LOGICALIS
Architects of Change

Infographic

Zero Trust Simplified

We're living in a new age where trust-but-verify security methods no longer work. Sophisticated cybercrime and broader attack surfaces have left CIOs wondering: **How do I know who to trust?**

The proliferation of remote workers and interconnected devices means that traditional network perimeter defense methods aren't enough. **Today's threats require a modern "zero trust" model.**

What is Zero Trust?

It's a new way of thinking about security that trusts no one and verifies everything. Zero Trust promotes productivity and remote access – within limits – using network segmentation to protect sensitive data from inside the network. And it's a model that offers CIOs better access-based control with insight into the users and devices requesting connection to the network.

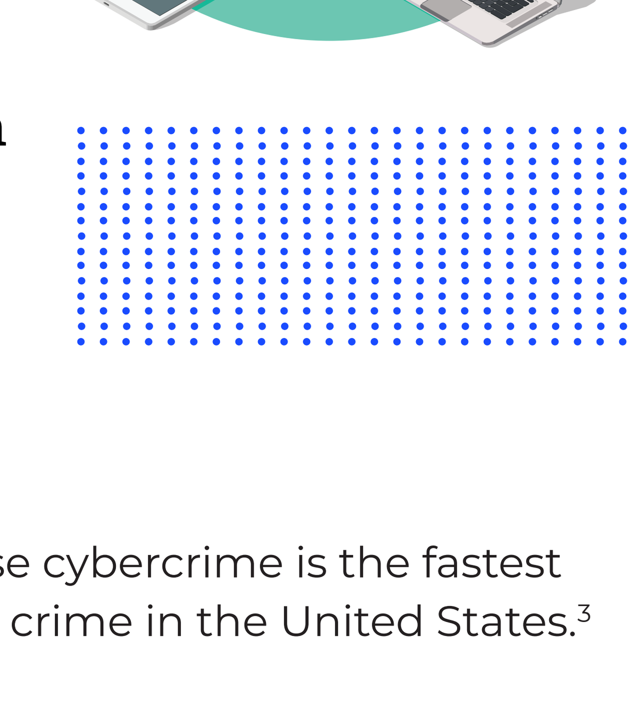
"Zero trust is an approach that moves you beyond 'trust everyone and deny specific cases' to a more effective 'trust no one and allow specific cases' security model."

- Ron Temske, Vice President, Security and Network Solutions, Logicalis

What's Different with Zero Trust?

Traditional Approach:
Trust is established when first connecting to a network, then maintained throughout that connection.

Zero Trust Approach:
Trust is established for every access request regardless of location inside or outside the network, and every user, device and access attempt is continuously validated.[1]



"Don't think of zero trust as getting rid of the perimeter, but rather as tightening security on the inside so that the network perimeter isn't the only thing keeping the attacker at bay."

- Cisco[2]

Why We Need Zero Trust

Because cybercrime is the fastest growing crime in the United States.[3]

$6 Trillion
Predicted annual cybercrime damages by 2021[5]

11 Seconds
Time between businesses falling victim to a ransomware attack by 2021[4]

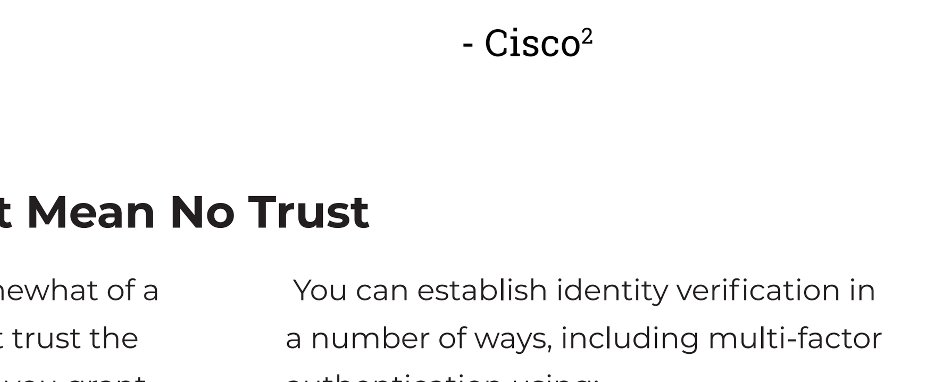
$20 Billion
Global ransomware damage costs by 2021[5]

Implementing Zero Trust

Protection and detection start with dividing security efforts into three important pillars: **Workforce, Workloads and Workplace**.[2]

1. The Workforce: Where Are the Breaches Coming From

90%
Successful breaches that stem from phishing emails[6/7]



74%
Percentage of breaches that involved access to a privileged account[8]

80%
Data breaches with a connection to compromised privileged credentials[9]

"Let's face it…a sufficiently successful outsider looks exactly like an insider."

- Cisco[2]

Zero Trust Doesn't Mean No Trust

The idea of "zero" trust is somewhat of a misnomer because you must trust the identities of parties to whom you grant access to your network. That's where trust-but-verify still comes into play within the zero-trust model.

You can establish identity verification in a number of ways, including multi-factor authentication using:

- Tokens such as USB keys or pin codes sent to trusted devices
- App-generated one-time codes that must be used within a certain period of time[10]

2. Workloads and The Rise of Cloud Computing

94%
Workloads and compute instances that will be processed in cloud data centers by 2021[11]

92%
Percentage of malware delivered through email[12]

Biggest Application Security Challenges IT Teams Face

62%
Securing access to private apps distributed across data center and cloud environments[13]

50%
Minimizing exposure of private apps to the internet[13]

50%
Gaining visibility into user activity[13]

"If you can't see it, you can't protect it."

- CISO Survey Respondent[14]

3. The Workplace: A Larger Attack Surface

Endpoints and servers are obvious attack vectors, but today's attack surface has grown well beyond the traditional boundaries. For example, what about "smart" devices and the Internet of Things (IoT)?

"For many organizations, their cyber-attack surface area is increasing as connected Internet of Things (IoT) endpoints proliferate. These include both legacy and the new breed of smart printers and multifunction printers (MFPs)."

- Quocirca[15]

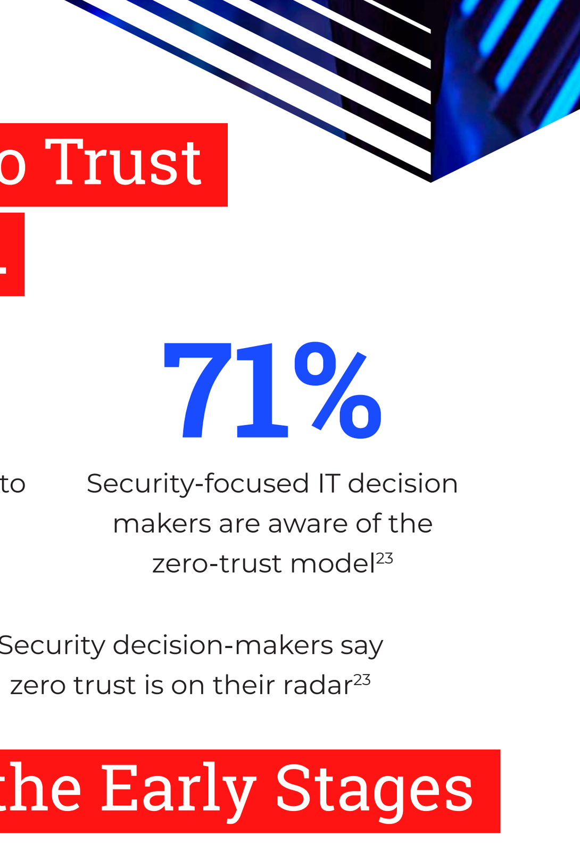
200B
Number of IoT smart devices expected to be in use this year[16]

500M+
Number of wearable devices expected to be sold worldwide by 2021[5/17/18]

$6 Trillion
Networked sensors in use in the next 14 years[5/19]

59%
Organizations that have suffered at least one print-related data loss[20]

2 Seconds
Time it takes to attach an IoT device[21]



3 Steps to Zero Trust

1. Validate User Identity
2. Employ Network Segmentation
3. Examine Access Behaviors

Data Shows Zero Trust Is Catching On…

78%
IT security teams that plan to embrace zero trust[13]

71%
Security-focused IT decision makers are aware of the zero-trust model[23]

42%
Security decision-makers say zero trust is on their radar[23]

…But Is Still In the Early Stages

47%
Enterprise IT security teams lack confidence in their ability to provide zero trust with their current technology[13]

10%
Piloting it[23]

8%
Actively using it in their organizations[23]

What Is the Government Doing?

74%
Federal government respondents say a zero-trust strategy is very important when expanding to the cloud[24]

48%
Federal IT executives say their agencies are moving away from traditional network perimeter defense tactics in favor of zero trust, identity-centered policies.[25]

59%
Government contractors and industry say their organization is on its way to adopting and identity-focused security approach[24]

"Today's networks are like castles that may have already been infiltrated. A rock-solid perimeter with a moat is still important, but guards keeping a watchful eye are now needed throughout the castle's interior to ensure valuables remain safe behind every wall. Segmenting can limit potential losses, and adopting a zero-trust policy ensures a stronger defense. There's no time to waste in implementing zero trust. Cybercriminals are already sneaking in through the back door."

- Cory Kramer, Principal Architect, Cybersecurity, Logicalis

Logicalis + Cisco: Taking business transformation seriously

An award-winning, Cisco-certified partner, Logicalis is trusted to deliver the expertise you can count on to transform your organization and enable business outcomes. We bring unrivaled knowledge, skills and experience to deliver IoT, cloud and security solutions that maximize existing investments, meet your needs and drive confidence.

LOGICALIS
Architects of Change

CISCO Partner
Global Gold Certified

Sources:
[1]Cisco: Zero Trust Security Website
[2]Cisco: Zero Trust - Going Beyond the Perimeter
[3]CNBC: Protect Against the Fastest-Growing Crime: Cyber Attacks
[4]Cybercrime Magazine: Top 5 Cybersecurity Facts, Figures, Predictions, And Statistics for 2019 To 2021
[5]Cybercrime Magazine: Cybercrime Damages $6 Trillion By 2021
[6]Verizon: 2019 Data Breach Investigations Report
[7]Cybercrime Magazine: Global Cybercrime Damages Predicted to Reach $6 Trillion Annually By 2021
[8]Centrify: Privileged Access Management in the Modern Threatscape
[9]Forrester: The Forrester Wave: Privileged Identity Management, Q4 2018
[10]CSO: Why a 'Zero Trust' Security Strategy is the Future for Your Business
[11]Cisco: Cisco Global Cloud Index: Forecast and Methodology, 2016-2021 White Paper
[12]IANS Research: Insights: 92% of Malware is Delivered Through Email
[13]Cybersecurity Insiders: 2019 Zero Trust Adoption Report
[14]Cisco: Anticipating the Unknowns
[15]Quocirca: Quocirca Global Print Security Landscape, 2019
[16]Intel: A Guide to the Internet of Things
[17]Gartner: Gartner Says Worldwide Wearable Device Sales to Grow 17 Percent in 2017
[18]Cybercrime Magazine: Cybercrime Damages $6 Trillion by 20201 with Official Annual Cybercrime Report

What we can do for your organization?

Contact Logicalis to learn how we can help.

Visit
www.us.logicalis.com

Call
866 456 4422