

# Security Resilience & Convergence

Are you (In)Secure

Chris Lapp  
Technical Solutions Architect – Media & Entertainment  
Cisco Distinguished Speaker

November 2023



# Who am I?

I help Cisco Customers in the Media Space align technology to their Objectives. 15+ years' experience in broadcast, AV, and live entertainment.



## Education

Studied at South Alberta Institute of Technology and graduated the BXST program



## Experience

Bell Media, Evertz Microsystems, and Diversified



## SMPTE

Currently hold the title of Membership Director for SMPTE for 4<sup>th</sup> term



## Standards and Working Groups

Participate in the active standards body for SMPTE, AIMS, VSF, IETF and others with emphasis on Video over IP standards,



# Agenda

- 1 Key Trends
- 2 Change in Security Landscape
- 3 Secure Concepts
- 4 Reference Architecture
- 5 Readiness Index
- 5 Top Threats / Lessons Learned



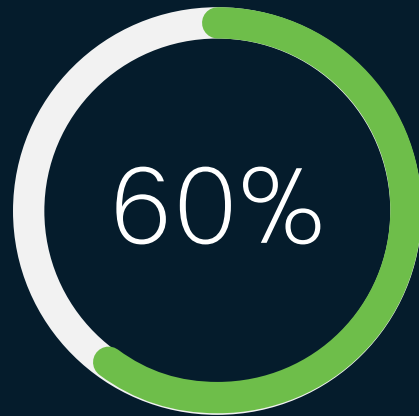
## Key IT Trends

- | Adoption of a Cloud Experience
- | Applications are now the Lifeline of Every Business
- | Shift to Hybrid Work
- | Security is Moving to the Cloud
- | Transition to 5G & Wi-Fi 6
- | Apps & Workloads are Moving Closer to Users & Devices

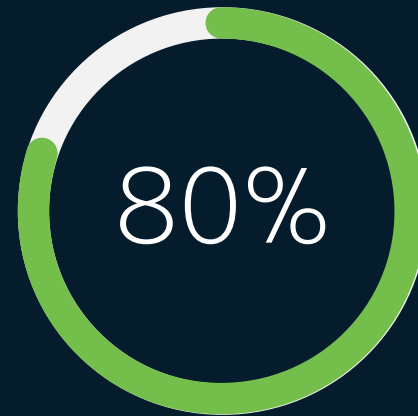
# Cybersecurity trends in 2023



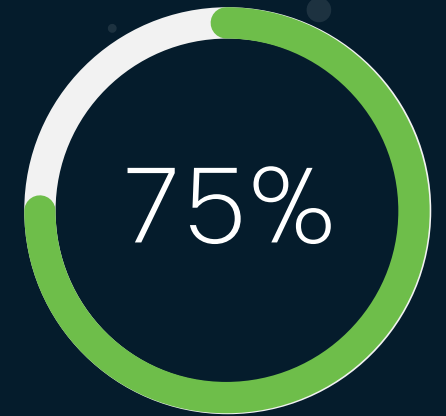
of C-level executives will have performance requirements related to risk built into their employment contracts



of organizations will use cybersecurity risk as a primary determinant when doing business



of enterprises will unify web, cloud services and private application access from a single vendor's SSE platform



of Organizations are pursuing Security Vendor Consolidation

# Cybersecurity **Trends**

**Privacy regulation**  
continues to expand

**Hybrid workforce** and data  
everywhere, accessible by everything

**Security Vendor  
Consolidation**

**Zero Trust** is both a  
security principle and an  
organizational vision

**Cybersecurity risk**  
determines whether organizations  
conduct business with third parties

Boards regard **cybersecurity  
as a business risk** rather  
than solely a technical IT problem

The decision to make a  
**ransomware  
payment** or not is a  
business-level decision, not  
a security one.

**Business continuity  
management** in response to  
large-scale disruption.

Threat actors will have weaponized  
**OT environments**  
successfully to cause human  
casualties.

# Gartner Security Trends 2022

## Top Trends in Cybersecurity, 2022

01



Attack surface  
expansion

02



Identity system  
defense

03



Digital supply  
chain risk

04



Vendor  
consolidation

05



Cybersecurity  
mesh

06



Distributed  
decisions

07



Beyond  
awareness

[gartner.com](https://www.gartner.com)

Source: Gartner  
© 2022 Gartner, Inc. All rights reserved. PR\_1764850

**Gartner**

Data in seconds



83%

of organizations were phished

435%

increase in ransomware

358%

increase in malware





The world has changed

and with it..

The demands of cybersecurity



“security is a public health matter”  
“to protect anyone, we must  
protect everyone”

– Edward Snowden

# Everything we do has been redefined



From **office**



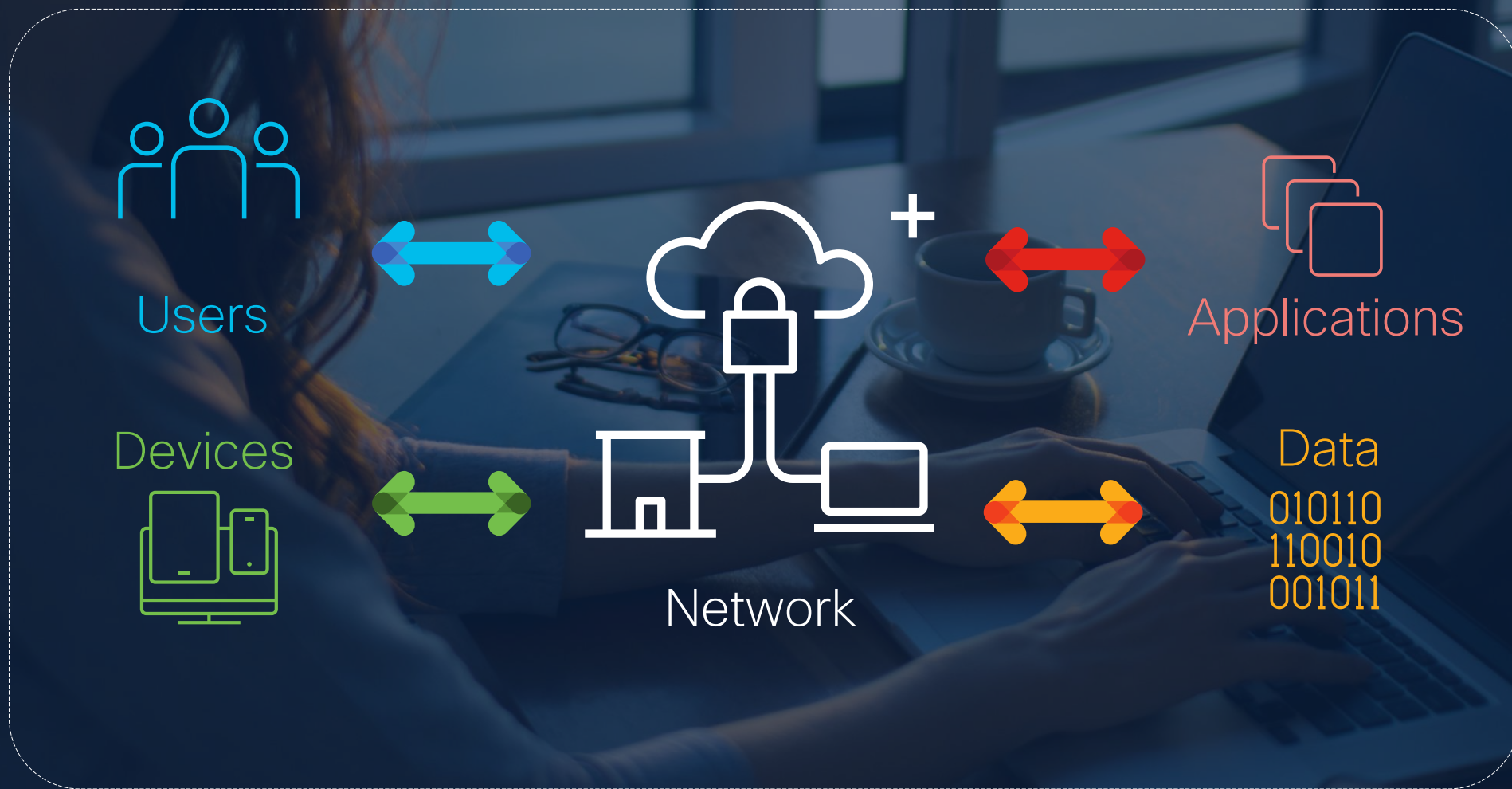
From **home**



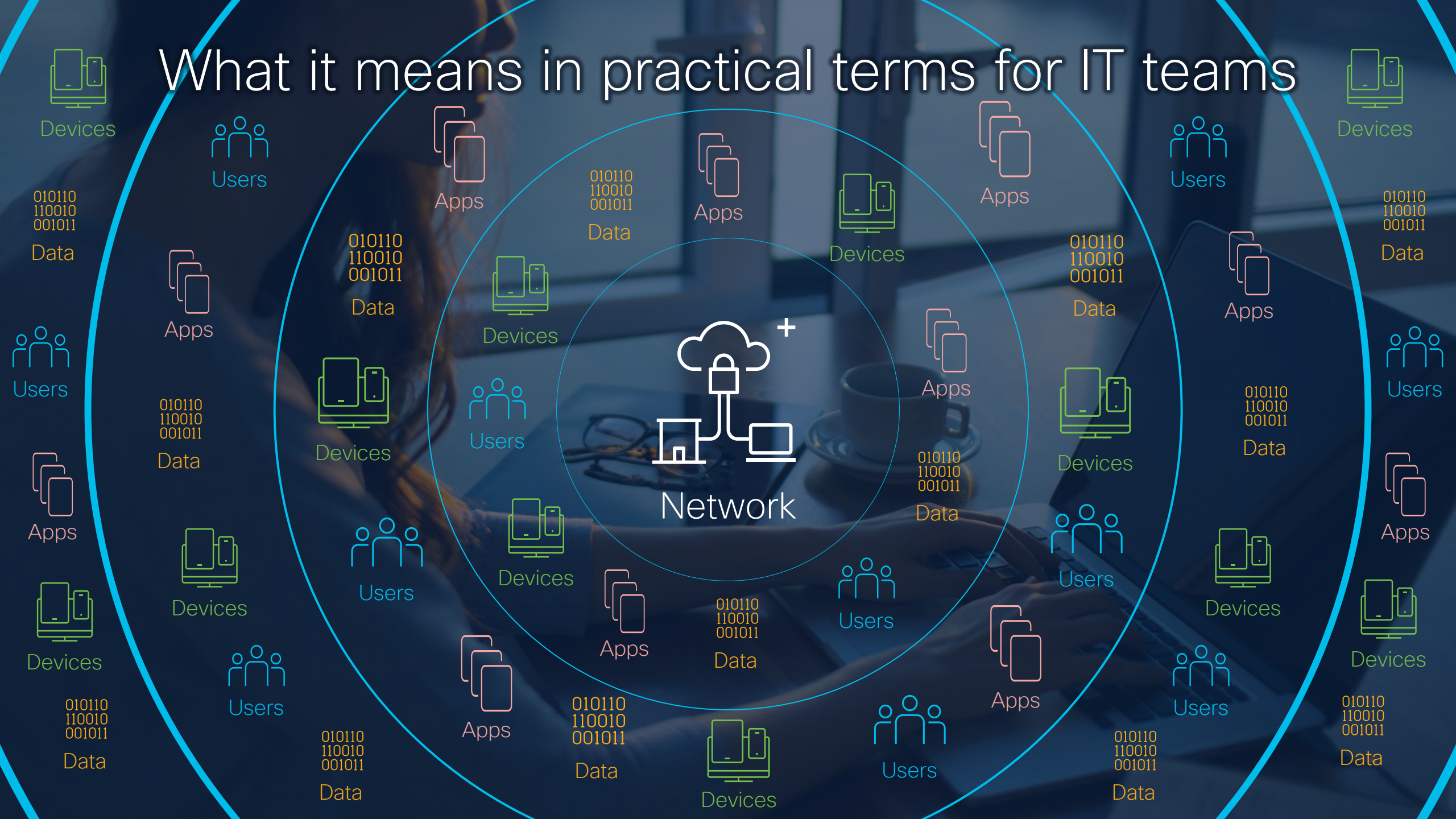
Anywhere in **between**



# What it means in practical terms for IT teams



# What it means in practical terms for IT teams



# The (In)security industry



Way Too Many Vendors  
(and the wrong vendors are the breakout stars)

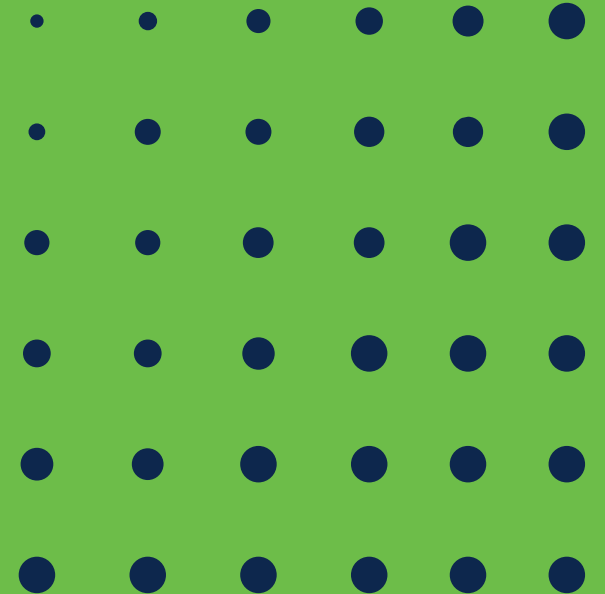


Way Too Many Tools  
(and most tools don't work together)



Way Too Little Cooperation  
(and too much focus on profits over security)

# Key Security Concepts



# 1. Nothing is 100% Secure

Breaches will happen

Until everything is secure, nothing is secure

Good guys need to be right 100% of the time – Bad guys only need to be right once

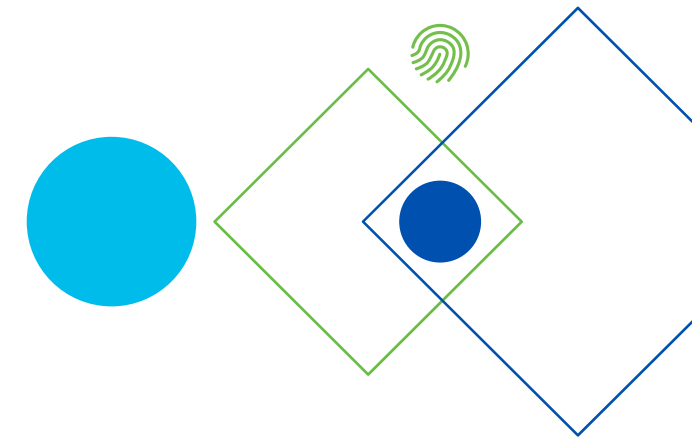
People are still the main reason breaches occur

Security solutions are only as effective as the weakest link



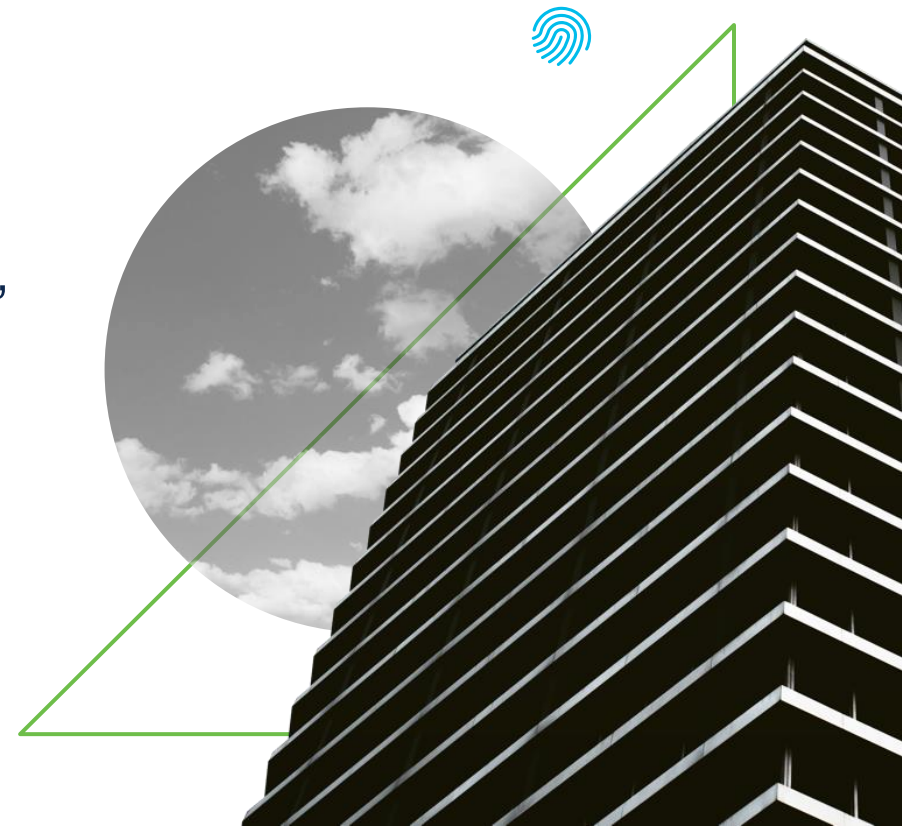
## 2. People Are (Still) The Biggest Threat

- Tremendous Security knowledge gap
- Most people are trustworthy, helpful, and eager to answer emails and phone calls (and bad guys use this against us)
- People will download almost any app and give that app almost any permissions
- Most people's [motivated perception](#) is flawed
- Bad guys use these traits (and more) against us



# 3. Too Many Businesses Are Underfunded Or Unprotected

- Security still seen as a complex cost center
- Hard to find, pay, retain talent
- Firewalls no longer good enough
- Patching and updates are tedious and sporadic
- Many companies lack basic training, basic policies, basic enforcement



# 4. Security Models, Frameworks and Laws Matter

- Models and Frameworks:
  - Work
  - Can help justify investment
  - Drive efficiency and efficacy
- Laws can help:
  - Ensure breach reporting
  - Mandate investment
  - Protect personal and business information
- Note:
  - Federal regulation is coming ([example](#))



# 5. Threat Intelligence and Automation Matter

- Security solutions are only as good as their last Threat Intelligence Update
- Effective solutions must be easy to use and maintain, be manageable by people of all talent levels, and adapt to new and changing threats
- Platforms are becoming more important than point products





 Threat Intelligence

 Extended Detection and Response

 ZERO TRUST

 SASE

 User / Device Security

 Cloud Edge Network

 On Premises Network

 Workload, Application, and Data

 Platform



TALOS THREAT INTELLIGENCE

Actionable threat intelligence

Collective responses

Comprehensive visibility

Signal identification

Threat research & analysis

XDR SECURITY OPERATIONS TOOLSET

Cisco Vulnerability Management | Secure Analytics XDR | Secure Client | Talos Incident Response

SERVICES

- Custom threat research on demand
- Implement and manage
- Incident response retainer
- Managed detection & response
- Strategy & assessment

CAPABILITIES

- Network detection & response
- Device discovery & insights
- Endpoint detection & response
- Open API platform & 3rd party native integrations
- Risk-based vulnerability management
- Security analytics
- Security orchestration, automation & response
- Threat visibility incident response & threat hunting

ZERO TRUST

SASE

User / Device Security

Cisco Secure Client (AnyConnect) | Umbrella | Secure Endpoint | Meraki Systems Manager | Duo | Secure E-mail | ThousandEyes

- Cloud managed
- VPN
- Telemetry Visibility
- Endpoint detection & response
- DNS-layer security
- Secure web
- Anti-virus Anti-malware
- Query
- Host FW
- Mobile device management
- Risk-based MFA
- Password-less
- Device trust
- Continuous Trust
- Email, Phishing, SPAM, BEC, DLP, content filtering
- Digital experience monitoring

Cloud Edge Network

SASE/Security Service Edge

Duo | Secure Access | Umbrella | Secure Connect

- Browser access control
- Cloud access security broker
- Cloud malware detection
- Data loss prevention
- DNS-layer security
- FWaaS
- Identity / posture
- RAaaS
- Remote browser isolation
- Secure web gateway
- TLS decryption
- Zero Trust Network Access
- Tenant restrictions

On-Premises Network

SASE/SDWAN

Meraki | Secure Firewall | ThousandEyes | Viptela

- Analytics
- Application performance optimization
- Cloud based orchestration
- Cloud OnRamp
- Digital experience monitoring
- Group tag propagation
- IPSecVPN
- Integrated security
- Middle mile optimization
- Segmentation
- Visibility

In the Office/Managed Location

Catalyst | DNAC | ISE | Meraki | Secure Firewall | Secure Network Analytics | Secure Web Appliance

- Application network gateway
- Configuration orchestration
- Content filtering
- Encrypted visibility
- Zero Trust Network Access
- Group tag classification
- Identity/pxGrid Cloud
- Network access control
- Network security analytics
- NGFW
- NGIPS
- Security analytics & logging
- Segmentation
- Threat mitigation
- Profiling

Industrial Threat Defense

DNAC | CyberVision | Industrial Networking | ISE | Secure Firewall | Secure Network Analytics

- Anomaly detection
- Compliance
- Group tag classification
- Identity pxGrid
- Ruggedized
- Segmentation
- Threat mitigation
- Visibility

Workload, Application, and Data Security

ACI | Attack Surface Management | Panoptica | Radware | Secure Application | Secure Endpoint | Secure Firewall | Multicloud Defense | Secure Workload

- Anti-virus Anti-malware
- API security
- App discovery
- Cloud analytics
- Cloud Native Security
- CSPM/CAASM
- DDoS, WAF/Bot
- Identity pxGrid
- Micro/Macro Segmentation
- Run-time application
- Telemetry
- Threat mitigation
- Visibility
- Firewall
- Data access & Integrity
- Defense Gateway

# What are we fighting?

# Internet of Things



Almost anything with a circuit is now Internet connected



Bad guys can use unprotected IoT devices against businesses



Many IoT companies put features and profit ahead of protection:



Many IoT devices have poorly written (hackable) software



Unpatched systems and IoT insecurity can lead to Supply Chain hacks (Covered later)



# Threat As A Service

- Many hacking groups now offer Threat as a Service
- Threats are no longer only single-purpose, but blended
- Some groups are state sponsored, some are private

# The War is Tough

What Attackers are doing today	What your defenders will do today
1. Breach your network	1. Four hours of meetings
2. Monetize	2. Status Updates
	3. Add notes to tickets
	4. Timesheets
	5. HR mandated training
	6. close tickets as "False Positive"
	7. update slide decks
	8. update policies + KBs
	9. 23 minutes of Infosec work

Who will win?

# Media & Entertainment

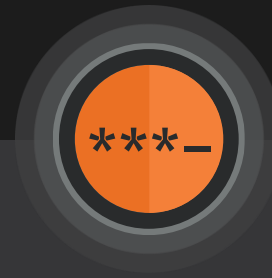
Key threats Talos is tracking

## Blackbyte Ransomware



Criminal ransomware-as-a-service combining data exfiltration with encryption.

## Credential Stuffing



Criminal attackers attempting to guess credentials many times each second.

## Hacktivist Activity



Politically motivated hackers seeking to cause highly visible disruption.

# Cybersecurity Readiness Index

# Security Readiness in a hybrid world

Identity  
Verification

Devices

Network

Application  
Workloads

Data



To achieve this, they need solutions that offer



Visibility and Analytics

Automation and Orchestration

Governance

# Measuring Security Readiness



But how does one measure it?

# Measuring Security Readiness

## Identity Verification

Traditional Data stores like AD

Integrated IAM solution

Privileged Access Management

## Devices

Built-in protections in the OS such as AV and host controls

Anti-virus with some enhanced features

End-point protection platform (Firewall, malware, USB controls, process viability)

## Network

Network segmentation policies based on identity

Firewalls with built-in IPS

Network behavior Anomaly detections tools

Packet capture and sensor tools

## Application Workloads

Host software firewall

Endpoint protection capabilities

DLP

Application centric protection tools

Visibility and forensic tools

## Data

Encryption tools

Identification and Classification with DLP

Backup and Recovery

Host IPS & Protection tools

# Measuring Security Readiness

Identity Verification		Devices		Network		Application Workloads		Data	
Traditional Data stores like AD	30%	Built-in protections in the OS such as AV and host controls	10%	Network segmentation policies based on identity	40%	Host software firewall	15%	Encryption tools	10%
Integrated IAM solution	60%	Anti-virus with some enhanced features	20%	Firewalls with built-in IPS	25%	Endpoint protection capabilities	35%	Identification and Classification with DLP	20%
Privileged Access Management	10%	End-point protection platform (Firewall, malware, USB controls, process viability)	70%	Network behavior Anomaly detections tools	25%	DLP	10%	Backup and Recovery	50%
				Packet capture and sensor tools	10%	Application centric protection tools	20%	Host IPS & Protection tools	20%
						Visibility and forensic tools	20%		



# Measuring Security Readiness

## Identity Verification

Traditional Data stores like AD

Integrated IAM solution

Privileged Access Management

Do you have this in your posture?

If yes, what is the scale of deployment:

- Fully Deployed
- Partially deployed
- Just started the deployment
- Budgets approved, deployment yet to start

If no, do you intend to deploy?

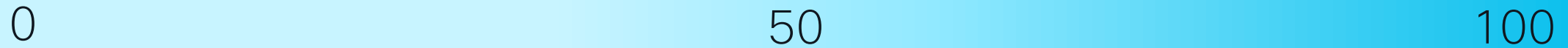
If yes, do you have the budget approved?

If yes, what is the intended timeline of deploying?

# Measuring Security Readiness

Three levels of scores / weightages:

1. Scale of deployment of each technology under respective pillar

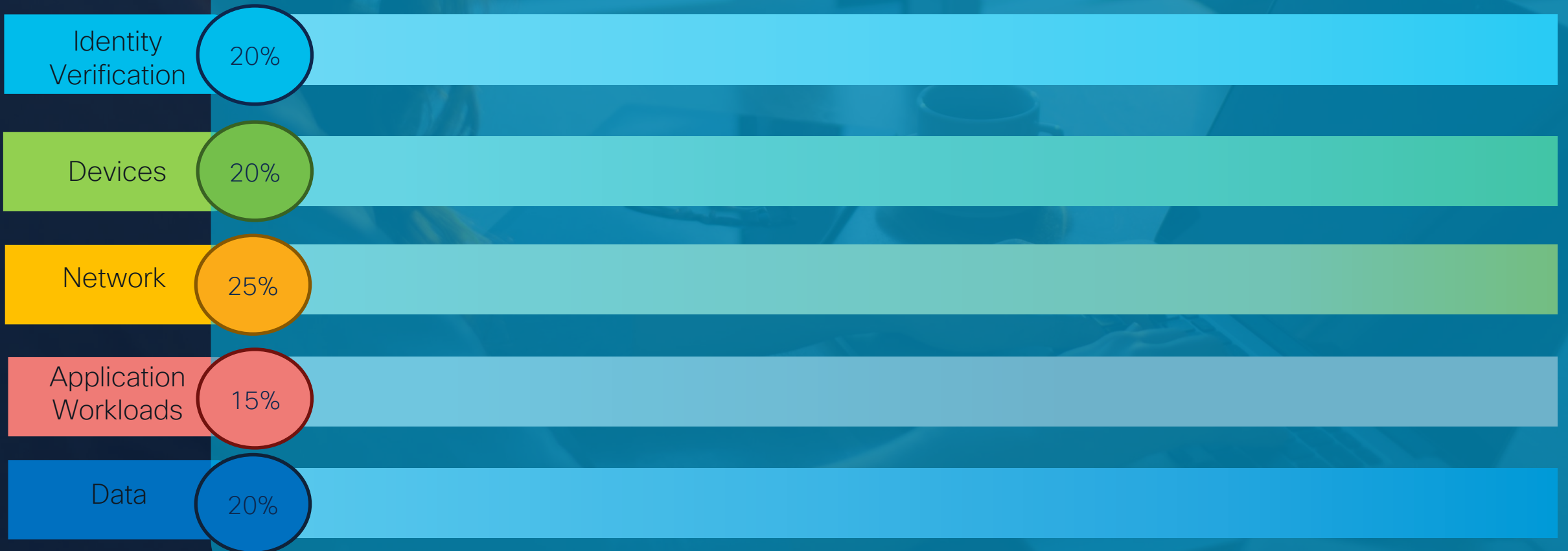


0 50 100

2. Individual weightage of each technology

# Measuring Security Readiness

## 3. Weightage of respective pillars



# Measuring Security Readiness

Overall Score



Beginner

Formative

Progressive

Mature

Stage of Security Readiness

How do  
companies stack  
up globally?



# Measuring Security Readiness

Overall



■ Beginner ■ Formative ■ Progressive ■ Mature

# Measuring Security Readiness

## Identity Verification



■ Beginner ■ Formative ■ Progressive ■ Mature

# Measuring Security Readiness

Devices



■ Beginner ■ Formative ■ Progressive ■ Mature



# Measuring Security Readiness

Network



■ Beginner ■ Formative ■ Progressive ■ Mature

# Measuring Security Readiness

Application Workloads



■ Beginner ■ Formative ■ Progressive ■ Mature

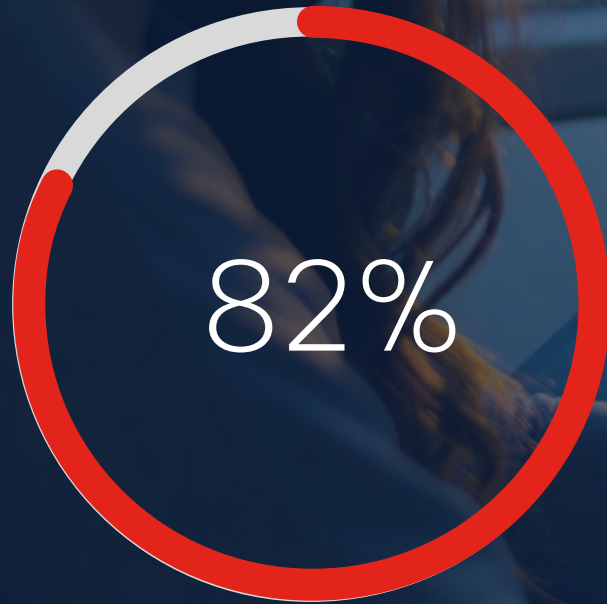
# Measuring Security Readiness

Data



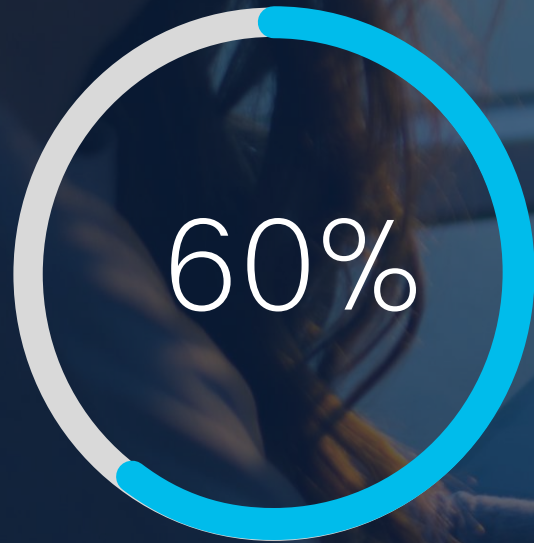
■ Beginner ■ Formative ■ Progressive ■ Mature

# Security Readiness: The gap is alarming



Companies that expect a cybersecurity incident to disrupt their business in the next 12 to 24 months

# Security Readiness: Being unprepared comes at a price



Companies have had a cyber incident in the past 12 months

Of affected companies said it cost them US\$500,000 or more

# What's Next

- More Supply Chain Hacks
- More Application, Internet of Things, Device Threats
- More Insider Threat
- Artificial Intelligence-Aided Threats
- Nation State Cyberwarfare
  - Which can affect private business



Our IT Industry is inexorably international, and anyone involved in the process can subvert the security of the end product. We cannot trust anyone, yet we have no choice but to trust everyone. No one is ready for the costs that solving this would entail

---

Bruce Schneier

American cryptographer, computer security professional, privacy specialist

# Top Threats, Lessons Learned...



The Cisco Talos logo, featuring the Cisco logo (a stylized bridge) and the word "TALOS" in a blue, sans-serif font, positioned at the top of a central dark grey circle.

CISCO | TALOS

The central message "OUR JOB IS YOUR DEFENSE" is written in a large, grey, italicized, sans-serif font, centered within a dark grey circle that has a subtle shadow and is set against a background of blue circuit lines and orange dots.

*OUR JOB  
IS YOUR  
DEFENSE*

# Top Threats – Incident Response

- January – March 2023

Since January 2023, Talos IR has observed a **novel increase in web shell usage** compared to previous quarters, making up nearly a fourth of the threats responded to in Q1 2023.

Ransomware made up less than 10 percent of engagements vs. previous quarter's ransomware engagements (20 percent).

Ransomware and pre-ransomware incidents combined, however, made up nearly 22 percent of threats observed...

...collectively observed as often as web shells were this quarter.

Qakbot commodity loader was observed across engagements this quarter leveraging ZIP files with malicious OneNote documents

Adversaries are increasingly relying on OneNote to spread their malware after Microsoft disabled macros by default in Office documents in July 2022.

Exploitation of public-facing applications was the top initial access vector this quarter, contributing to 45 percent of engagements, a significant increase compared to 15 percent in the previous quarter.

# Lessons Learned – Incident Response

• January – March 2023

# 30%

Thirty percent of engagements either did not have multi-factor authentication (MFA) enabled or only had it enabled on a select handful of accounts and critical services.

# NO MFA!

Recent law enforcement efforts to disrupt major ransomware gangs, including **Hive ransomware**, have been successful in the past few months, though Talos IR suspects this creates space for other, new families to emerge or new partnerships to be formed.



This quarter also featured Daixin ransomware, a newer ransomware-as-a-service (RaaS) family that was previously unseen in prior Talos IR engagements.

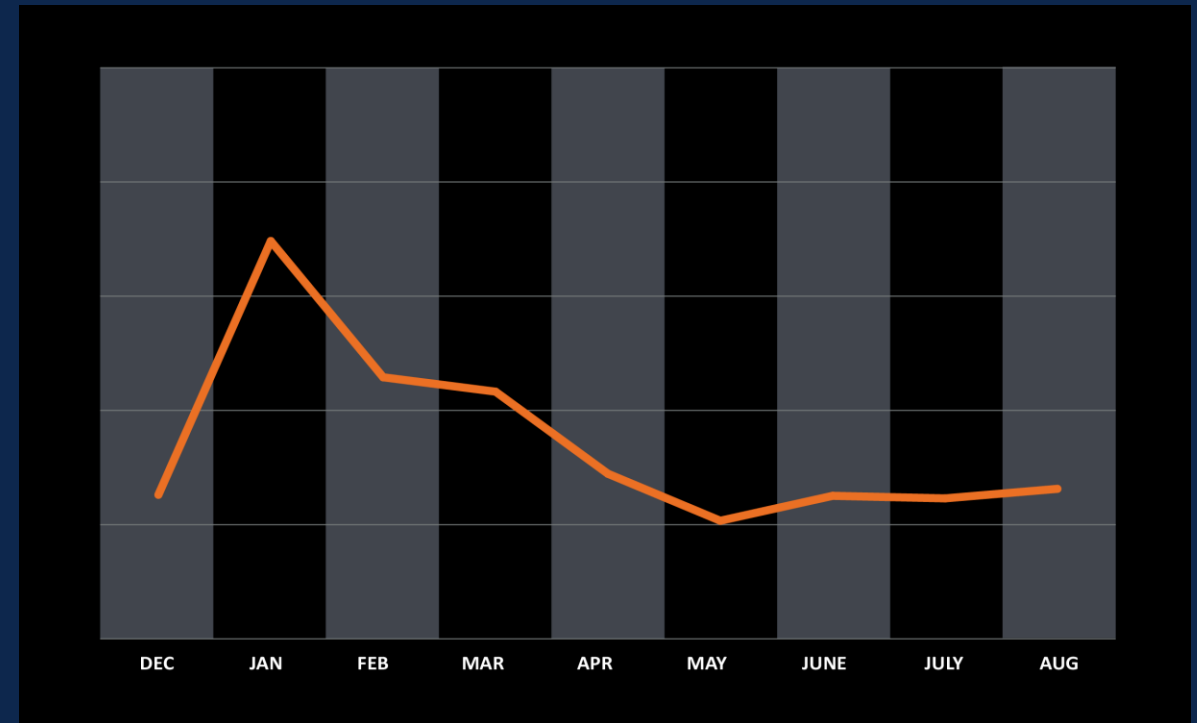
**Ransomware-as-a-Service**

# Log4j

Threat actors continue to exploit known vulnerabilities

- Alerts tied to log4j still remain in the 10s of millions
- Ransomware actors and cybercriminals quick to exploit
- Observed state-sponsored activity from China and North Korea

Total alerts on malicious network traffic identified as Log4j exploitation attempts.



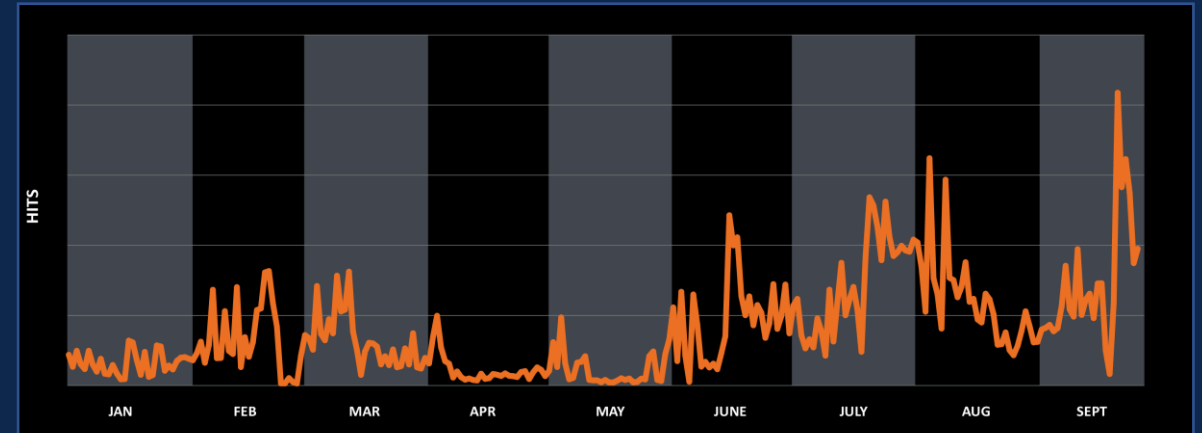
Source: Cisco Talos 2022 Year in Review  
<https://blog.talosintelligence.com/talos-year-in-review-2022/>

# USB Attacks

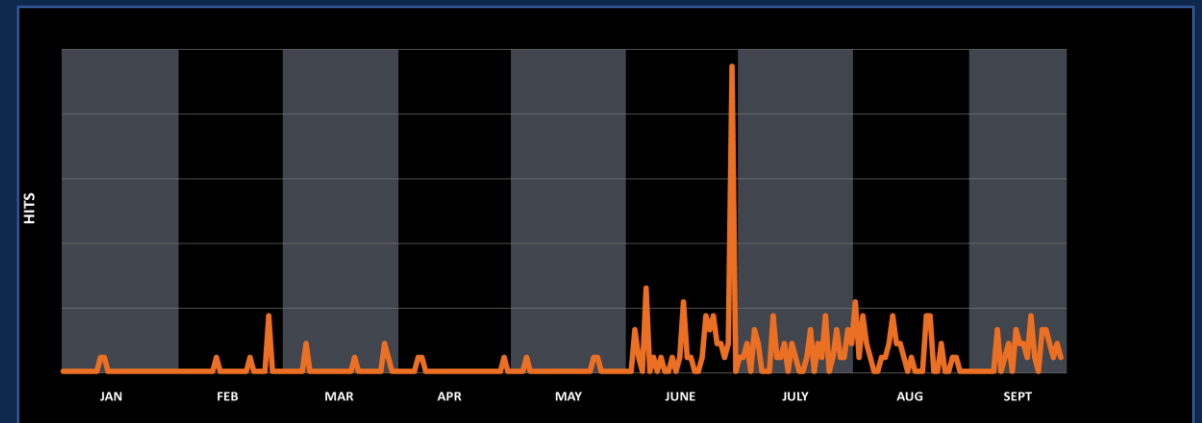
Observed increase in various USB-related alerts

- Talos Incident Response has a growing number of engagements in which removable USB drives infected organizations with malware.
- State-sponsored groups have updated their toolkits to include USB-related tools and techniques

Behavioral indicators for executables written to USB.



Behavioral indicators for setting hidden attributes for files on a USB.



Source: Cisco Talos 2022 Year in Review  
<https://blog.talosintelligence.com/talos-year-in-review-2022/>



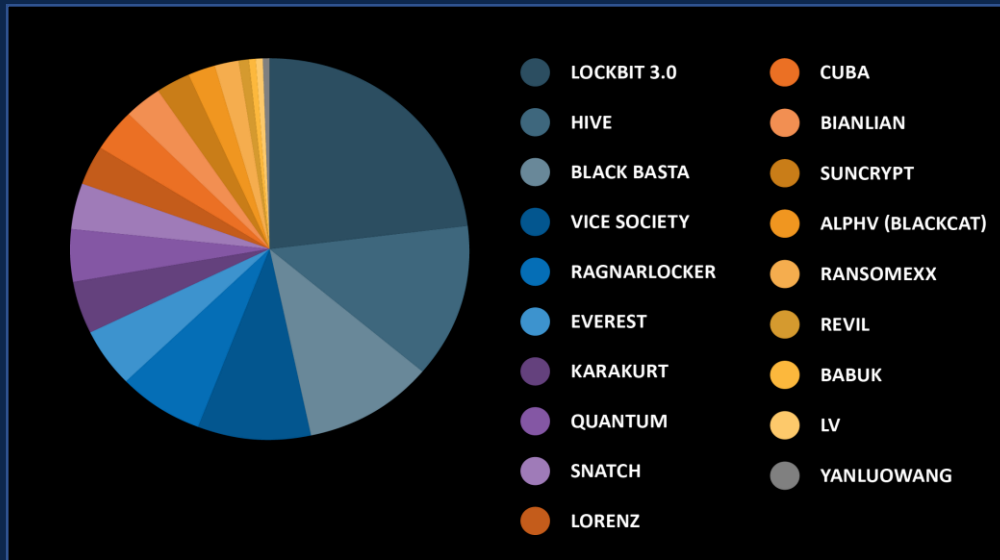
# Ransomware Evolution

# Ransomware – Evolving Behaviors and Trends

Initial Access	Business Model	Ecosystem	Targets
<p><b>Top 3</b></p> <ul style="list-style-type: none"><li>• Phishing Emails</li><li>• RDP exploitation</li><li>• Vulnerability exploitation</li></ul>	<ul style="list-style-type: none"><li>• Ransomware-as-a-service (RaaS)</li><li>• Payment Services</li><li>• Customer Support</li><li>• 24x7 Help Center</li></ul>	<ul style="list-style-type: none"><li>• Victim Sharing</li><li>• Victim access for sale</li><li>• Affiliates no longer structured in silos and work across multiple groups and campaigns</li></ul>	<ul style="list-style-type: none"><li>• Greater democratization of ransomware groups</li><li>• Shift from Big Game focus</li><li>• Organizations of all sizes proving lucrative</li></ul>
<b>Increased Impact</b>	Targeting Cloud, MSPs, Industrial Processes, Software Supply Chain .... and they work weekends and holidays!		

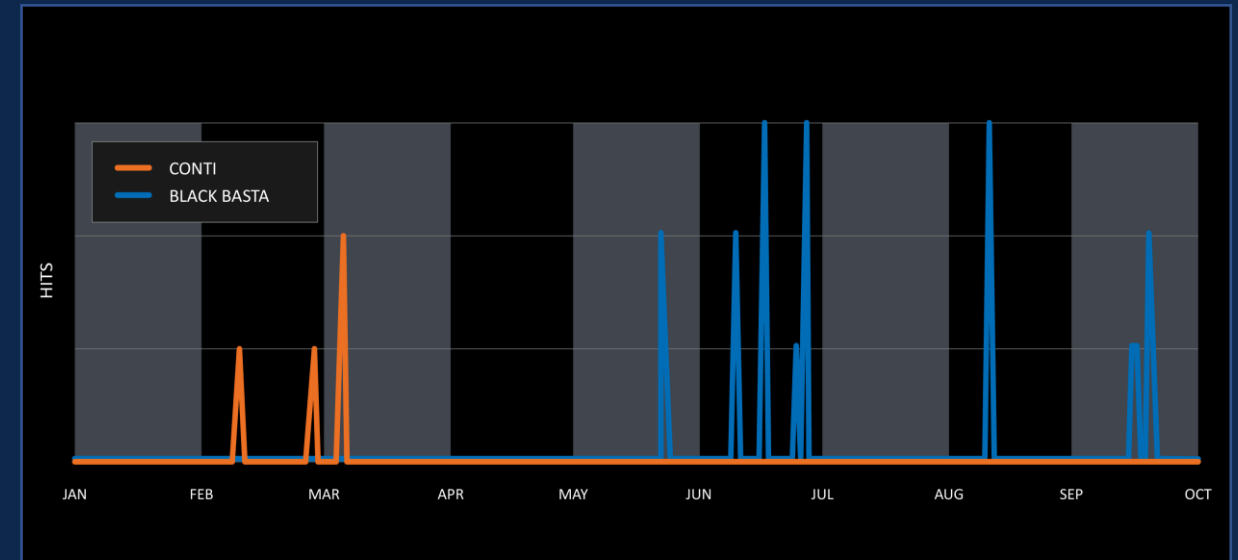
# Activity across ransomware groups

- Number of posts made to ransomware data leak sites tracked by Talos, January-October, 2022



Talos is tracking over 20 active ransomware cartels on the dark web

- Behavioral indicator detections for Conti Ransomware and Black Basta registry modifications



Even after takedowns, many cartels rebrand and reappear with similar tactics and techniques

Source: Cisco Talos 2022 Year in Review  
<https://blog.talosintelligence.com/talos-year-in-review-2022/>



# Defensive Takeaways

# Top 3 Defense Strategies to walk away with

Mastering the basics is still the most effective way to reduce risk

## **MFA!**

Credential stealing and reuse is **STILL** the most widely seen attack type.

- Protect your Credentials with MFA
- Be consistent with implementation
- Use Unique Logins / avoid defaults
- Use a secure browser (like Brave) and a password manager

## **Patching!**

2022 reporting estimates that more than 80% of network devices and 60% of applications remain unpatched.

- Ransomware Cartels are increasingly targeting unpatched systems and groups of systems
- Unpatched systems are **EASY** targets\*

\*A report by Redscan Labs showed that 90% of all common vulnerabilities and exposures (CVEs)

## **Education!**

Email and SMS are still the top vectors for attack

- Phishing education should be highest priority
- Generative AI can make malicious emails almost indistinguishable
- Mitigating the human-factor + solid security investments in Email, DNS and Endpoint protection are critical



chlapp@cisco.com



chrisjlapp