

Your Time Is Now

Cisco
Connect

Portorož, 15. in 16. marec 2017



Your Time Is Now

What can we lose not
implementing proper
security in our IT
environment?

Aleksandar Pavlovic
Security Account Manager
Cisco

Cisco
Connect

Portorož, 15. in 16. marec 2017



Increasing Digital Traffic Creates a Greater Attack Surface

Global IP Traffic to Triple by 2020



2.3

ZB
Annual global
IP traffic



66%

of IP traffic will be
from Wi-Fi and
mobile devices



82%

of all consumer
Internet traffic
will be video



2x

Broadband
speeds will
double

Crack in the Bottom Line

Over 25% of Revenue at Risk from a Security Breach

29%

experienced a
loss of revenue

38% of them experienced a significant loss (>20%)

Global

2017 Security Capabilities Benchmark Study



- 16 billion web requests a day
- 600 billion emails a day
- In aggregate, block almost 20 billion threats per day
 - More than 1.5 million unique malware samples daily
- 18.5 billion AMP queries



CloudLock Telemetry

- 10 million users under management
- 15 billion user activities being tracked
- 222,000 apps discovered
- 1 billion files monitored daily



Conducted over the summer of 2016



Study included 13 countries

United States	China
Brazil	India
Germany	Japan
Italy	Mexico
United Kingdom	Russia
Australia	France
	Canada



Over 2900 respondents

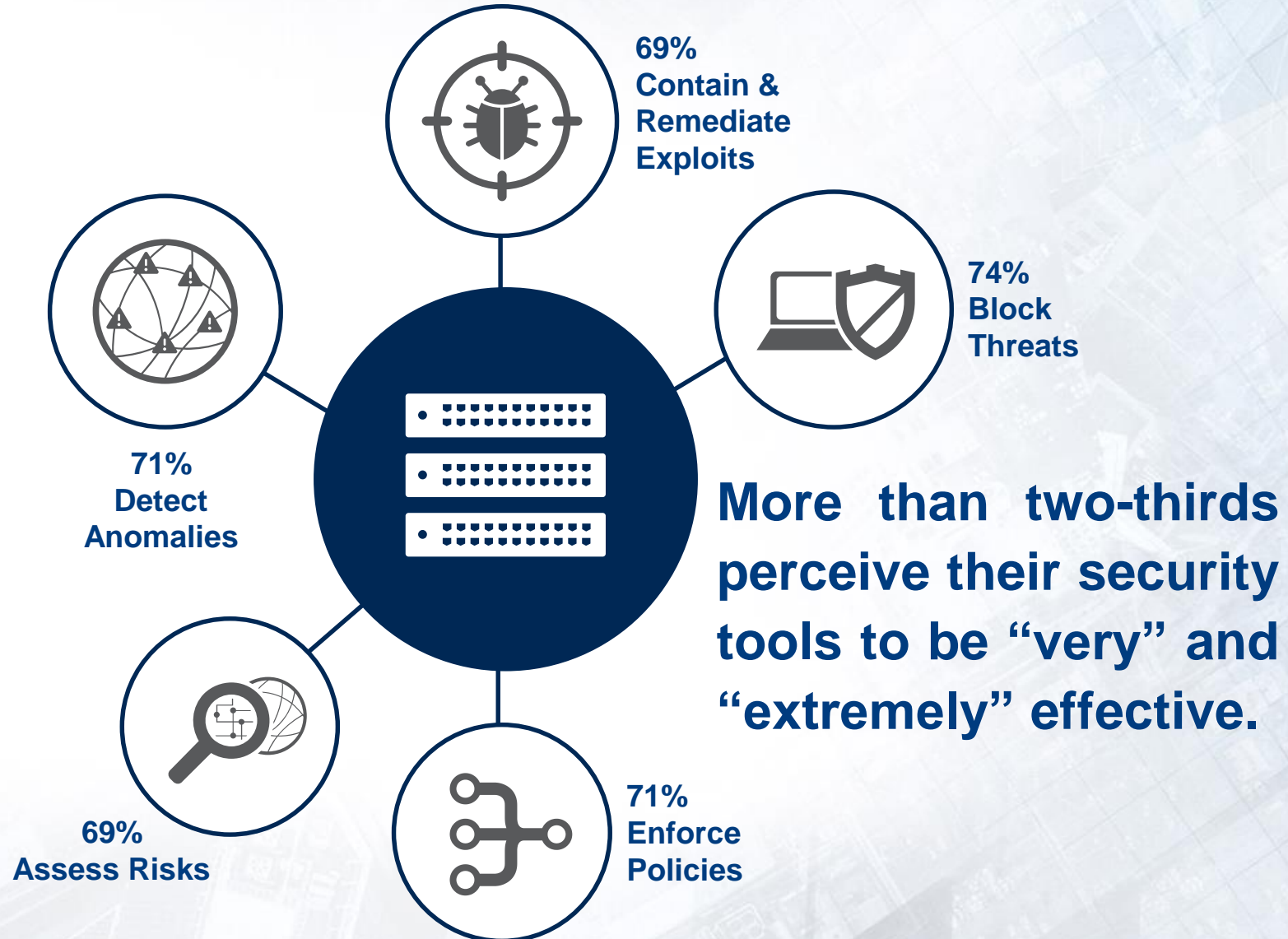
CSOs	49%
SecOps	51%
Large enterprise	12%
Enterprise	38%
Midmarket	50%

Perception

High confidence in tools

58%

of professionals
feel their security
infrastructure is
very up to date.



Out in the Open

Half of Organizations Come Under Public Scrutiny Due to Security Breach



49% of organizations have
faced public scrutiny
of a security breach

How did this most recent breach become known externally?

50%
Voluntary
Disclosure

31%
Involuntary
Disclosure

31%
Reporting
Requirements

The Top 4 Sources of Concern

Which Security Professionals Found in Defending Against a Cyberattack



Mobile Devices

58%



Data in Public Cloud

57%



Cloud Infrastructure

57%

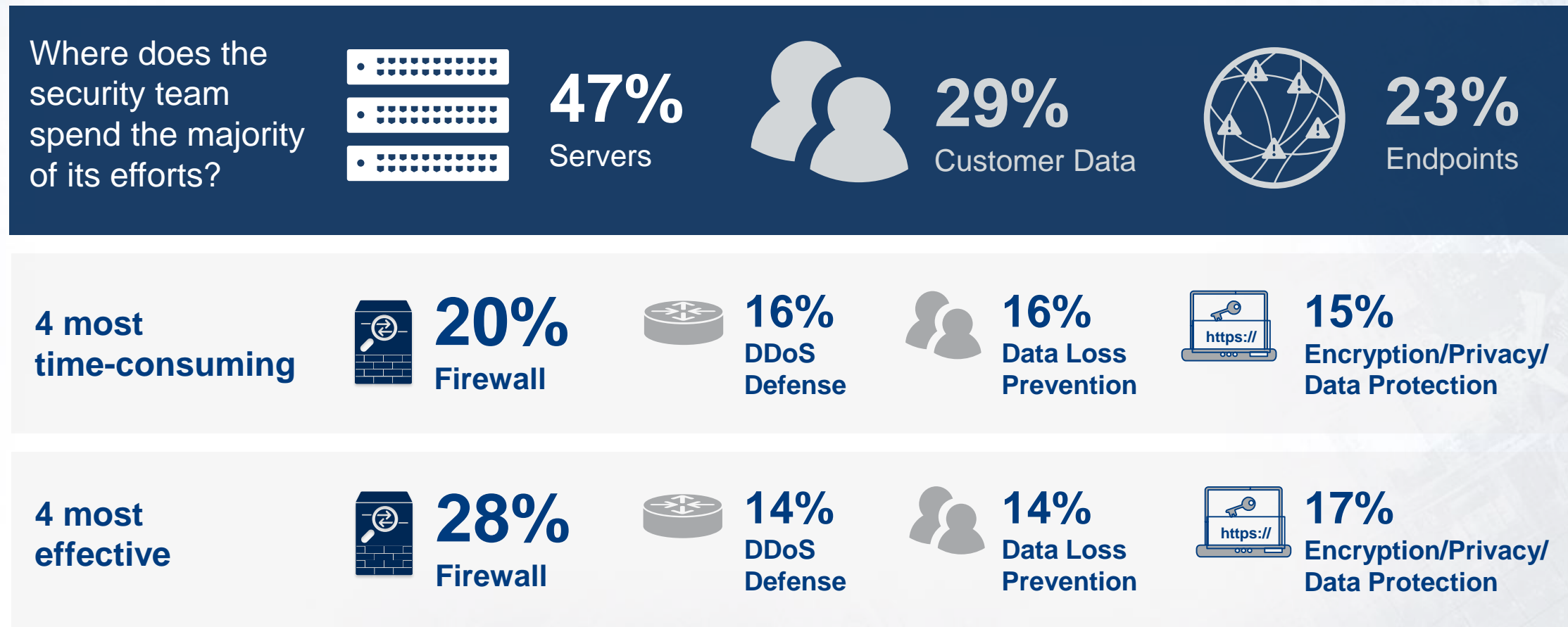



User Behavior

57%

Hard to Defend

Effort and Time Spent on Areas of Concern





Email is still the #1 threat vector
(people are still the weakest link)



Cisco is a Market Leader for Secure Email Gateways for a Whole Decade

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Cisco.

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Gartner's Magic Quadrant for Secure Email Gateways
Peter Firstbrook, Neil Wynne, June 29, 2015

Figure 1. Magic Quadrant for Secure Email Gateways

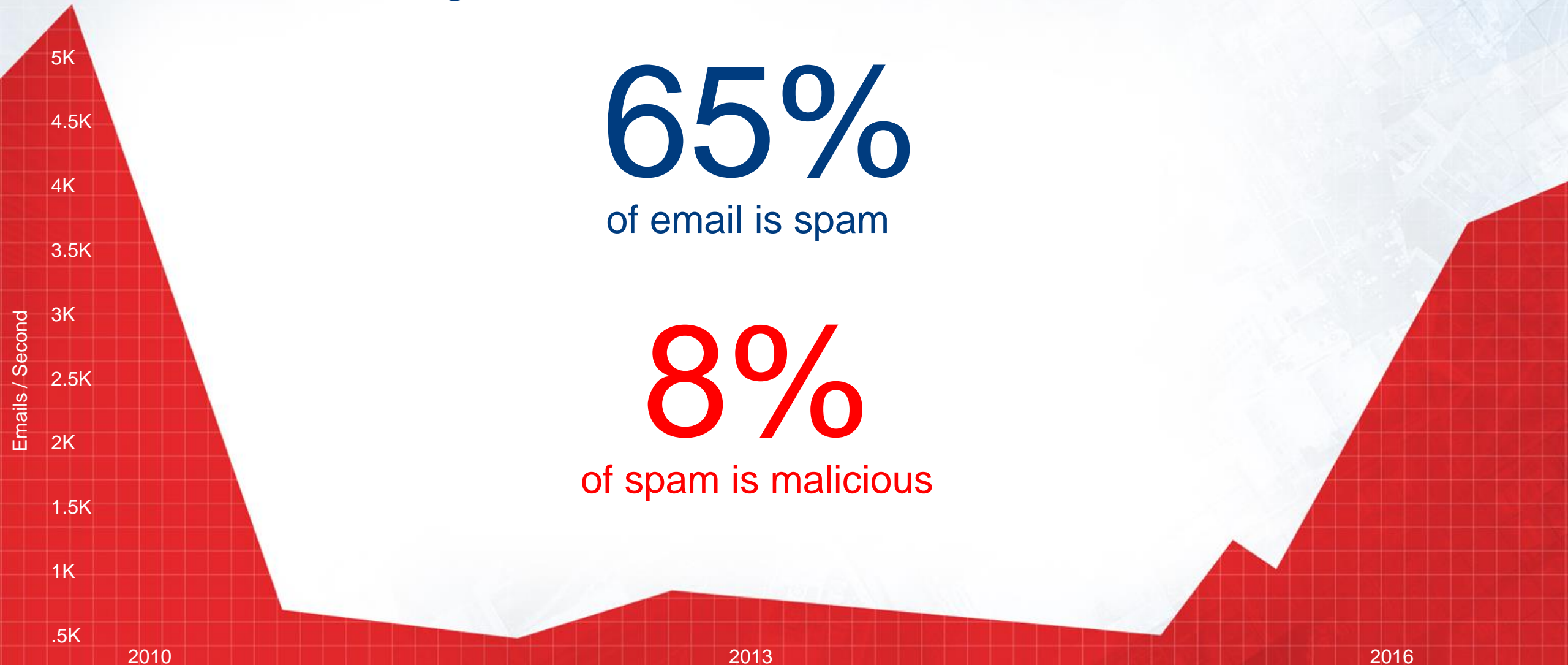


Spam Comes Roaring Back

Email is Back in Vogue

65%
of email is spam

8%
of spam is malicious



Phishing leaves businesses on the line

Cisco
Connect



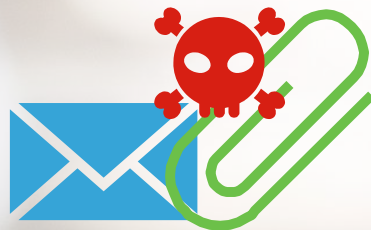
Phishing



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

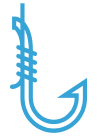
Messages contain
attachments and URL's

Socially engendered
messages are well crafted
and specific

Credential "hooks" give
criminals access to your
systems

Spoofing rates are on the rise

Cisco
Connect



Phishing



Spoofing



Ransomware



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

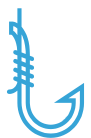
Forged addresses
fool recipients

Threat actors extensively
research targets

Money and sensitive
information are targeted

Ransomware holding companies hostage

Cisco
Connect



Phishing



Spoofing



Ransomware



Ransomware represents the biggest jump in occurrences of crimeware¹

\$60M



Cost to consumers and companies of a single campaign²

9,515

users are paying ransoms per month²

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

Malware encrypts
critical files

Locking you out of your
own system

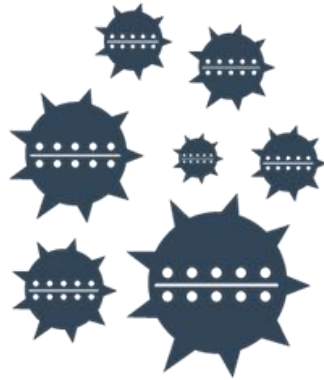
Extortion demands
are made

Process of Attacks



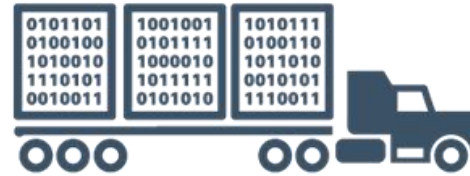
Recon

**Research,
identify and
select targets**



Weaponization

**Pair remote access
malware with exploits**



Delivery

**Deliver cyberweapons
by email, website and
attachments**



Installation

**Install payloads to
gain persistent
access**

Obstacles to Advancing Security

Business Constraints

35%

Budget

(-4%)

28%

Compatibility
Issues

(-4%)

25%

Lack of Trained
Personnel

(+3%)

25%

Certification
Requirements

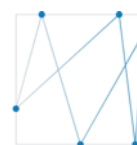
(+/-0%)

(Change from 2015)

Complexity



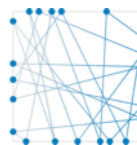
1-5 (45%)



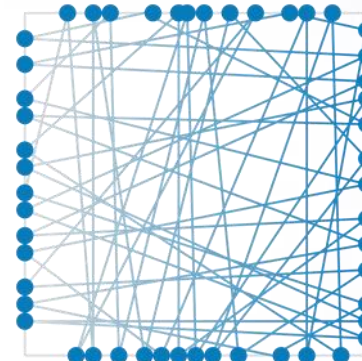
6-10 (29%)



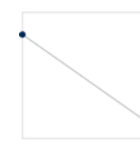
11-20 (18%)



21-50 (7%)



Over 50 (3%)



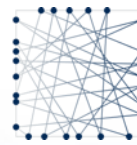
1-5 (35%)



6-10 (29%)



11-20 (21%)



21-50 (11%)



Over 50 (6%)

Vendor

55%

of organizations use 6 to
>50 security vendors

2016 (n=2,850)

Products

65%

of organizations use 6 to
>50 security products

2016 (n=2,860)

Over 4 Out of 10 Security Alerts are Never Investigated: Why?

The Uninvestigated Alerts Create Huge Business Risk

7%
experienced NO
security alert

44%
of alerts are
NOT investigated

56%
of alerts are
investigated

46%
of legitimate alerts are
remediated

54%
of legitimate alerts
are NOT remediated



28%
of
investigated
alerts are
legitimate

93%
experienced
security alert

For Every 5000 Alerts, 616 Legitimate Were Never Investigated or Remediated

Cisco
Connect



Security Breaches Paralyze Systems and Impact Key Business Operations

Business Impact

36%

Operations

30%

Finance

26%

Brand
Reputation

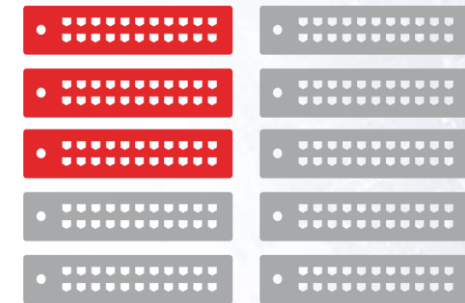
26%

Customer
Retention

Operational Impact



1-8 Hours
time that systems
were down for 65%
of organizations



Nearly 30%
of systems were
impacted for 61%
of organizations



Losses After an Attack are Real for Organizations



Opportunity

23%

42% were
losses >20%



Revenue

29%

38% were
losses >20%



Customers

22%

39% were
losses >20%

Breaches Driving Improvement



38%

said a breach drove **improvements** in security threat defense policies, procedures or technologies to a **great extent**.

(2016: n=1388)

Improvements Made to Protect Your Company from Security Breaches *(Top 5 mentions)*

38%

Separated the security team from the IT department

38%

Increased security awareness training among employees

37%

Increased focus on risk analysis and risk mitigation

37%

Increased investment in security defense technologies or solutions

37%

Increased investment in the training of security staff

(2016: n=1375)

Drivers Minimizing Risk



Make Security a Business Priority

Leadership must own, evangelize, fund security.



Measure Operational Discipline

Review security practices, control access points, patch.



Test Security Effectiveness

Validate, improve security practices, network connection activity.



Integrate Defense Approach

Implement architectural approach to security, automate processes to reduce time to react to, stop attacks.



Attack Preparedness Plan

Drivers Minimizing Risk



Executive Leadership

Executive leadership must own and publicly evangelize security as a high priority.



Policy

Regularly review security practices, and control access points to networks systems, applications, functions, and data.



Protocols

Regularly, formally and strategically review and improve both security practices and connection activity on the network.



Tools

Put tools in place to enable users to review and provide feedback on security, and empower them to increase security controls on high-value assets.



Detect

To alert your organization to security weaknesses before they become full-blown incidents, implement a system for categorizing incident-related information.



Prevent

To minimize impact of breaches, encourage employees to report failures and problems, and clearly communicate security processes and procedures.



Mitigate

Implement and document exact procedures for incident response and tracking. Inform and educate all parties on precise, step-by-step crisis management response protocol.



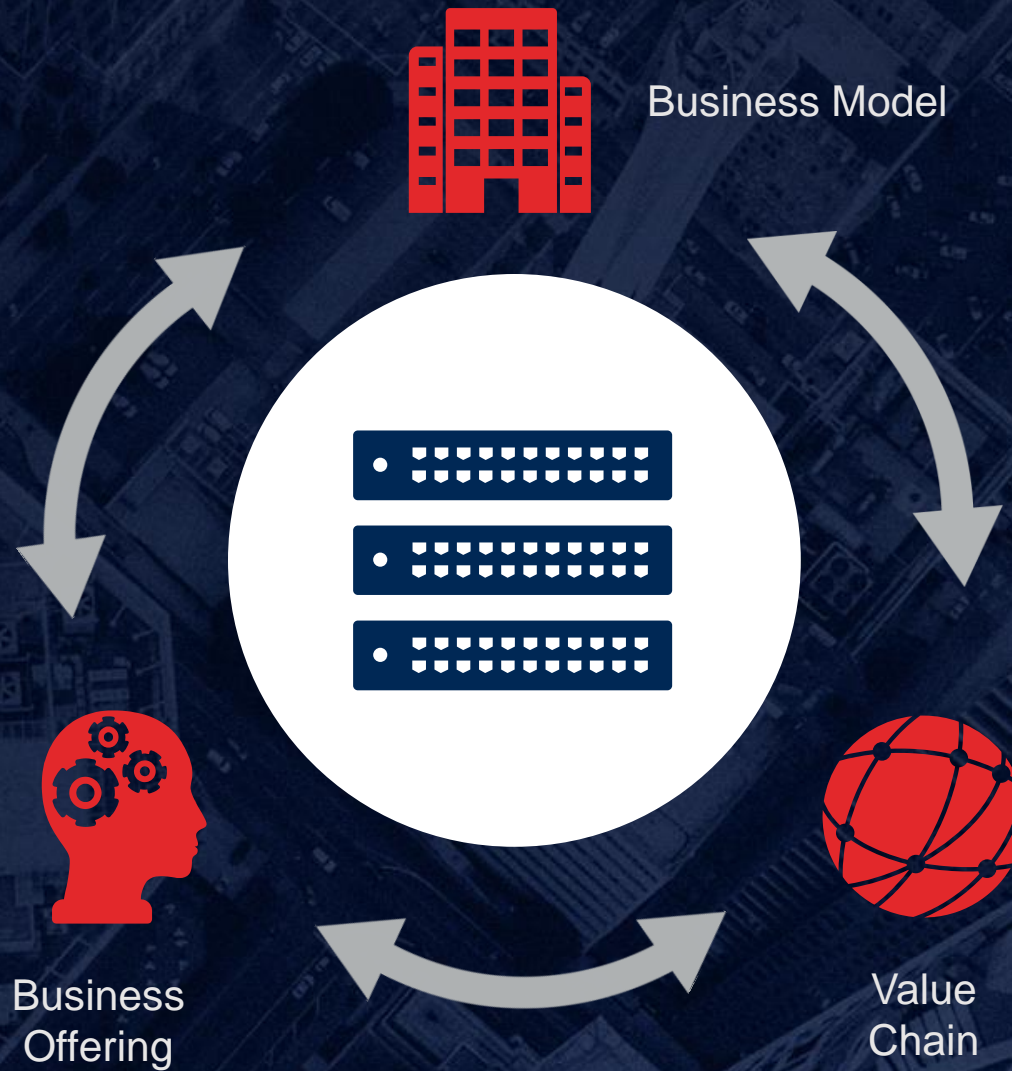
**Minimized
Risk**

CISCO

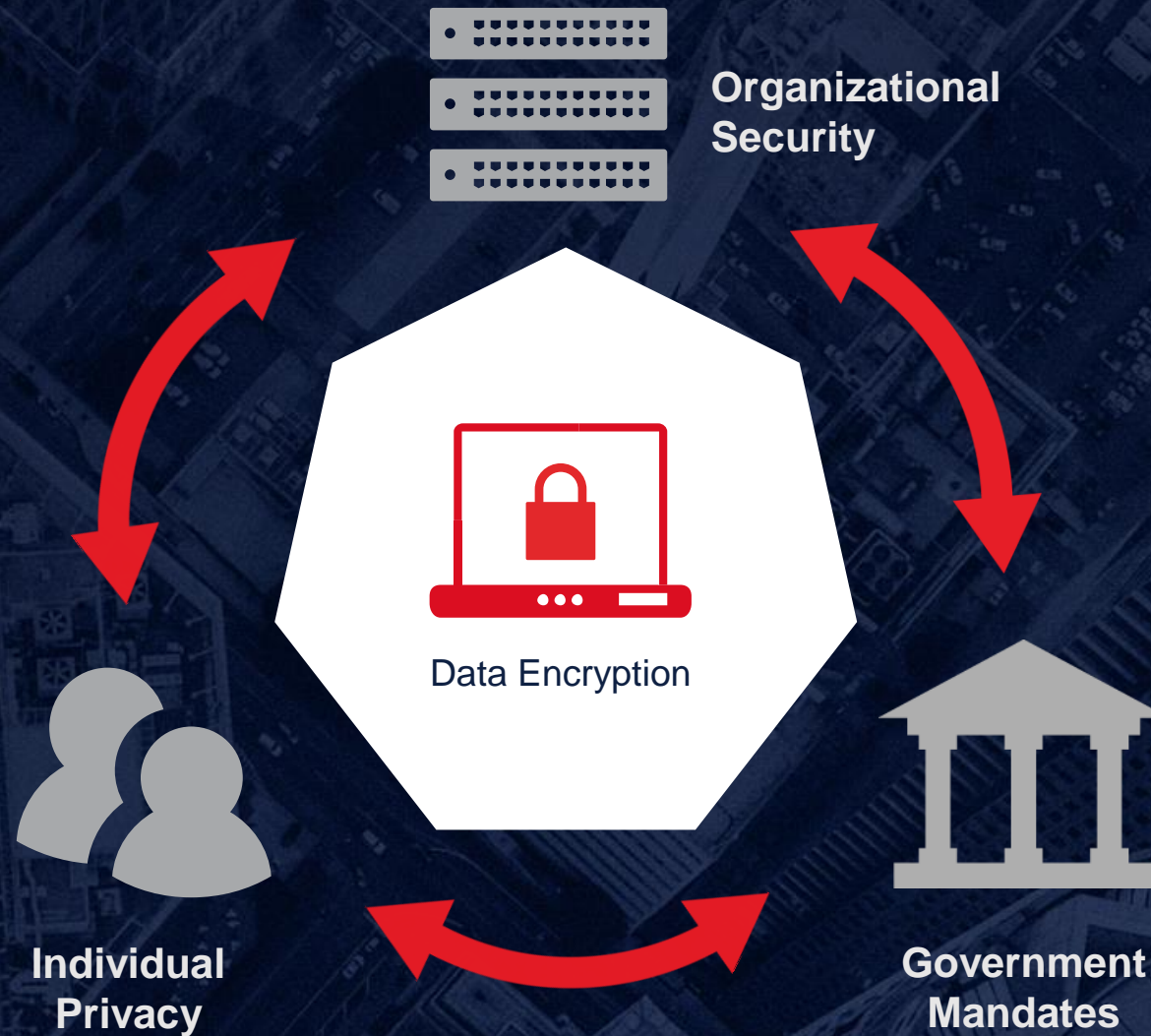
Industry Perspective



Mitigating Third-Party Risk

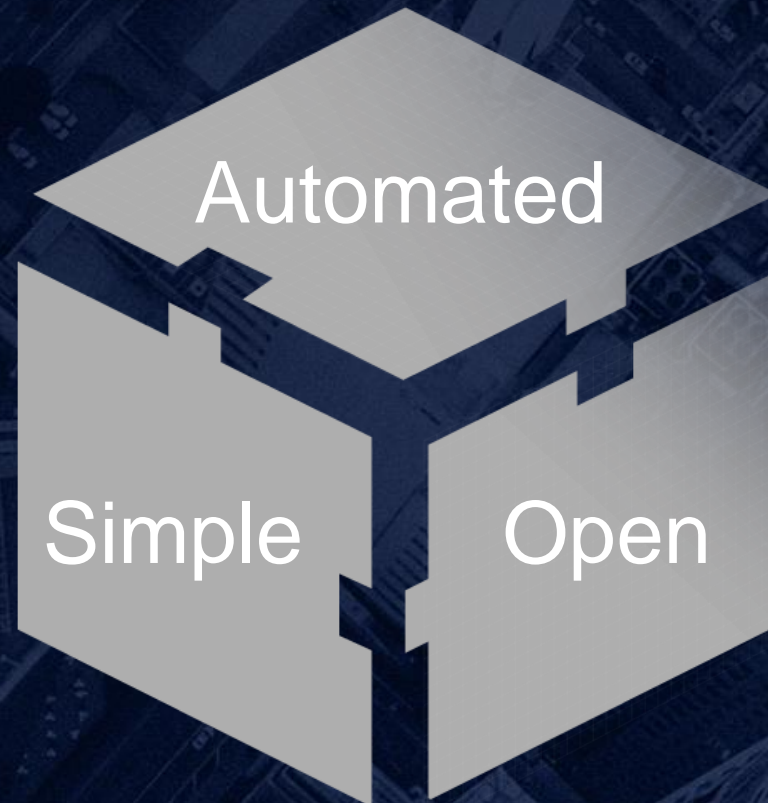


Encryption and Security



Keys to Success

Integration of technology reduces opex for success, reduces the burden on existing people, and delivers better outcomes.



Summary

Cisco
Connect •



Annual Cisco Cybersecurity Report

Cisco
Connect ●

Download the Cisco 2017
Annual Cybersecurity Report

www.cisco.com/go/acr2017

