Intelligent Cybersecurity for the Real World

Luis Fernando Garzon- lugarzon@cisco.com
Product Sales Specialist - Security
Current Threat Landscape

• Evolution of Ransomware
• Advances in Malicious Tradecraft
• Questionable Network Hygiene
• Conflicting Geopolitical Perspective
Encryption technique allows per-target customization

Marking systems and files have already been encrypted

Using Bitcoin for anonymous payment

Dual deadlines for:
1. Cost increase
2. Deleting data
Malware Use of HTTPS:
HTTPS increased 300% for ad-injectors in the last 4 months.

Increased
300% in 4 months

Ad injection is the biggest contributor. Adversaries are using HTTPS traffic to expand time to operate.
Infrastructure: Building Out of Digital Economy on Fragile Infrastructure

Fragile, insecure infrastructure will not be able to securely support the next-generation economy.

Devices running known vulnerabilities for an average of 5 years

And the problem is systemic

Cisco
5.64 years

Apache/Open SSH
5.05 years
Vertical Risk of Malware Encounters

No industry is safe. Attackers shift around industries.
Web Blocks by Country

Adversaries don’t respect borders and shift their base of operations.
Aging Infrastructure Is a Worldwide Problem
Conclusion

- Ransomware Widespread and Potent
- Regular Data Backup
- Improve Network Hygiene
- Integrate Defenses
- Measure Time to Detection
Security Should Be a Business Enabler
Collapse of the Old Security Model

Symptoms of Failure

- 100% of Organizations Compromised
- Average Time from Breach to Detection is 200 days
- 500,000+ Firewall Rules
- 80+ Security Tools
- Terabytes of Logs yet Little Visibility
- Security Complacency
Silos Create Security Gaps

- Traditional Firewall Functions
- VPN Functions
- Context-Aware Functions
- IPS Functions
- Malware Functions

Context-Aware Functions
IPS Functions
VPN Functions
Architecture Defeats Complexity

Key Elements of an Architecture

1. Capabilities/Solutions … That work well together … Effectively
Enabling the Process of Security
Cisco Security Architecture Imperatives

Doing Security Differently

**Intelligence Driven**
- Network-Integrated, Broad Sensor Base, Context and Automation

**Security Everywhere**
- Continuous Advanced Threat Protection, Cloud-Based Security Intelligence

**Integrated Defense**
- Agile and Open Platforms, Built for Scale, Consistent Control, Management

OUTCOME ACCELERATION

Network, Endpoint, Mobile, Virtual, Cloud, IoT/OT
Security Everywhere
Leveraging the Network as the Defender

WHO
WHAT
WHERE
WHEN
HOW

Visibility, Context, and Control

ENFORCE
Apply policy at connection to reduce the attack surface

DETECT
Leverage Context and NetFlow to get visibility you don’t have and anywhere you want it

MITIGATE
Take action against offensive or unauthorized threats/behaviors

Hardware-enabled NetFlow Switch

Device

Internal Network

Context

Cisco ISE
Cisco FTD+NSEL
Cisco ISR G2 + NBAR

Firesight And/or Lancope Stealthwatch
OpenDNS Acquisition
Leveraging a Single Global Recursive DNS Service

**BENEFITS**

- Global Internet Activity Visibility
- Network Security w/o Adding Latency
- Consistent Policy Enforcement
- Internet-Wide Cloud App Visibility

![Diagram showing network architecture with OpenDNS integration](Image)
Cisco Security is Pulling Away

**IDC**
Cisco’s Security Everywhere …“that’s pretty brilliant”

**CRN**
“Vendors Like Palo Alto, FireEye Are Selling Legacy Technology”

**Gartner**
“Network security architects … need to adopt new products and/or services that will enable the network to be an integral part of a strategy that focuses on detecting and responding to security incidents.”

**CIO Survey’s 1st in Customer Preference**
PiperJaffray  UBS  BARCLAYS

**Citi**
“Cisco’s strength in its Security business shows it is not an ‘old’ tech company”

“Cisco is making all the right moves… software-focused, cloud-friendly portfolio with double-digit growth in Security and acquisitions like OpenDNS”
Security Company of the Year