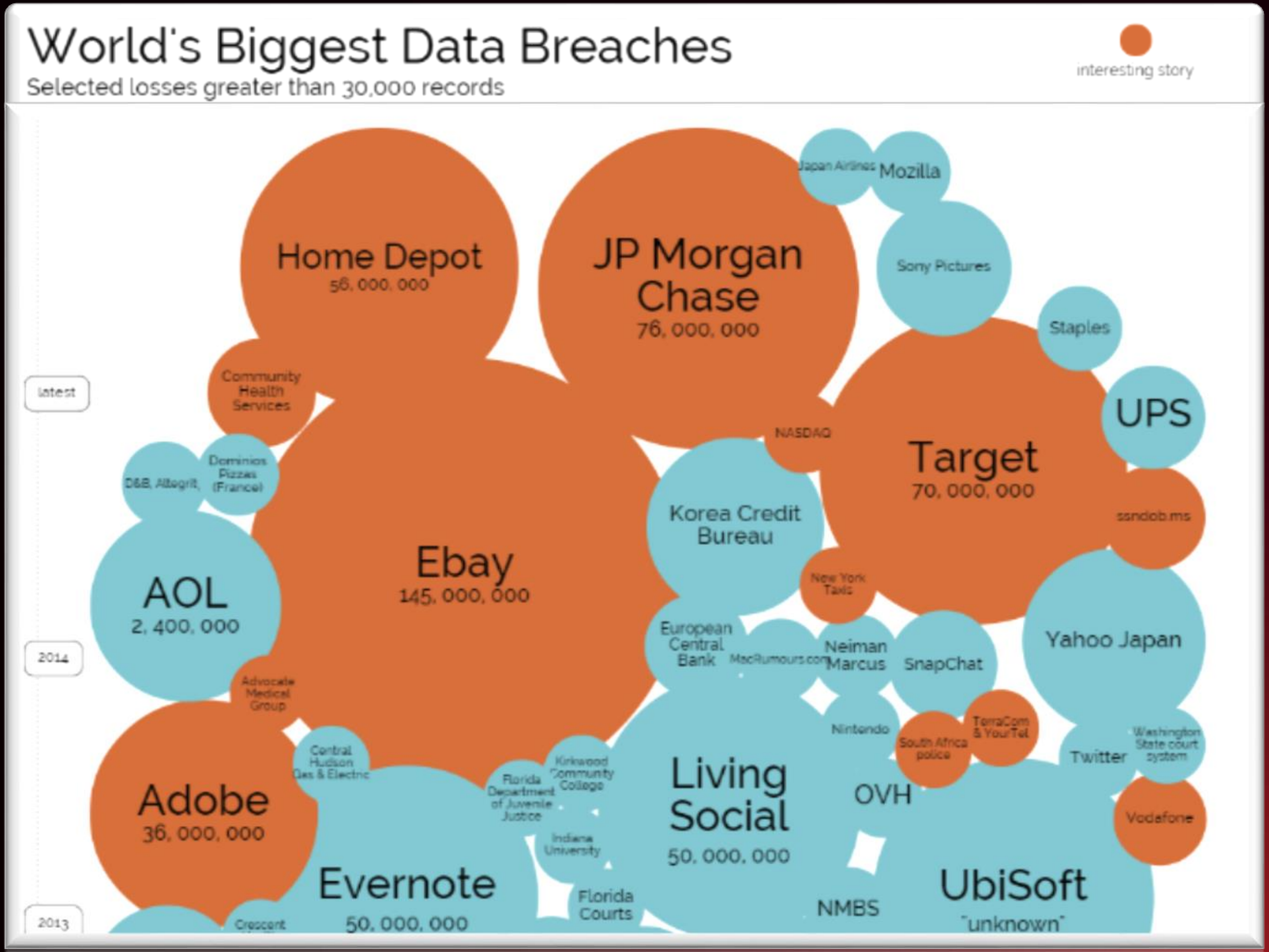
The Security Problem

Maintaining Security and Compliance as business models change (Agility)

Staying ahead in a very dynamic threat landscape

Reducing complexity and fragmentation of security solutions

Living in Dangerous Times



World's Biggest Data Breaches

Selected losses greater than 30,000 records

Cisco's 2015 Security Capabilities Benchmark Study

Conducted over the Summer of 2015

Study Included 12 Countries

US
Mexico
Brazil
UK
France
Germany
Italy
Russia
India
Australia
China
Japan

Over 2400 Respondents

• CSOs	45%
SecOps	55%
• Large Enterprise	13%
Enterprise	38%
Midmarket	49%

Security Weighs on the Minds of Executives

48% Of Executives Very Concerned About Security

41% Much More Concerned Than 3 Years Ago

92% Agreed More Information Will Be Expected

Attack Awareness Fades Confidence

59%

confident in having the latest technology

-5%

51%

have strong confidence in ability to detect a security weakness in advance

0%

54%

have strong confidence in ability to defend against attacks

-4%

45%

have strong confidence in ability to scope and contain an attack

-1%

54%

have strong confidence in ability to verify an attack

+0%

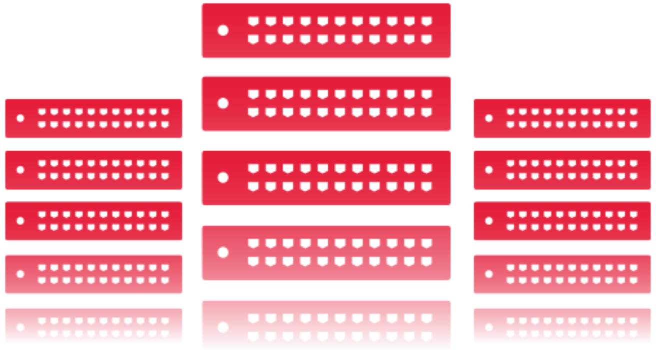
56%

review security policies on a regular basis

+0%

DNS: Doth Protest Too Much

A blind spot for attackers to gain command and control, exfiltrate data, and redirect traffic



91.3%

of malware uses DNS

68%

of organizations
don’t monitor it

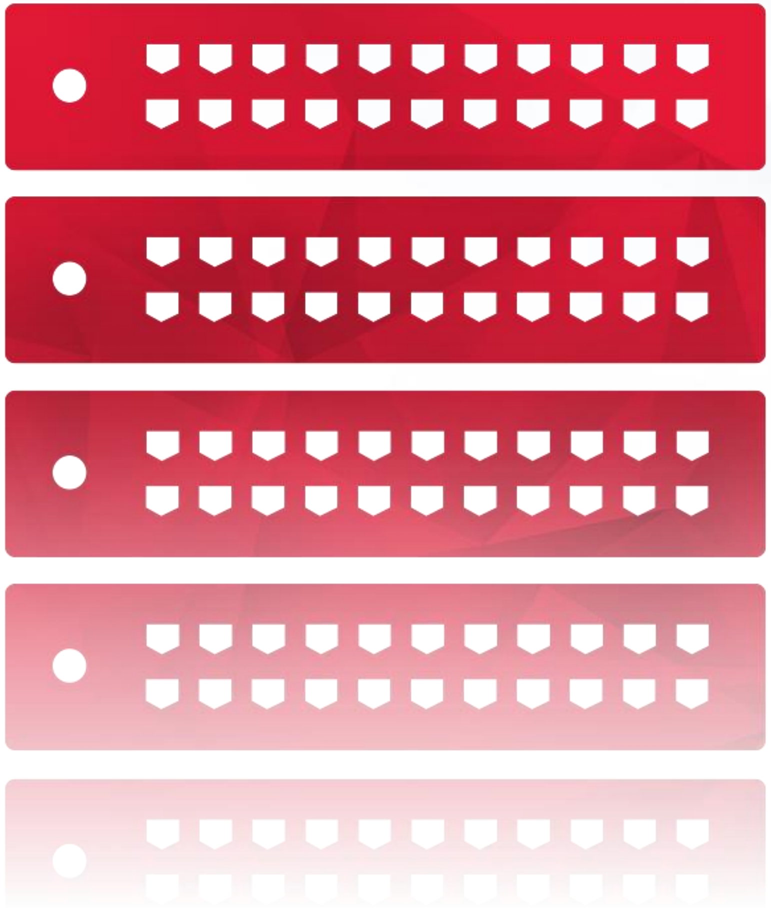
Browser Infections: The Pest That Persists

More than

85%

of the companies studied
were affected each month

“Patchwork Complexity” Breeds Complacency



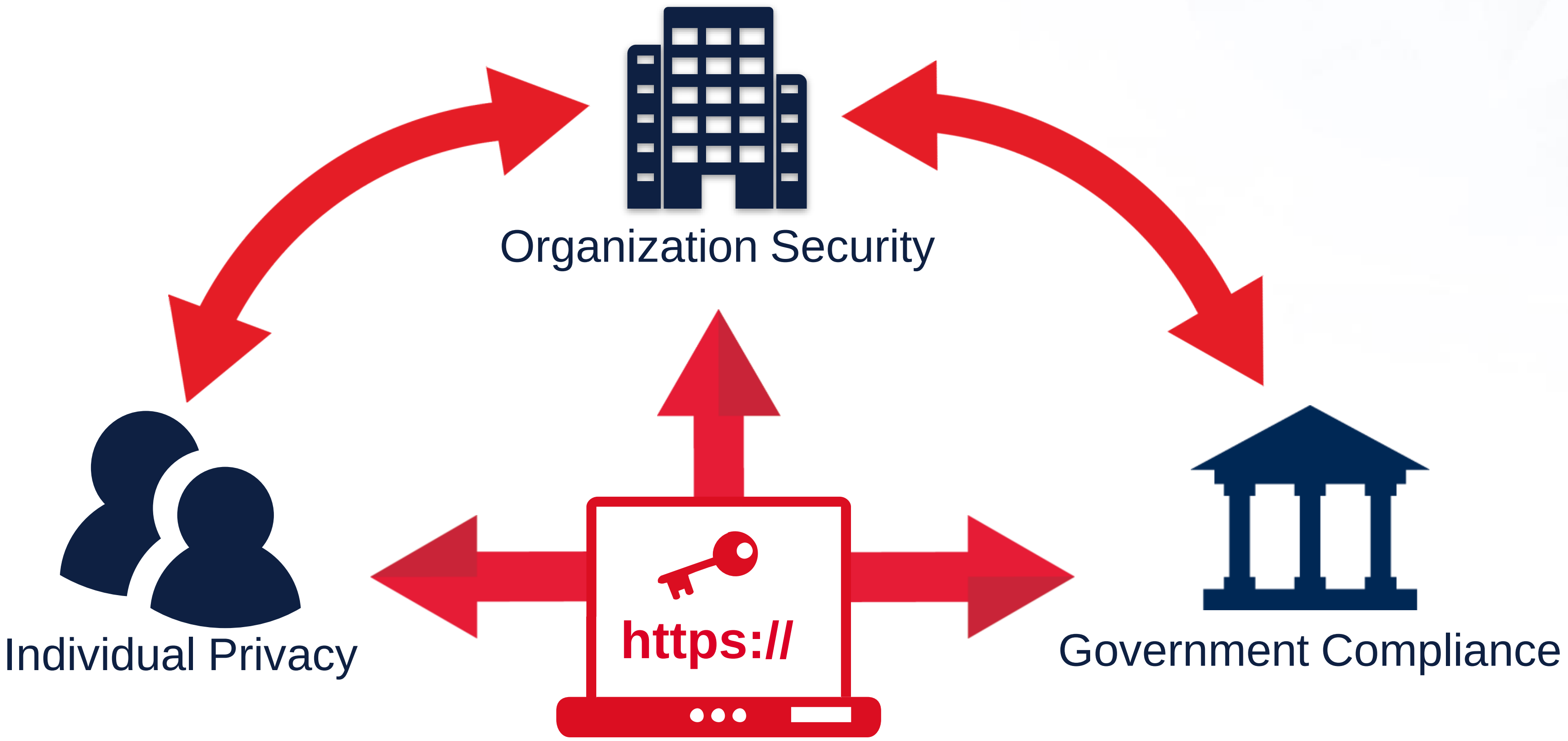
92% Of devices surveyed across the Internet were running known vulnerabilities with an average of 26 each

31% Of devices surveyed across the Internet were End of Service

5% Of devices surveyed across the Internet were End of Life

Encrypted Traffic: A Sign of the Times

The growing trend of web encryption creates false sense of security and blind spots for defenders



Organization Security

Individual Privacy

https://

Government Compliance

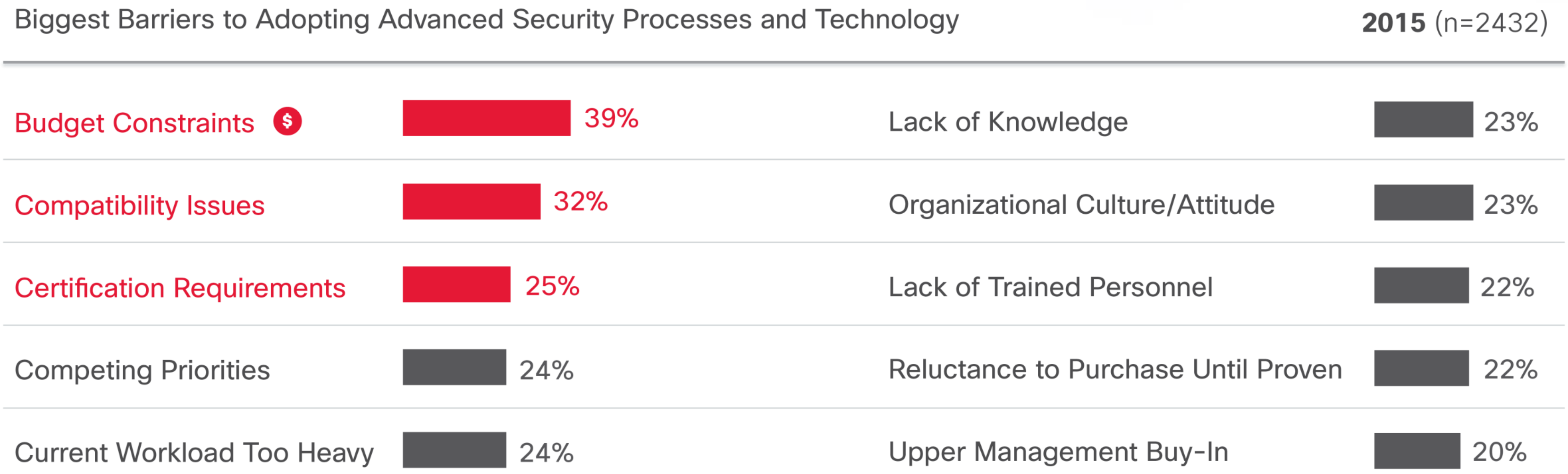
Encrypted Traffic is Increasing
It represents over 50% of bytes transferred

Increased Awareness Drives Effort

More organizations are taking actions to become more prepared for what’s going to happen.

Security Awareness and Training	90%	+1%
Formal Written Policies	66%	+7%
Outsource Audit and Consulting	52%	+1%
Outsource Incident Response	42%	+7%
Outsource Threat Intelligence	39%	N/A

Constraints: Budget, Compatibility, and Certification



Security teams may be limited in their ability to carry out their plans

VERIZON
Annual Data Breach Report

$100 billion

63,000

Annual loss to US Economy

Verizon DBR Confirmed Incidents

1.3 billion

$3.5 million

Usernames and Passwords Stolen

$148 million

Average Cost per Incident

Target Breach Expenses

If you KNEW you were going to be compromised, what would you do differently?

Today there is no such thing as a ‘magic box’ to solve your CyberSecurity challenge.

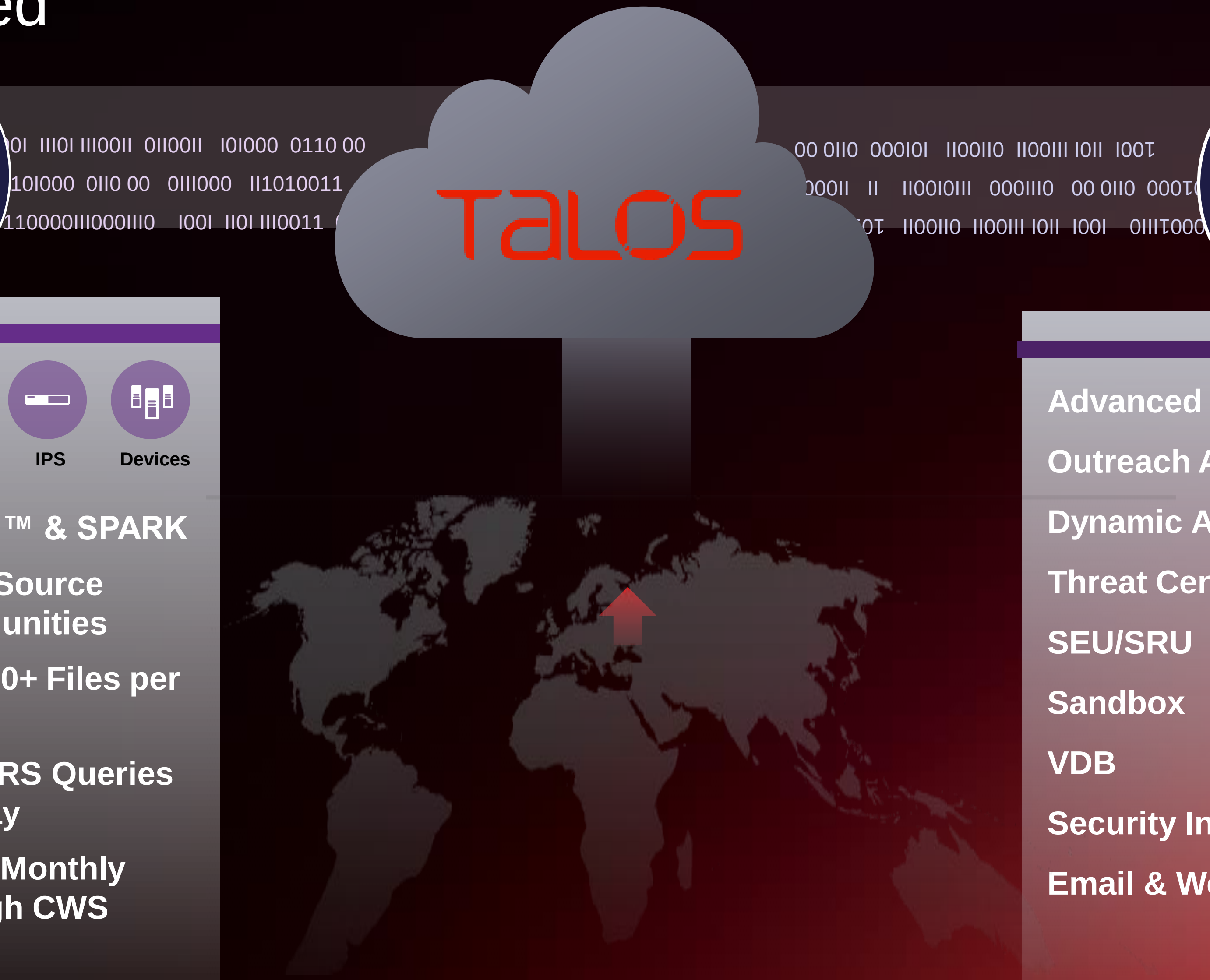
Information Superiority is a PREREQUISITE for enabling organisations to defend themselves.

Threat Focused

Threat Intelligence

Email
Endpoints
Web
Networks
IPS
Devices

- 100 TB Intelligence
- 1.6M sensors
- 150 million+ endpoints
- 35% email worldwide
- FireAMP™, 3+ million
- 13B web req
- AEGIS™ & SPARK
- Open Source Communities
- 180,000+ Files per Day
- 1B SBRS Queries per Day
- 3.6PB Monthly through CWS


0I IIIOI IIIOOII OIIOOII IOIOOO 0110 00
1OIOOO OIIO 00 OIIIOOO II1010011
110000IIIOOOIIIO IOOI IIOI III0011
TALOS
00 OIIO OOOIOI IIOOIIO IIOOIII IOII IOOT
OOOII II IIOOIOIII OOOIIIO 00 OIIO OOOT
OT IIOOIIO IIOOIII IOII IOOI OIIIT000

Research Response

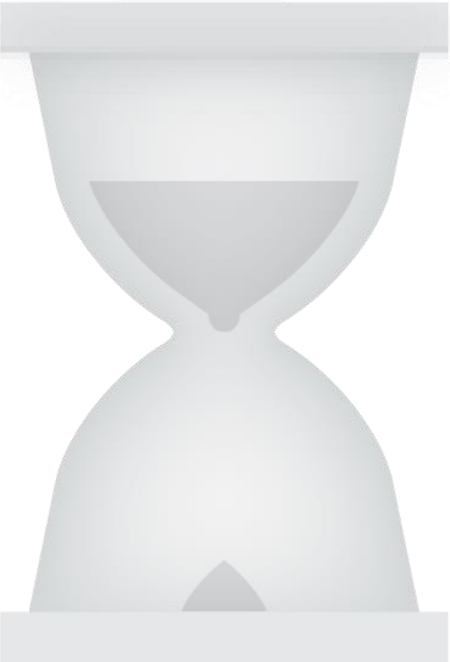
- Advanced Industry Disclosures
- Outreach Activities
- Dynamic Analysis
- Threat Centric Detection Content
- SEU/SRU
- Sandbox
- VDB
- Security Intelligence
- Email & Web Reputation

Time to Detection: Reducing Malicious Actors’ Unconstrained Operational Space

June (Median)

35.3

HOURS



VS

October (Median)

17.5

HOURS

Cisco far outpaces the current industry estimate of 100 to 200 days

The ‘Secret Sauce’

Visibility-Driven

Network-Integrated, Broad Sensor Base, Context and Automation

Threat-Focused

Continuous Advanced Threat Protection, Cloud-Based Security Intelligence

Architecture Focused

Agile and Open Platforms, Built for Scale, Consistent Control, Management

Network

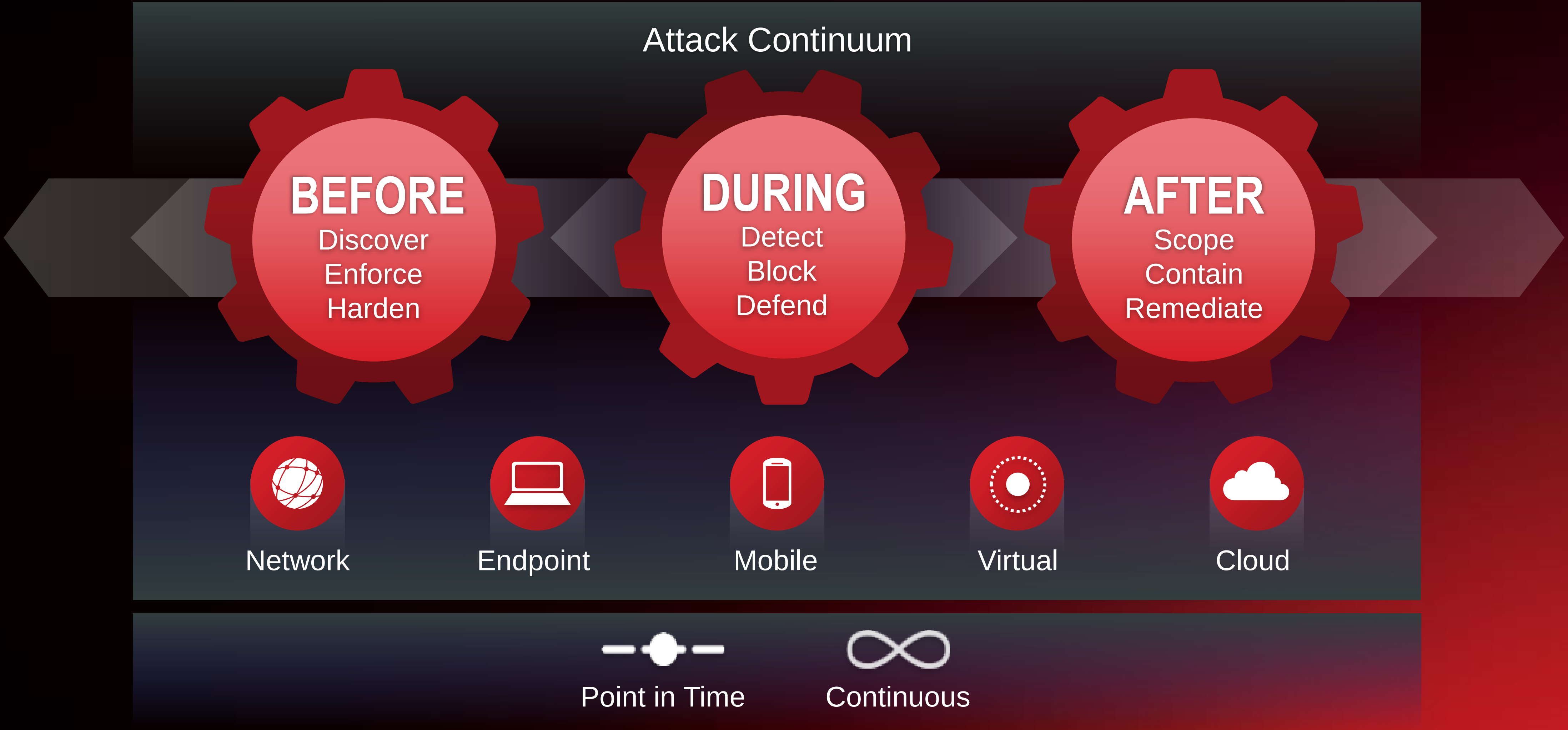
Endpoint

Mobile

Virtual

Cloud

The New Security Model



Attack Continuum

BEFORE
Discover
Enforce
Harden

DURING
Detect
Block
Defend

AFTER
Scope
Contain
Remediate

Network
Endpoint
Mobile
Virtual
Cloud

Point in Time
Continuous

How to Manage CyberSecurity Risk?...

1. Don’t focus on compliance – identify and manage YOUR critical risk.
2. Don’t focus on IT assets – protect BUSINESS OUTCOMES.
3. Treat CyberSecurity as ‘FACILITATION’, not ‘limitation’.
4. People are the weakest link – make CyberSecurity PEOPLE-centric.
5. There is no such thing as ‘perfect’ – you WILL be compromised:
   - ➢ *Do what you can to **MAKE IT MORE DIFFICULT** for cybercryminals to ‘breach the hull’.*
   - ➢ *Invest in **TECHNOLOGY**, **POLICY** and **SERVICES** to detect and manage compromise.*
   - ➢ *Invest in **RETROSPECTION** to ensure the same compromise will not happen twice.*

Thank You.

2016 Annual Security Report
www.cisco.com/go/asr2016