LOGICALIS
Architects of Change

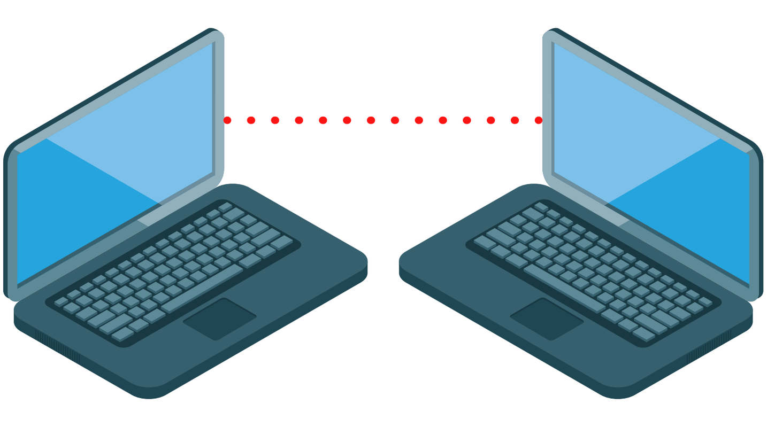
Infographic

Closing the Door on Cyberattacks

If you're responsible for the safety and security of your IT network, ask yourself this one critical question:
Is my network too open?

The Early Days

At the dawn of the internet, networking devices simply talked to one another. And it worked well. No boundaries meant free, easy access and open environments. But it also meant no walls or doors to keep bad guys out.



Fast Forward

Cybersecurity is the biggest IT challenge facing many businesses today. Every organization across every sector is under attack, and the cybercriminals behind these attacks are becoming more sophisticated, automated and destructive – and their attacks are becoming more costly.

Creating Boundaries Through Network Segmentation

Network segmentation is about using compartmentalization to limit the impact of a breach. By breaking a network into virtual compartments, you can lessen the spread of malware – including ransomware—by limiting how far it can travel. And by implementing the security principle of "least privilege," you can reduce both the likelihood and impact of these kinds of security incidents by only granting access to secure areas on an as-needed basis.

Does your sales team need network connectivity to your financial systems? Probably not. Imagine a cybercriminal entering your network through a salesperson's cloud-connected computer, then using that entryway to gain access to sensitive financial data. It's easy to do...unless you **close the door between sales and unrelated sensitive financial systems.**

"There are two types of companies: those that have been hacked and **those that don't know they have been hacked."**

- John Chambers, Chairman Emeritus, Cisco

FACT: No One is Safe

29.6%
Chance of experiencing a data breach within two years[0]

31%
Percentage increase since 2014 in the probability of experiencing a data breach in the next two years[1]

84%
Organizations that say traditional security solutions don't work in the cloud[3/4]

66%
IT enterprise professionals who say security is their biggest concern when it comes to embracing cloud computing[2/3]

68%
Businesses that took months or longer to discover a breach, often with a third party – like law enforcement or a partner – alerting them to the attack.[5]

FICTION: It Won't Happen To Me

Biggest Attacks on Record

- **3 Billion Records:** Yahoo holds the record for the largest data breach ever with 3 billion accounts compromised.[6]
- **$2 Billion:** An insider attack cost Boeing $2 billion and persisted for 30 years.[5]
- **110 Million Customers:** Data from 110 million Target customers was hijacked, including the banking and personal data of 40 million customers.[6/7]

Mid-Market Attacks are Rising

- **63%:** Midmarket companies experiencing a cyberattack in 2019, 27% more than in 2018[8]
- **55.6%:** Percentage of security threats midmarket companies investigate[9]
- **$184K:** The mean cost of cyber incidents among midmarket organization in 2019, a $140,000 increase over 2018's $44,000[8]

It Can Happen to Anyone

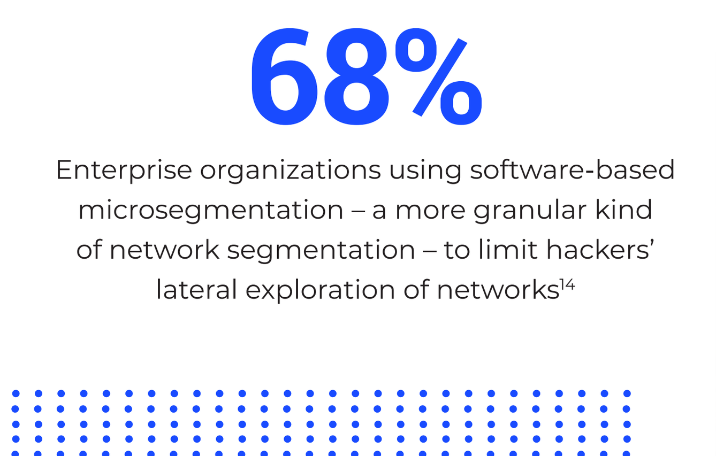
Frequency of Cyberattacks:
Every 39 Seconds[10/11]

1M+
The number of devices still at risk from WannaCry[12]

WannaCry Now?

Notable events such as the **WannaCry ransomware attack** caused substantial business disruption and economic loss by spreading rapidly through improperly segmented networks of large global name-brand companies. It affected hundreds of thousands of computers in 150+ countries in a matter of hours causing billions of dollars in damages.[12]

The Case for Network Segmentation



47%
Compromised organizations that say their attacker was able to move laterally from one data center server to another[13]

68%
Organizations that suffered a lateral attack and now have confidence additional network segmentation could definitely prevent future compromises[13]

Building Walls

68%
Enterprise organizations using software-based microsegmentation – a more granular kind of network segmentation – to limit hackers' lateral exploration of networks[14]

Zero Trust...

To combat cybercrime, many companies have adopted a **"zero trust" model:** Don't trust any entity inside or outside your perimeter; instead verify anything trying to connect to your network before granting access.[15/16]

...With Shades of Grey

Zero trust isn't quite as black-and-white as it sounds, though. Access doesn't have an on-off switch – there are thousands of shades of grey. A key lesson: *Grant only the appropriate levels of access.*

Example? When a smartphone is jailbroken, a laptop is using an outdated browser, or any device is requesting connection from outside of the corporate network, this risky behavior may require the user's access to be restricted to low-risk network segments or to be denied altogether.

No Fear

While malware and breaches are both inevitable and concerning, Logicalis believes in a "No Fear" policy:

"Don't make security decisions based on fear. Use best practices like **zero trust** and **network segmentation** to manage risk instead."

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

What Can Network Segmentation Do for You?

3 Important Benefits

1. Reduces Risk
2. Applies Best Practices from Cybersecurity Control Frameworks Like NIST CSF and ISO 27001
3. Decreases Excessive Broadcast Traffic, Improving Performance and Visibility

Build Your Walls and Doors Over Time

Take A Phased Approach to Network Segmentation

Network segmentation doesn't have to be an all-or-nothing proposition. Start with a few high-yield quick wins, then continue to build your network segmentation over time.[17]

"In sci-fi shows, spaceships always have doors that section off portions of the ship to limit damage in the event the perimeter is breached. The same is true of your network. If you section off your most valuable data, you'll limit what a criminal can steal or damage. The solution is clear: First install, and then close the doors."

- Jason Malacko, Director of Security Architecture, 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. IBM: "2019 Cost of a Data Breach Report"
2. LogicMonitor: "Cloud Vision 2020: The Future of the Cloud Study"
3. CMSWire: "What is Microsegmentation?"
4. Crowd Research Partners: "2018 Cloud Security Report"
5. Verizon: 2018 Data Breach Investigations Report
6. Wesley Clover: "23.2 Million Cyber Security Victim Accounts Worldwide Used "123456" as Password"
7. Computerworld: "Target Breach Happened Because of a Basic Network Microsegmentation Error"
8. Hiscox: Cyber Readiness Report 2019
9. Cisco: Small and Mighty Cybersecurity Special Report
10. Security Magazine: "Hackers Attack Every 39 Seconds"
11. Cybint: "15 Alarming Cyber Security Facts and Stats"
12. TechCrunch: "Two Years After WannaCry, a Million Computers Remain at Risk"
13. Cisco/Enterprise Strategy Group: "Cisco: ACL Survey"
14. Dark Reading: "Microsegmentation: Strong Security in Small Packages"
15. Cisco: "Cisco Zero Trust Security"
16. CSO: "What is Zero Trust? A Model for More Effective Security"
17. SC Media: "Improving Security with Microsegmentation: Where Do I Start?"

What we can do for your organization?

Contact Logicalis to learn how we can help.

Visit
www.us.logicalis.com

Call
866 456 4422