ISSA Information Systems Security Association

Thought Leadership Web CONFERENCE

Zero Trust: The Evolution of Perimeter Security

May 15, 2019

Zero Trust: The Evolution of Perimeter Security

ISSA
Information Systems Security Association International

Today's web conference is generously sponsored by:

Akamai

Akamai Technologies
https://www.akamai.com/

Zero Trust: The Evolution of Perimeter Security

Moderator

Jorge Orchilles, SANS Certified Instructor

Jorge Orchilles is a published author who holds post-graduate degrees from Stanford and Florida International University in Advanced Computer Security & Master of Science respectively. Jorge leads the offensive security teams in a large financial institution, is a SANS Certified Instructor and author with his new course Security 564: Red Team Exercises and Adversary Emulation debuting at SANS Network Security 2019, and serves on the Board of Directors of the ISSA South Florida Chapter since 2010. Jorge speaks English, Spanish, and Portuguese in decreasing order of fluency. He also loves to watch and play soccer.

Zero Trust: The Evolution of Perimeter Security

Speaker

Dipto Chakravarty, Chairman of Security COE, IoT Community

Dipto Chakravarty is the author of three best-selling books on computer architecture and security from McGraw-Hill and Wiley that have been translated in five languages. He has 11 patents to his credit in AI, security and cloud, holds a M.S in Computer Science from U. of Maryland, GMP from Harvard Business School, and EMBA from Wharton School U. Penn. He is currently the Chairman of Security, Privacy and Trust COE for IoT Community, and board member at RANK Software.

ISSA

Information Systems Security Association
International

www.issa.org

Zero Trust – The Evolution of Perimeter Security

May 15, 2019

ISSA
Information Systems Security Association International

Zero Trust Revolution within the Evolution of Perimeter Security

Dipto Chakravarty dchakravarty@gmp4.bs.edu
Board Member, RANK Software
Chairman of Security, Privacy & Trust COE, IoT Community

ZT Concept

WHAT:

- A security model that no longer assumes that actors, systems or services operating from within the perimeter should be implicitly trusted

HOW:

- Use micro-segmentation and granular perimeter enforcement.
- Base it on users, their locations and their data
- Determine whether to trust a user, machine or app seeking access to a part of the enterprise.

ZT Principles

REQUIREMENTS:

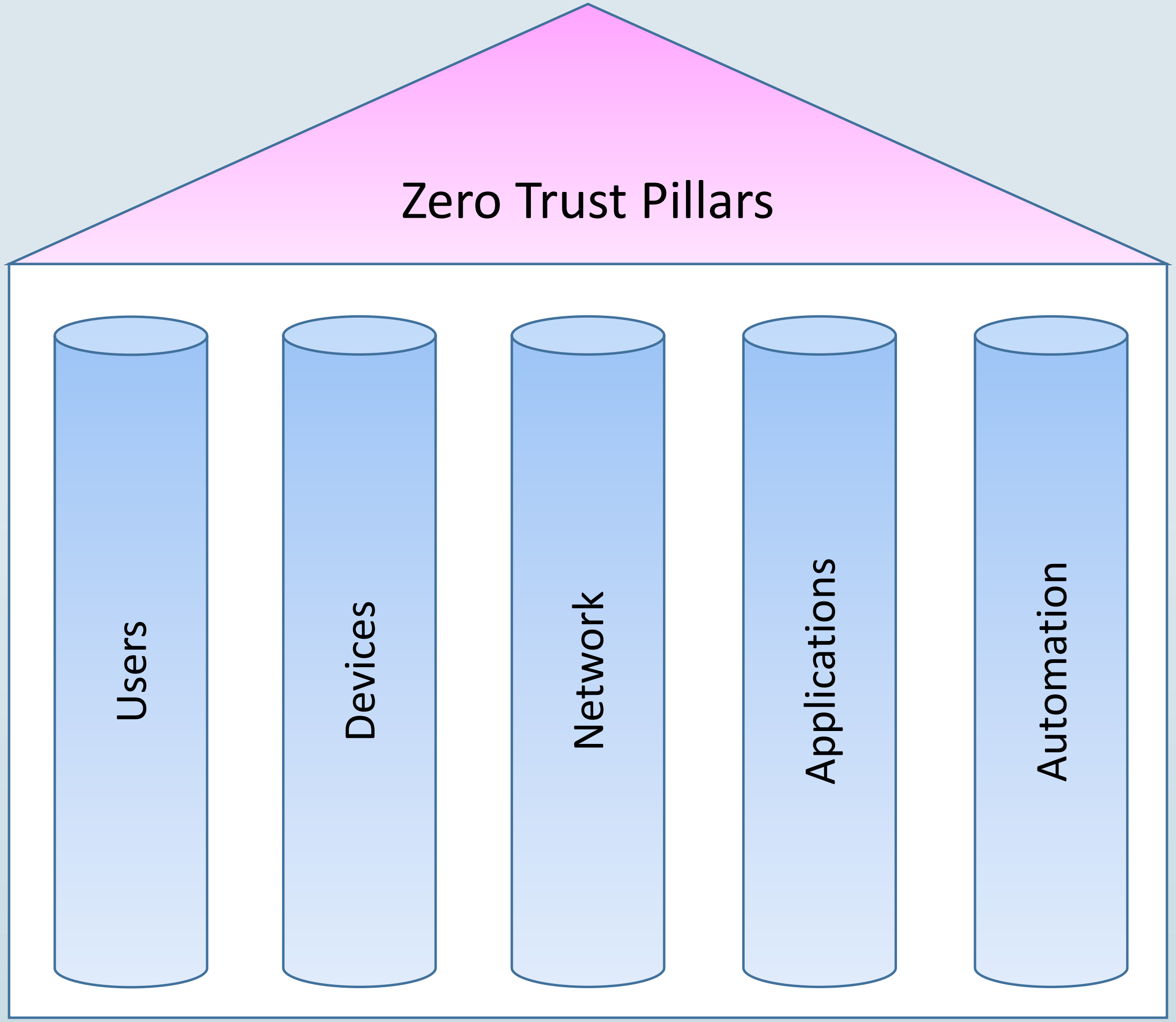
1. Access data to/from anywhere
2. Assume “never trust and always verify”
3. Continuous AuthN
4. 360 visibility across the network

ASSERTIONS:

1. Assume network hostility exists
2. Assume external and internal threats exist
3. AuthN/AuthZ every user and device
4. Make policies dynamic

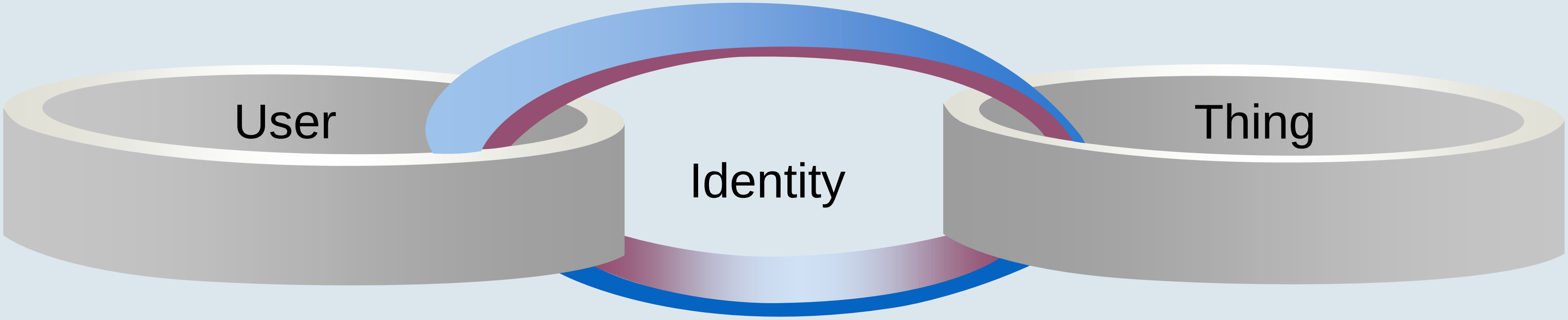
ZT Pillars

1. Users
2. Devices
3. Network
4. Applications
5. Automation



Source: Forrester Report, 2010

1. Security of the Identity

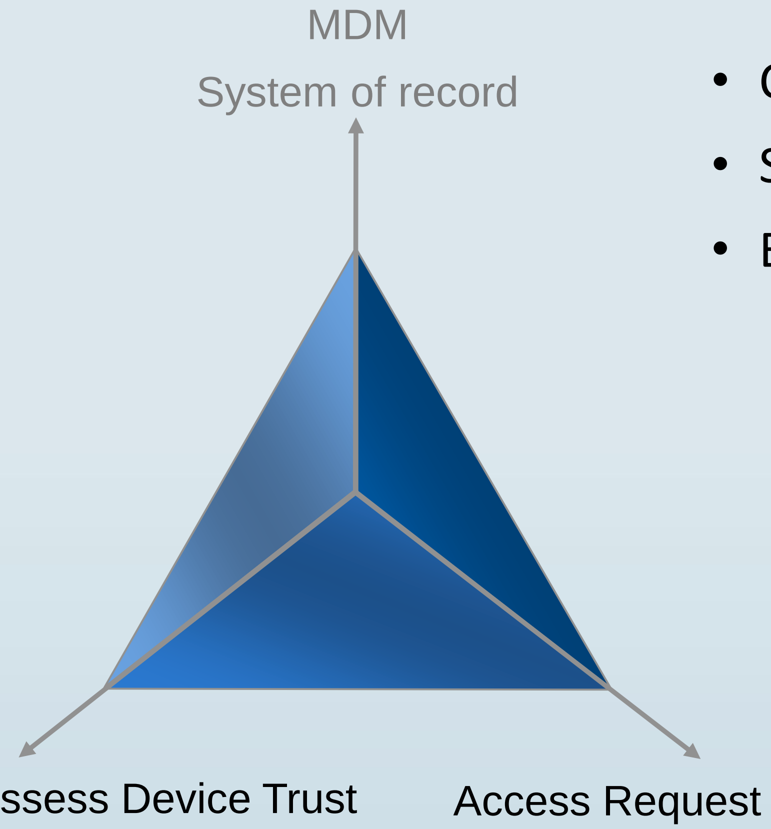


- ✓Credential
- ✓2nd Factor AuthN
- ✓Adaptive AuthN

- ✓Continuous monitoring
- ✓Minimum privileges
- ✓2nd Gen Gateways

2. Security of the Device

- Device
- Data
- Location

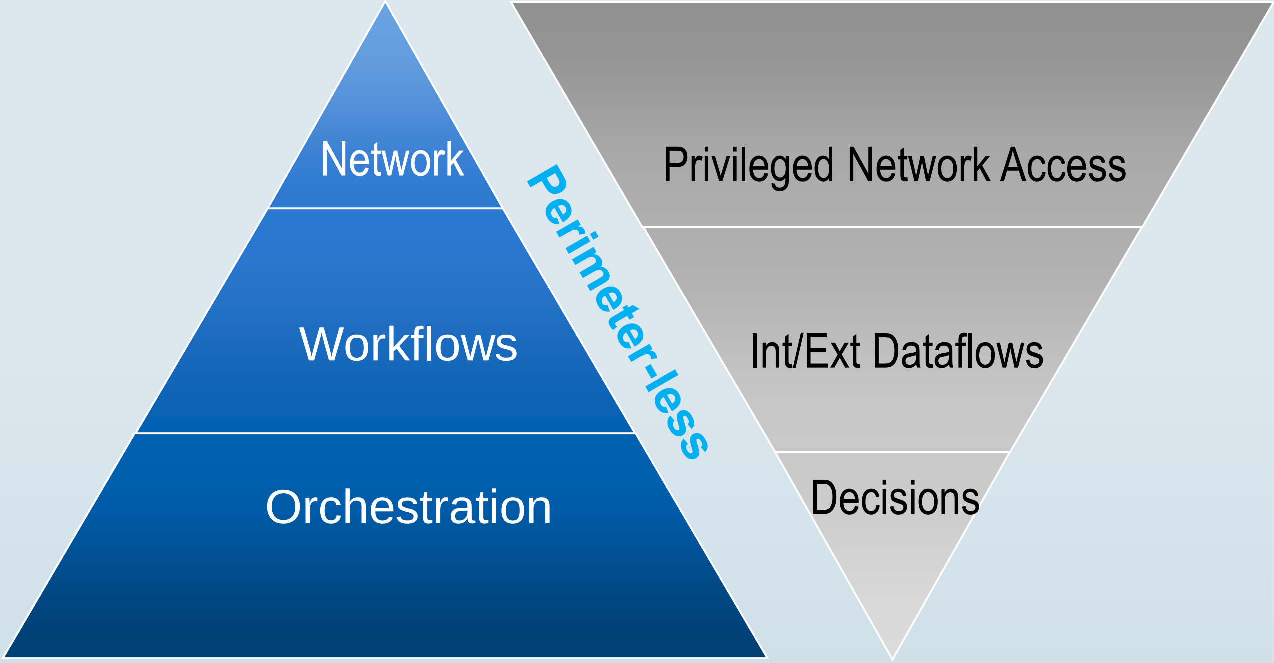


- Compromise state
- Software version
- Encryption

3. Security of the Network

- Dynamic
- Adaptive
- Resilient
- Segmented

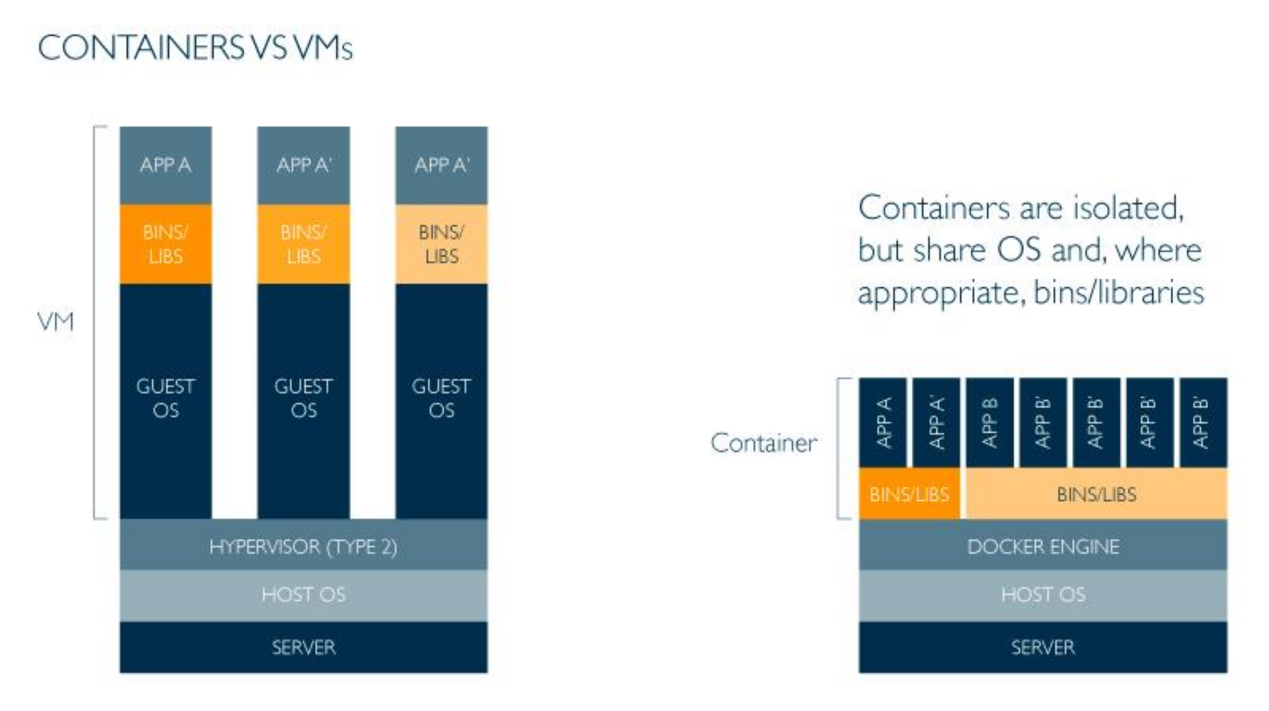
Modern Perimeter-less Sw-defined Network



Traditional Network with FW Perimeter

4. Security of the Apps

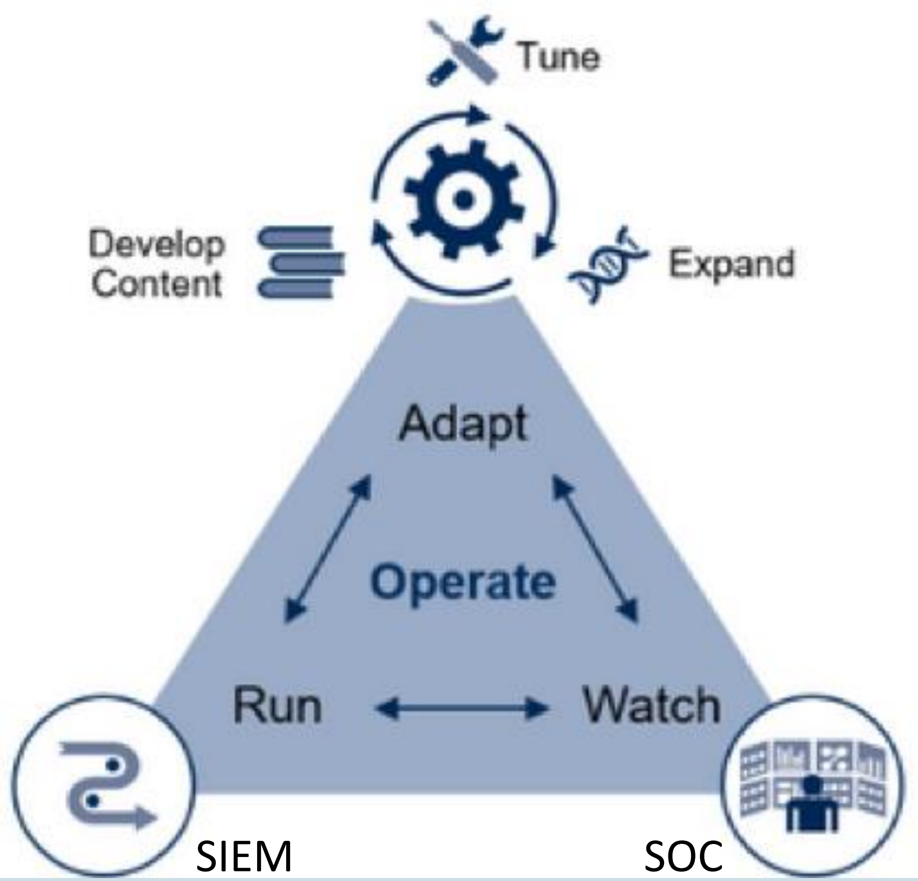
- VMs
- Containers



Better resource usage, faster startup, more portable

5. Security of Automation

- Automate tasks
- Enable interaction among
  - SOC and SIEM
  - SIEM with AI/ML
  - SIEM with SOAR
  - SIEM with UEBA
- Allow end-to-end oversight
- Streamline management of disparate security systems



Automation & Orchestration Team

Source: Gartner Report, Nov 2018

ZT Summary

- A pragmatic security approach that does not assume actors, systems or services within the perimeter should be implicitly trusted
- So, it uses micro-segmentation and granular perimeter enforcement
  - ✓ on users
  - ✓ user locations
  - ✓ user data
- ZT determines when to trust a user, machine or app seeking access to a part of the enterprise

ISSA

Information Systems Security Association International

www.issa.org

QUESTIONS?

Zero Trust: The Evolution of Perimeter Security

Speaker

Faraz Siddiqui, Principal Solution Engineer, Akamai

Faraz Siddiqui is a Principal Solution Engineer at Akamai where he helps large enterprises in adapting Zero Trust security model with various transformation stages. He is an enterprise security evangelist with years of experience working for industry leading players like F5 Networks, Cisco Systems and Alcatel Lucent.

Faraz joined Akamai in 2016 through an acquisition of Soha Systems, a security startup which developed a completely new and modern way of enterprise access using a Cloud perimeter approach, which became the foundation of Akamai Zero Trust architecture.

At Soha Systems, he was the first Sales Engineer/TME responsible for leading different aspects of product management and pre-sales activities. Faraz has been a frequent speaker at various public events and conferences F5 Agility, Cisco Live, RSA and Akamai Edge.

He has published several white papers, blogs, industry best practices on application delivery, data center virtualization, Identity aware proxies and L4-7 service insertion techniques.

Having worked with large scale enterprises for over a decade, he has a great deal of understanding of the frustrations and challenges most customer face in transformation their legacy access architectures.

Faraz holds Master’s in Electrical and Computer Engineering.

ISSA

Information Systems Security Association International

www.issa.org

ISSA Thought Leadership Webinar

Zero Trust: The evolution of Perimeter Security

May 15, 2019

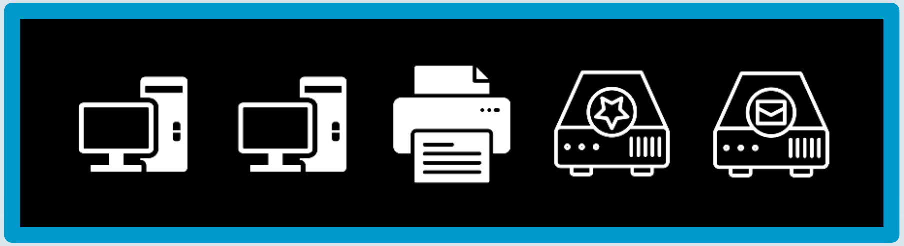
AGENDA

- Evolution of Perimeter Security
- Modern access requirements
- What is Zero Trust
- Zero Trust Implementation models
  - Micro-segmentation
  - Identity Aware Proxy
- Summary

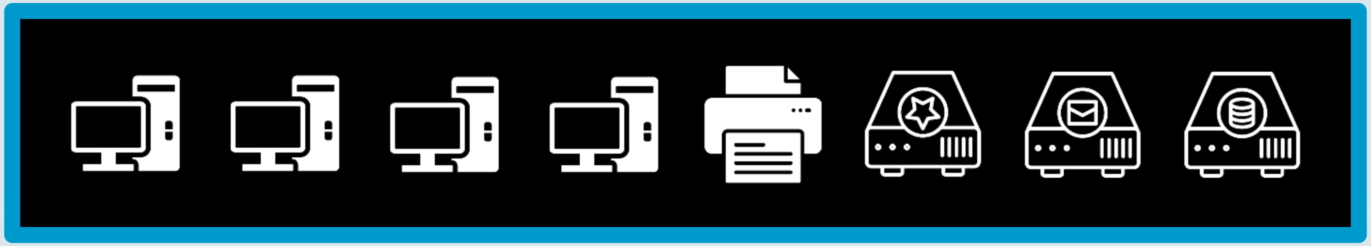
Evolution of Perimeter Security

Evolution of Perimeter Security

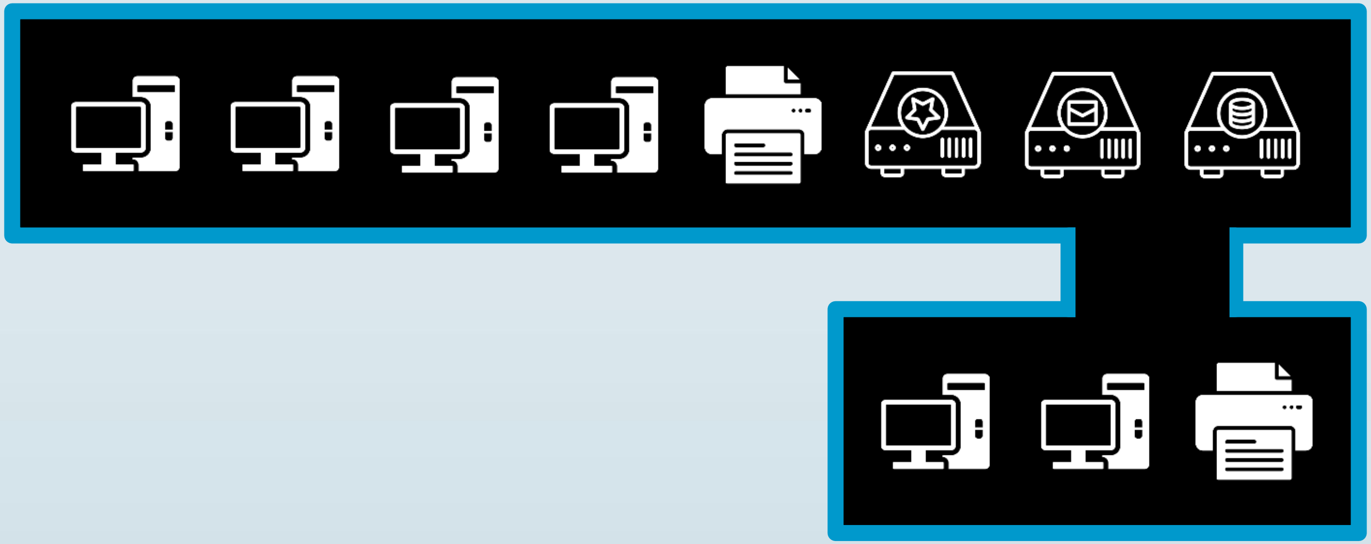
Corporate networks start out pretty simple.



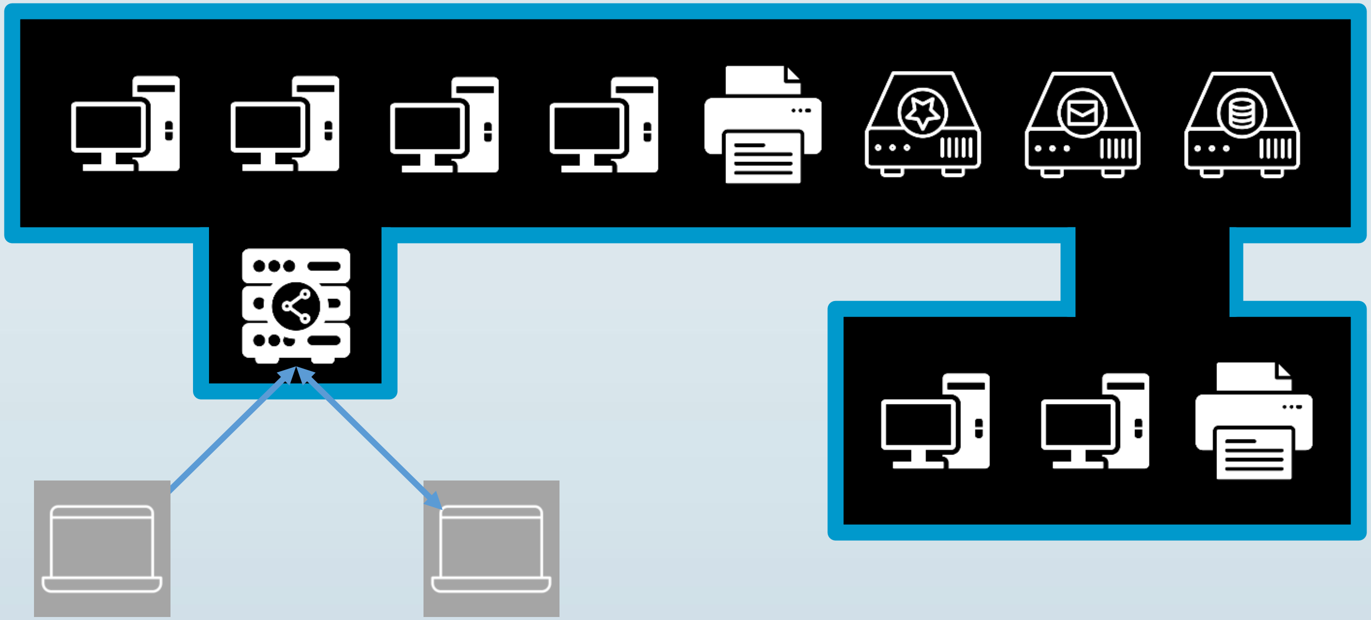
Evolution of Perimeter Security



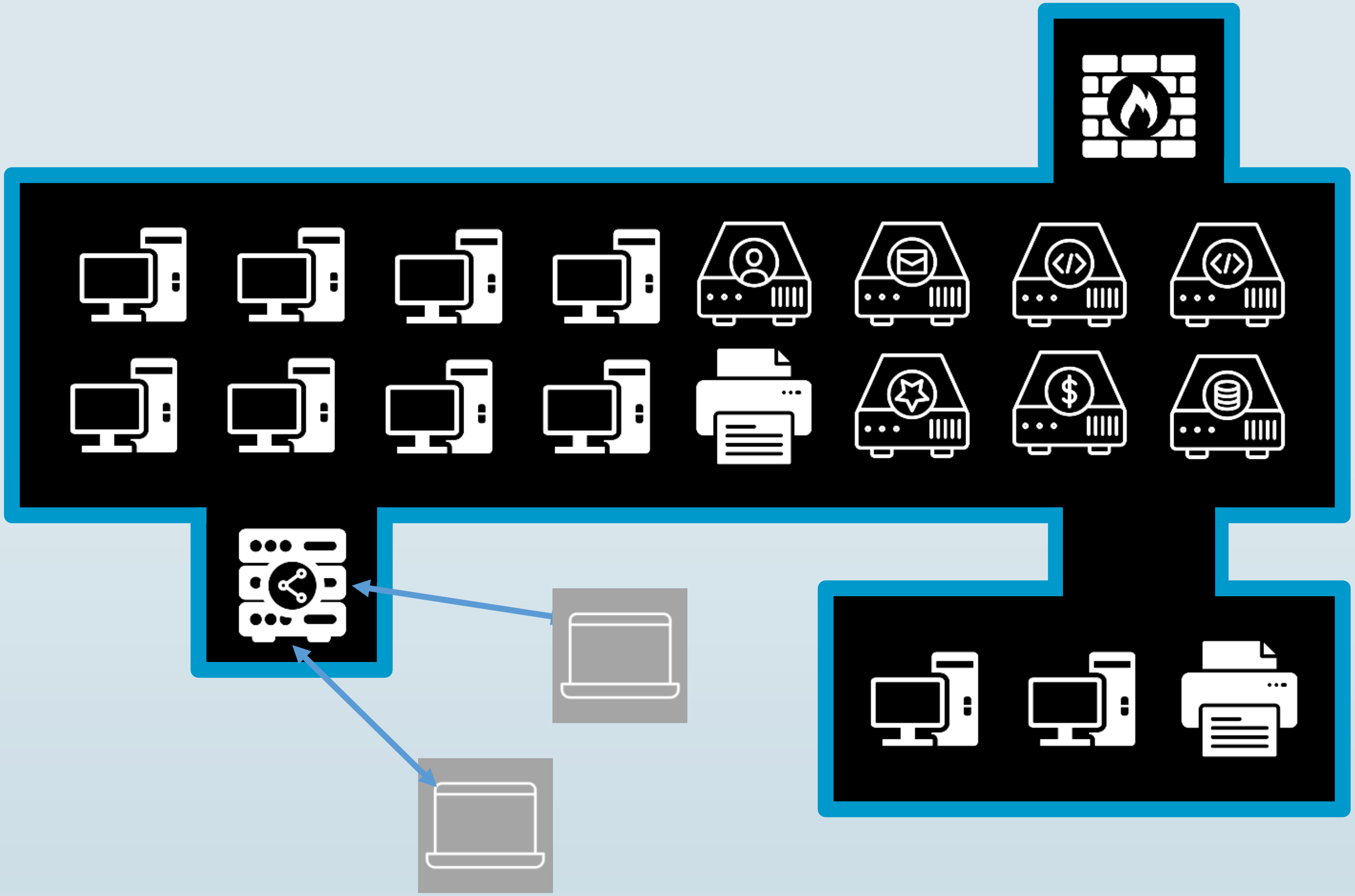
Evolution of Perimeter Security



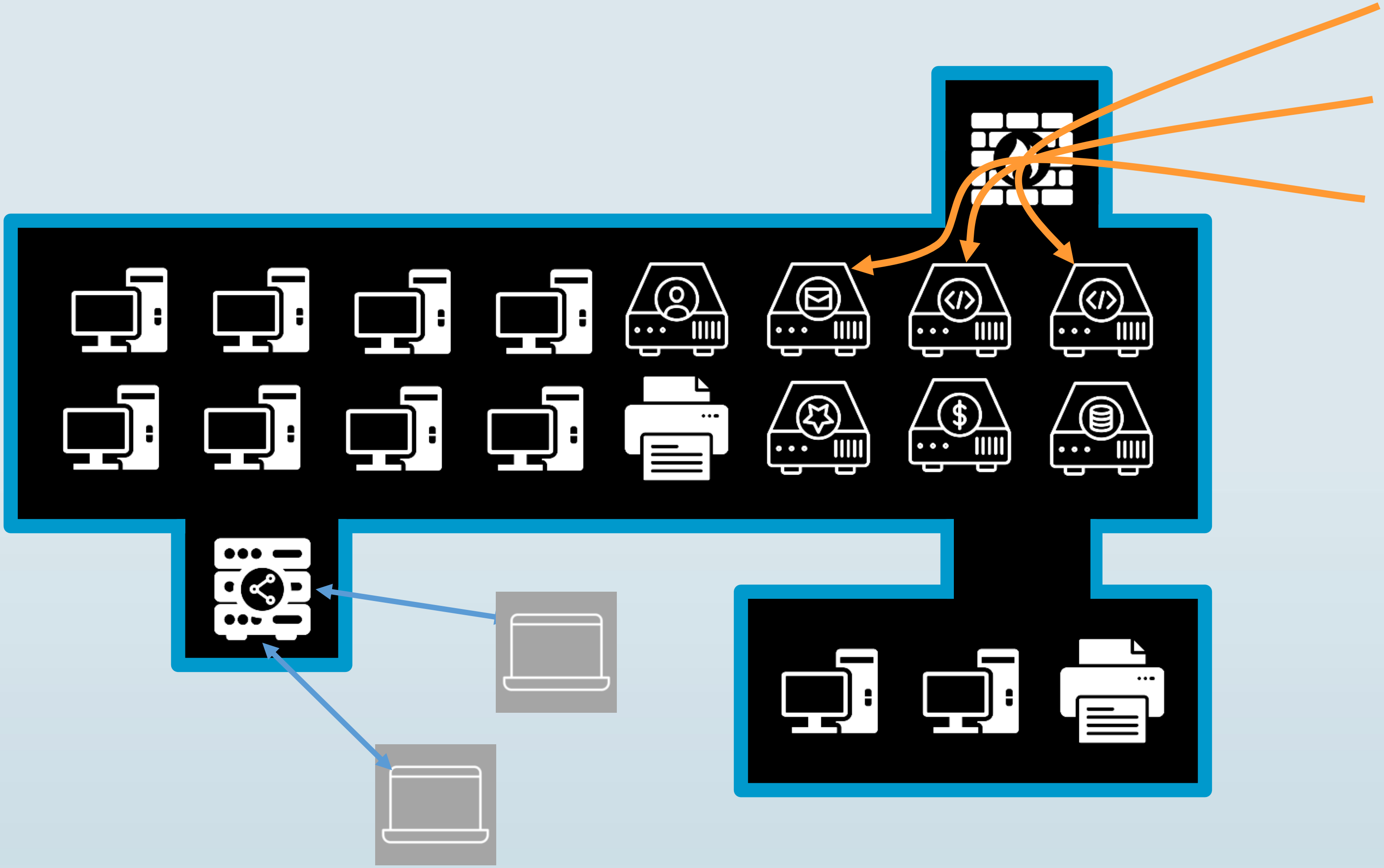
Evolution of Perimeter Security



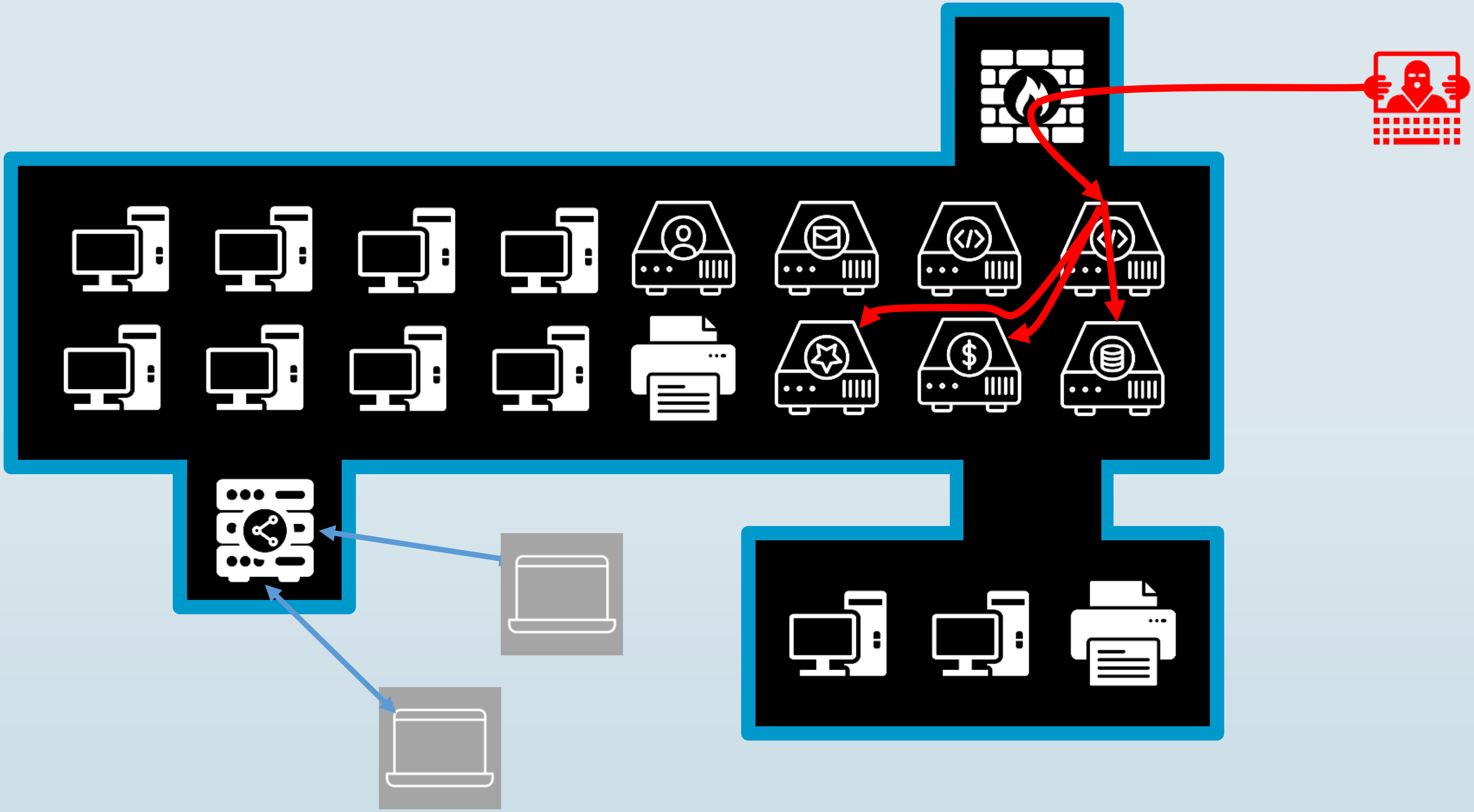
Evolution of Perimeter Security



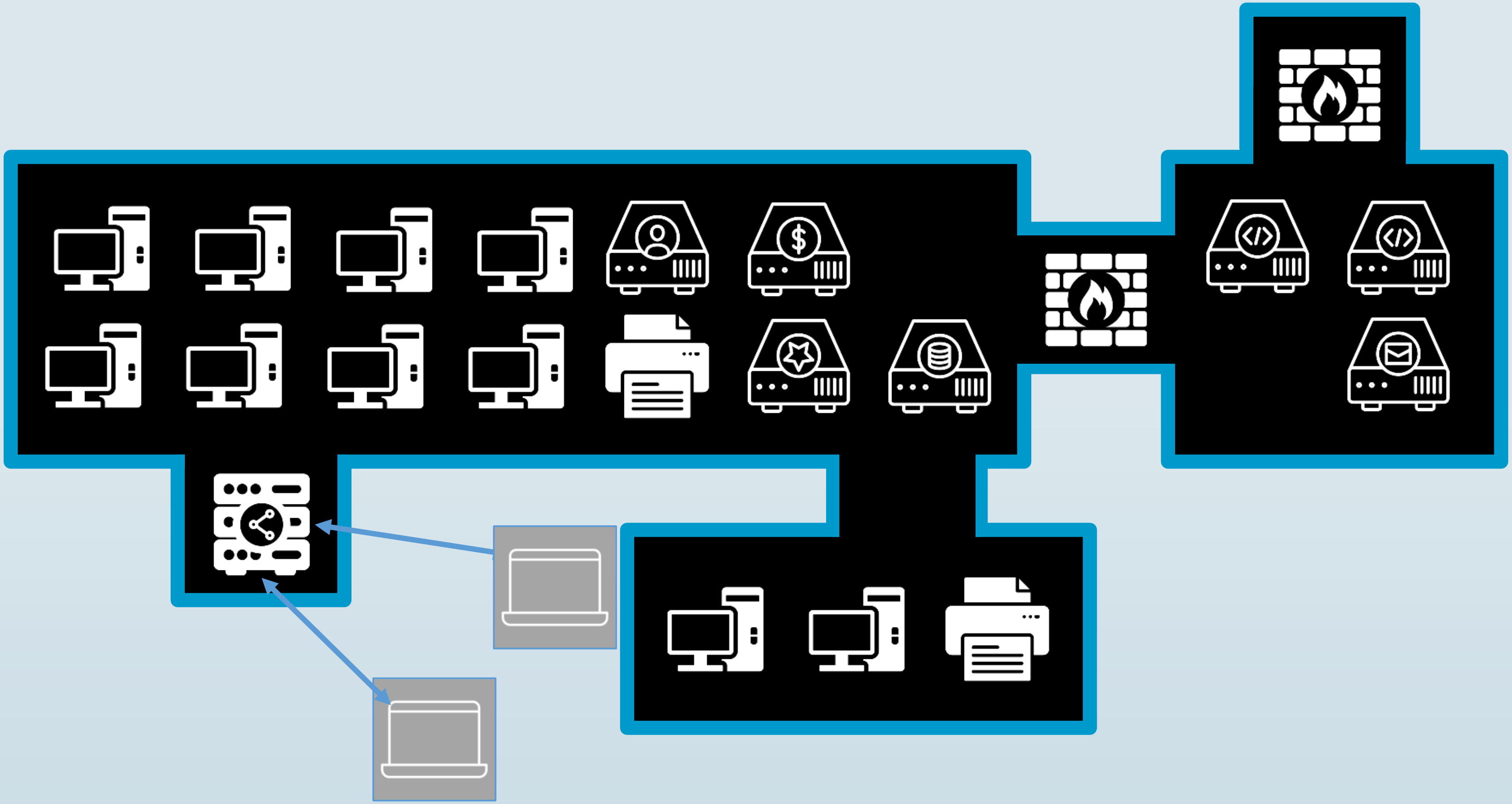
Evolution of Perimeter Security



Evolution of Perimeter Security



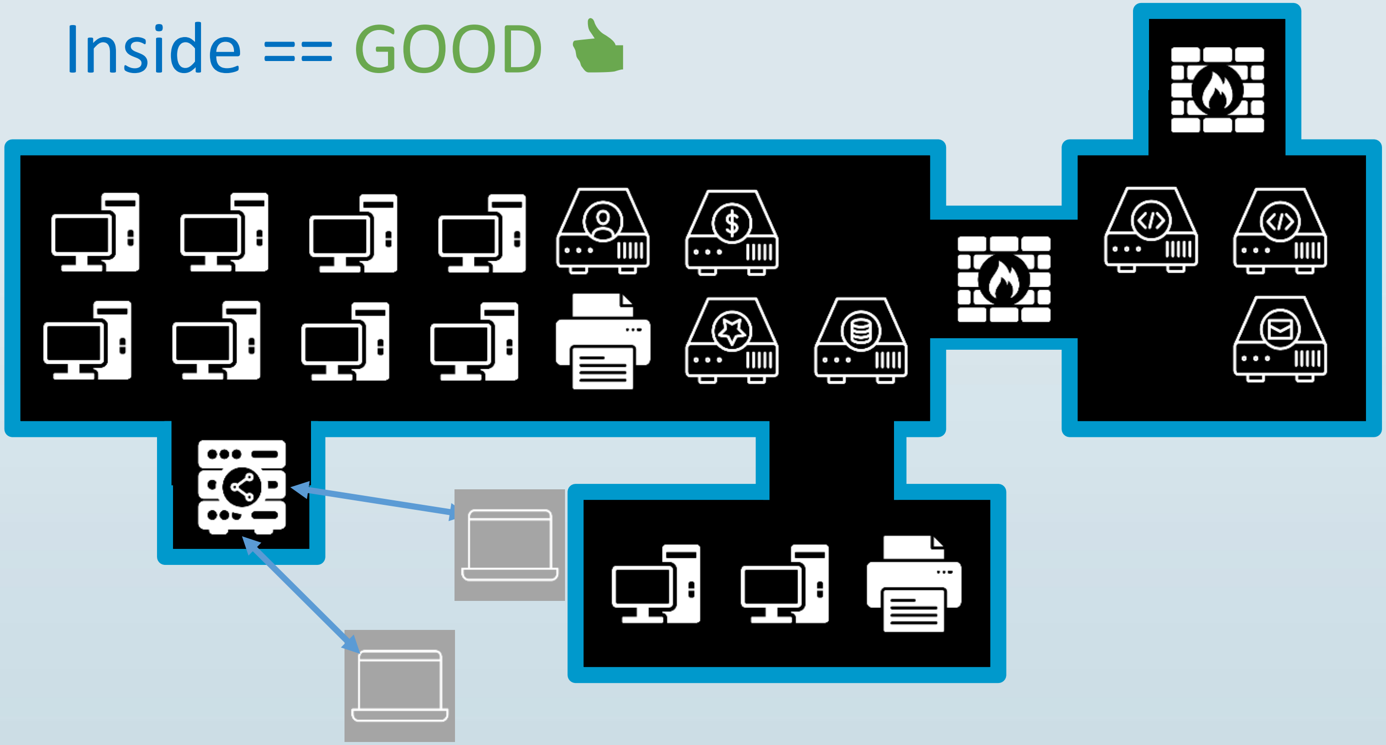
Evolution of Perimeter Security



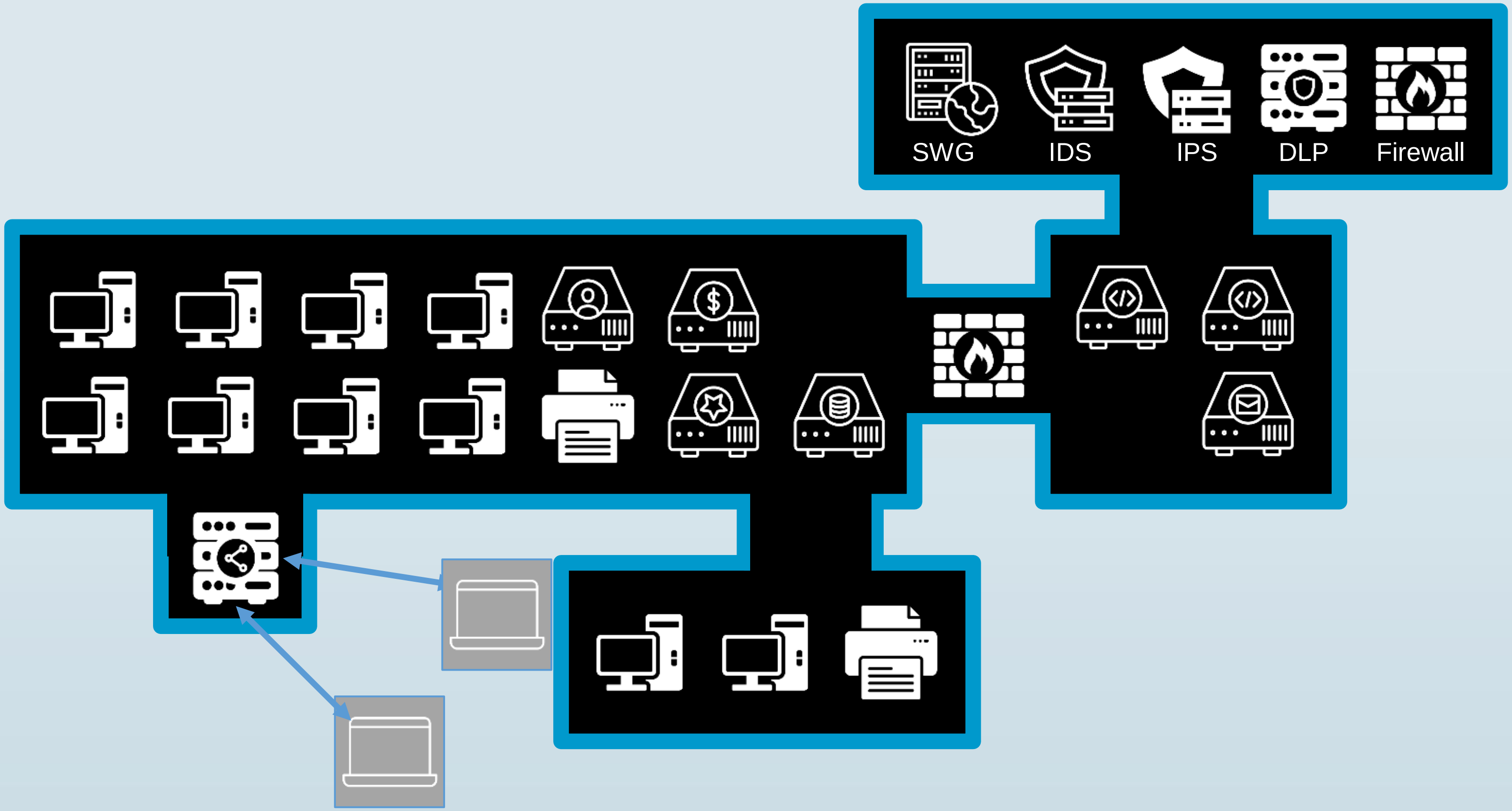
Evolution of Perimeter Security

Outside == BAD 👎

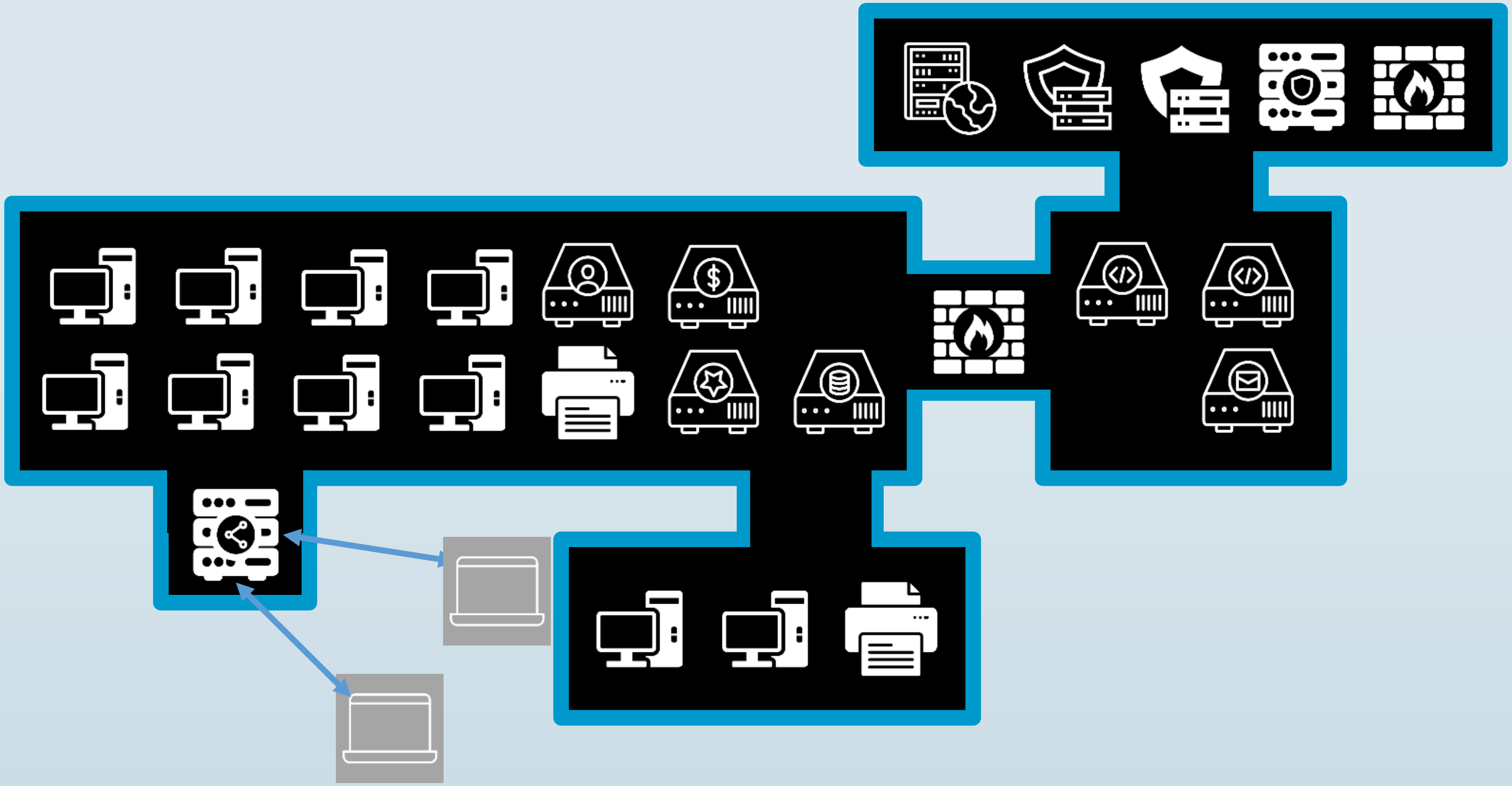
Inside == GOOD 👍



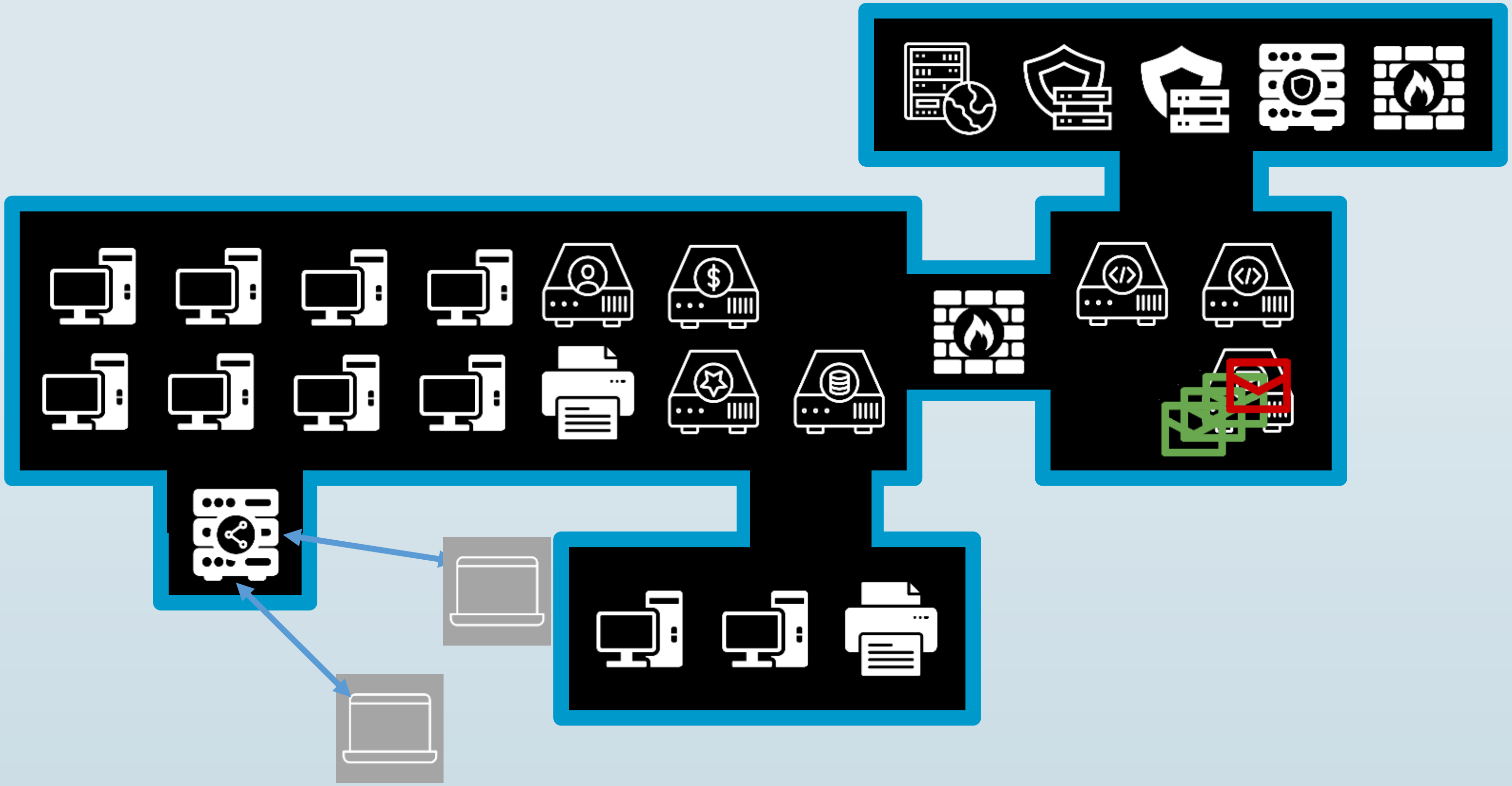
Evolution of Perimeter Security



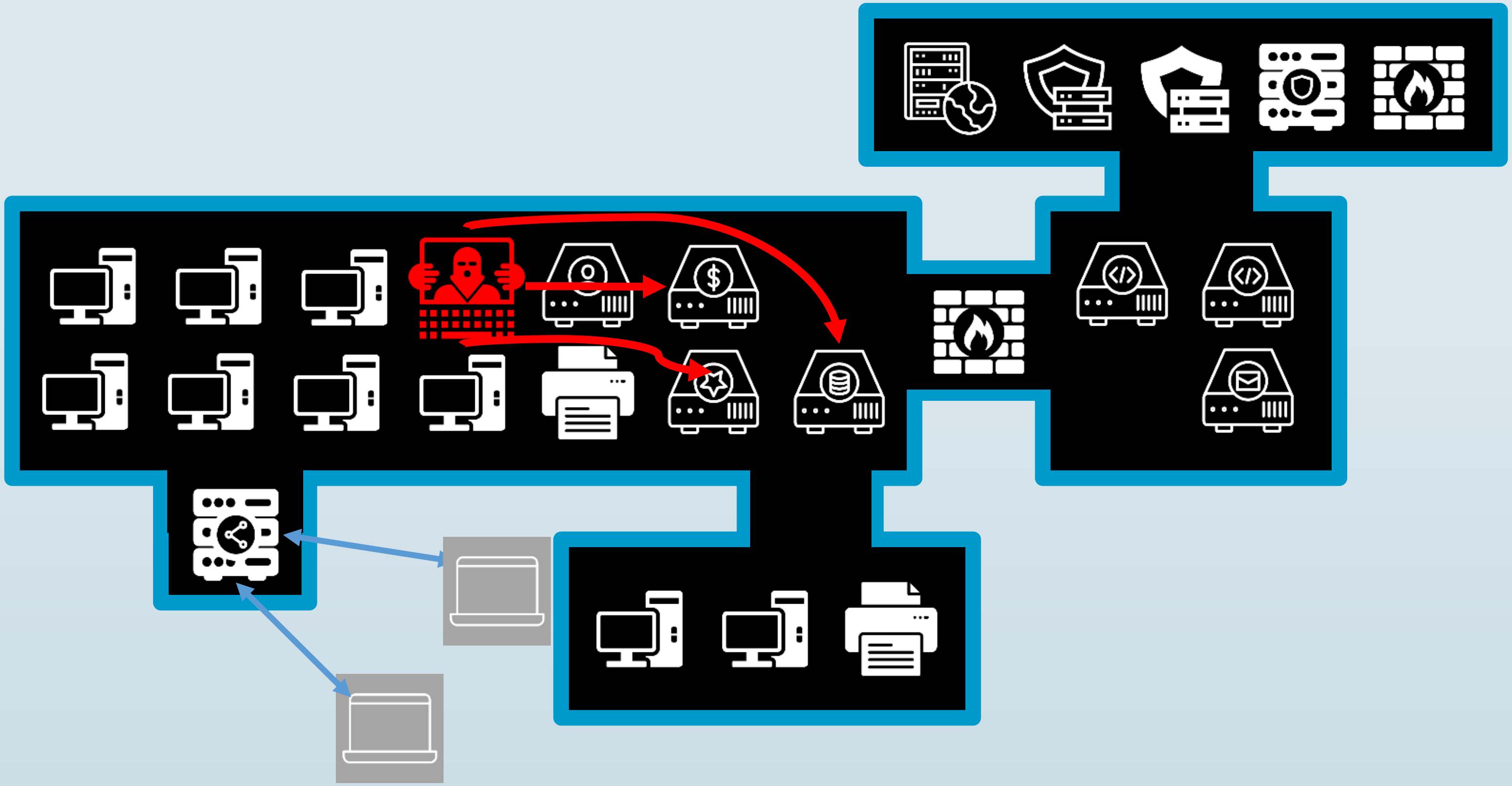
Evolution of Perimeter Security



Evolution of Perimeter Security

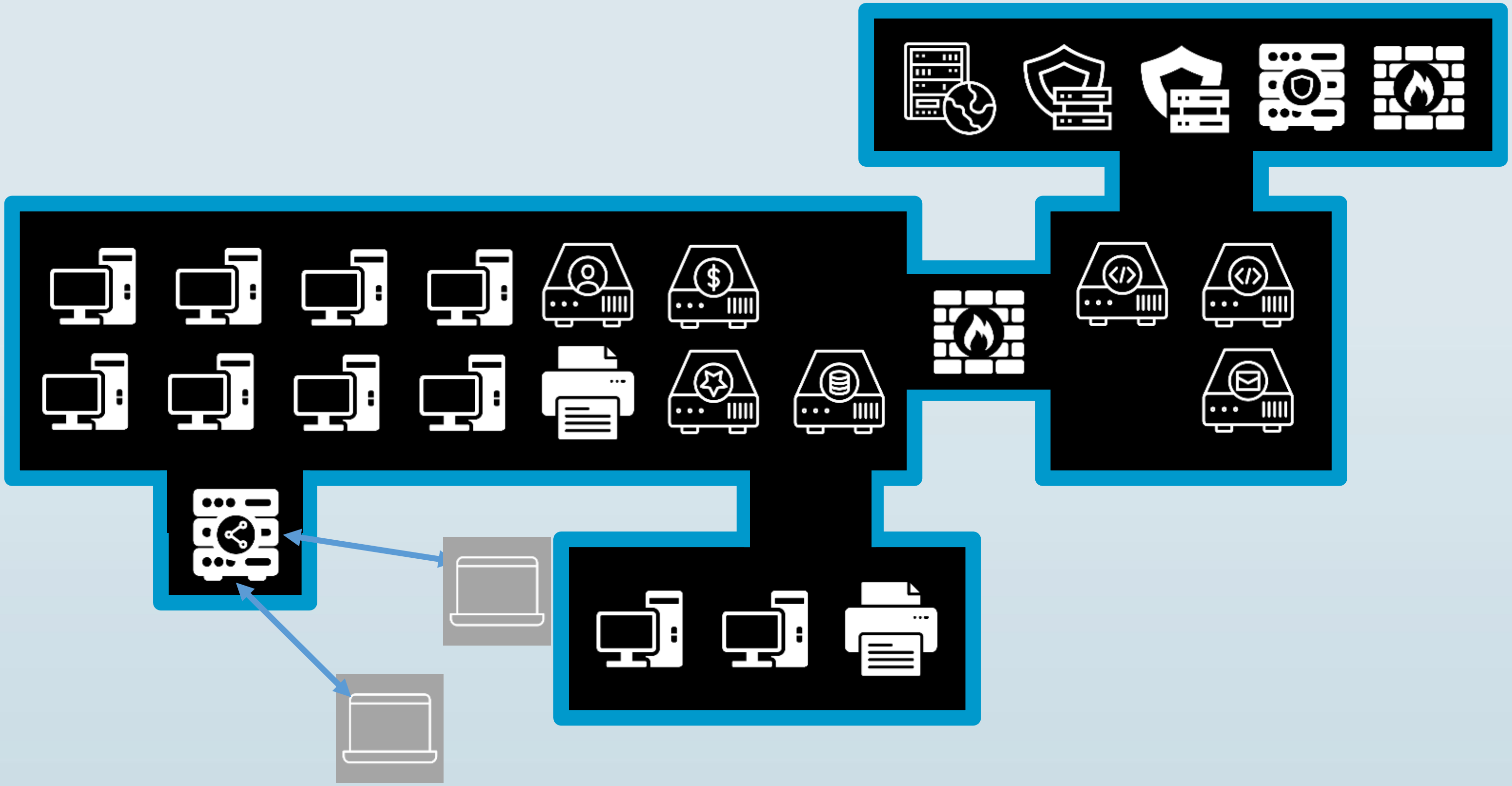


Evolution of Perimeter Security



Evolution of Perimeter Security

A common network



It’s understandable how we arrived here.

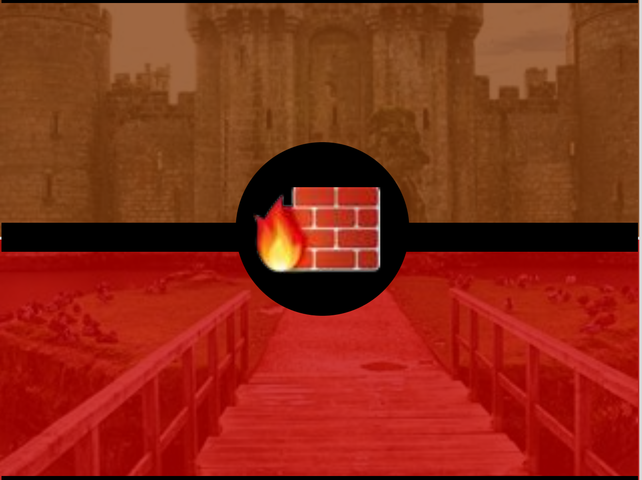
We reached this architecture through logical steps.

Inside is good

Outside is bad

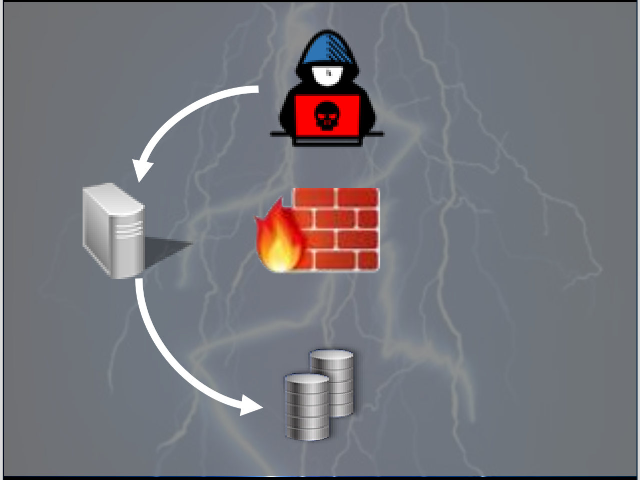
But the end result after 30+ years is highly dangerous.

Inside is good



Outside is bad

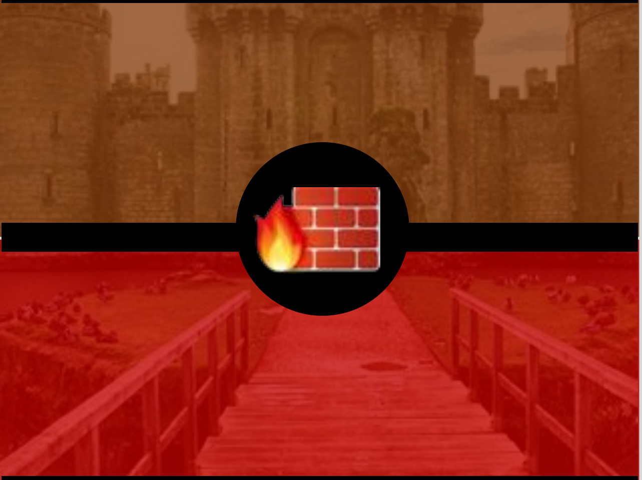
Hackers take



Easiest path

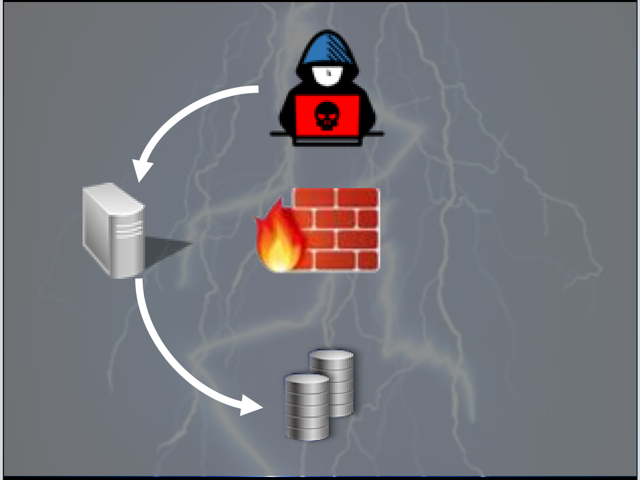
So what comes next?

Inside is good



Outside is bad

Hackers take



Easiest path

More point solutions

vs. new architecture

ISSA

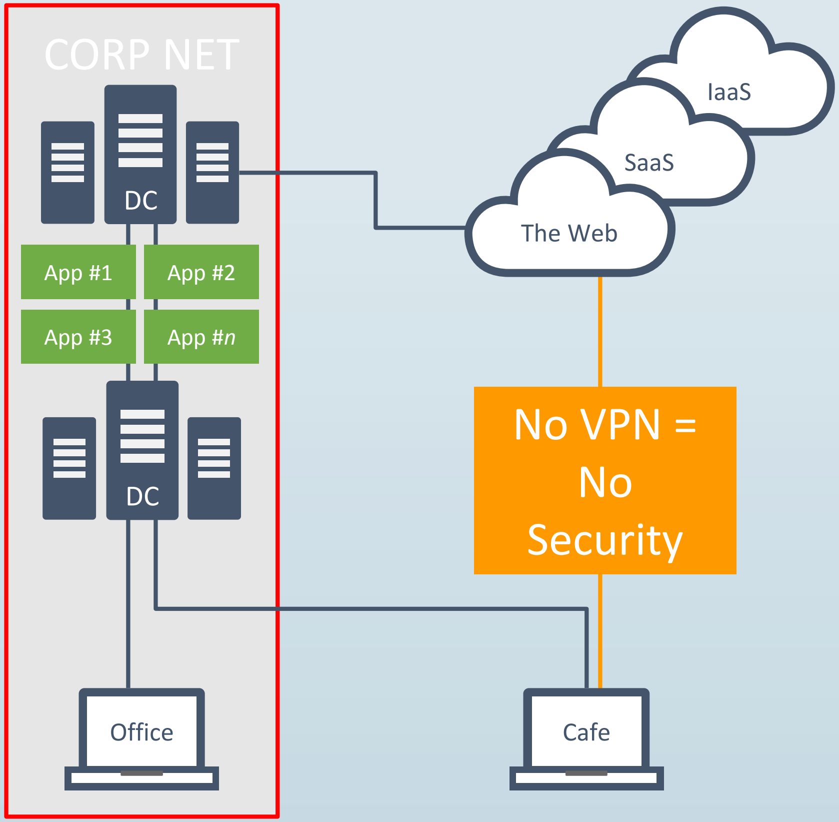
Information Systems Security Association International

www.issa.org

Modern Access Requirements

Enterprises Are Turning Inside Out

Users & Corporate Apps Have Left The Building



- Complex
- Slow
- High Risk

Bottom line: security perimeters belong in the past

"...the idea of a corporate perimeter becomes quaint–even dangerous."

Excerpt from Forrester's *Future-Proof your Digital Business with Zero Trust Security*

We no longer need to debate the need for change

What is Zero Trust?

Network security model championed by Forrester analysts

Zero Trust principles include

- Assume hostile environment
- Don't distinguish between external & internal
- Never trust and only deliver applications/data to authenticated & authorized users/devices
- Always verify with logging & behavioural analytics

ZERO TRUST –
It is largely a strategy

Acknowledgement by industry that more point solutions are not the answer.

Let’s fix the root problem: the architecture.

There is no

INSIDE

Your users and apps can be

ANYWHERE

All access must be

AUTHENTICATED

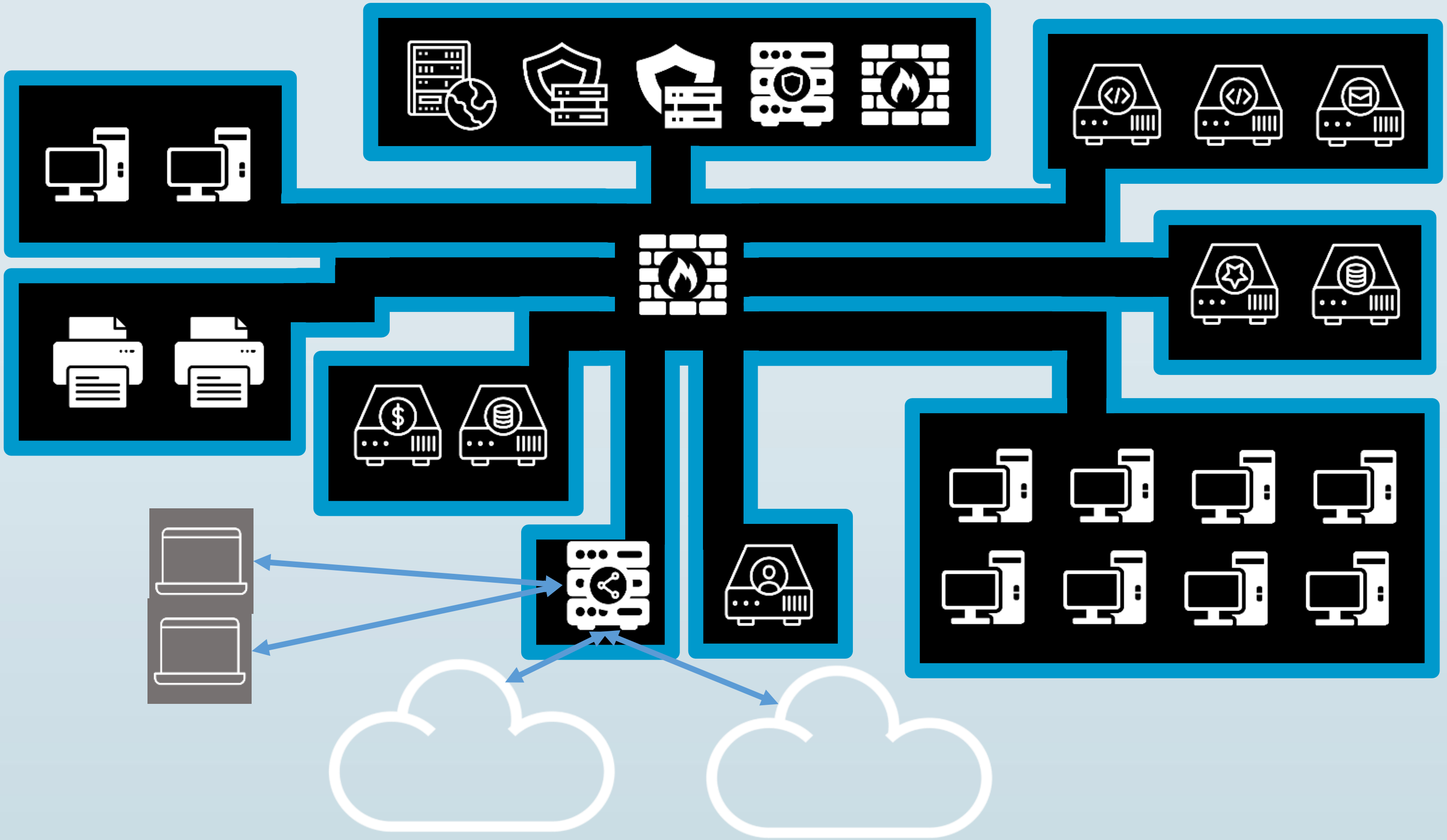
AUTHORIZED &

VERIFIED

Zero Trust Implementation models

Model 1

Micro-Segmentation



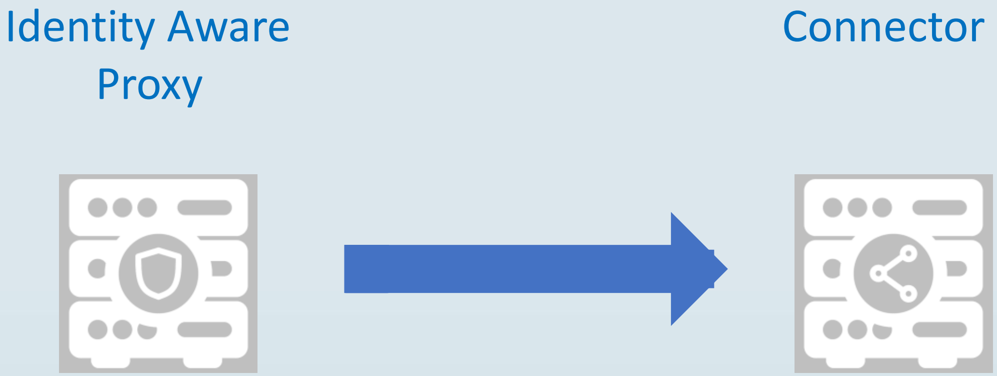
Model 1

Micro-Segmentation

- Hard / Expensive to maintain
- Hard to automate well
- The firewall can allow inter-segment access as needed
- Dramatically reduces the ability to pivot to unrelated systems

Model 2

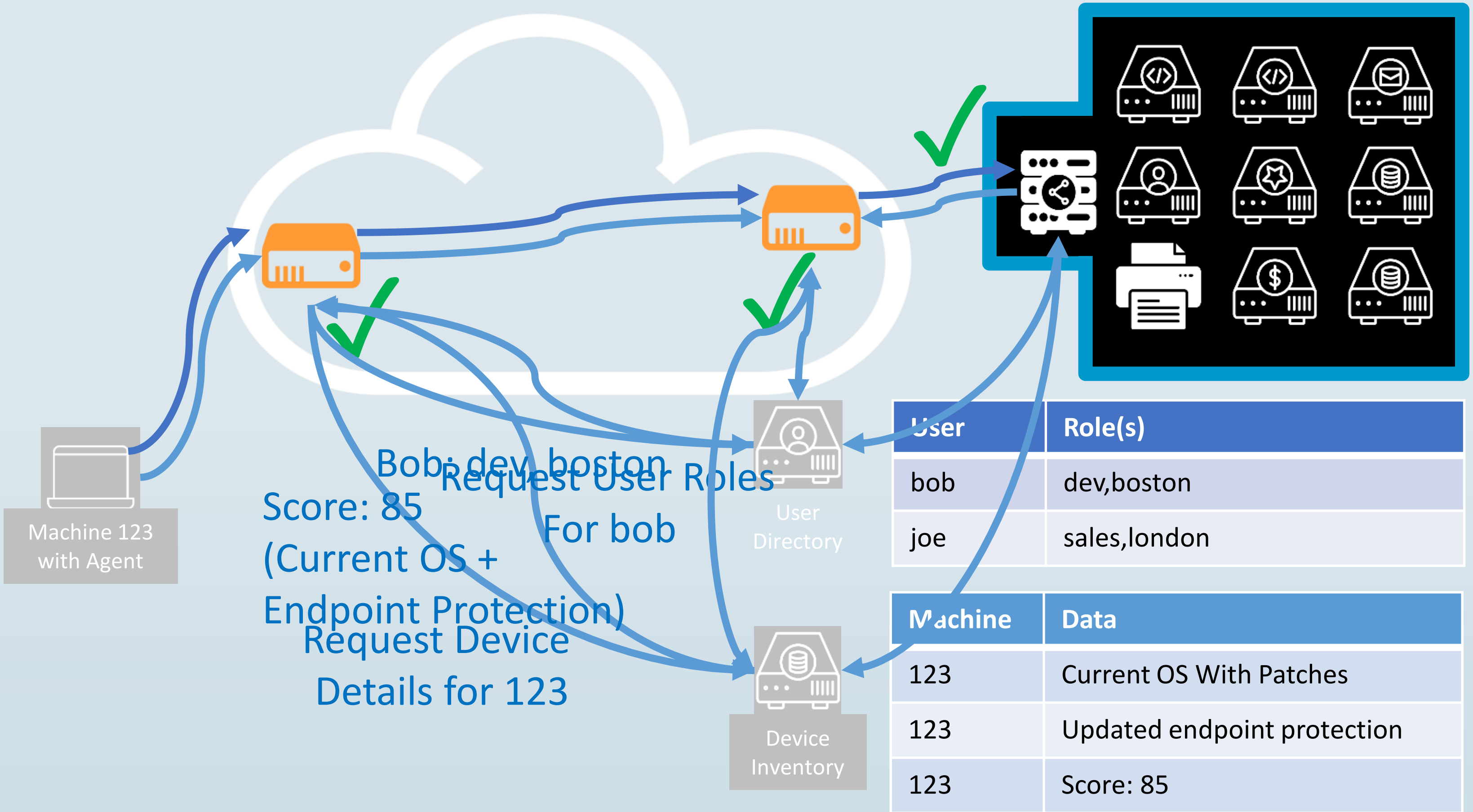
Identity Aware Proxies



Identity Aware Proxy

Connector

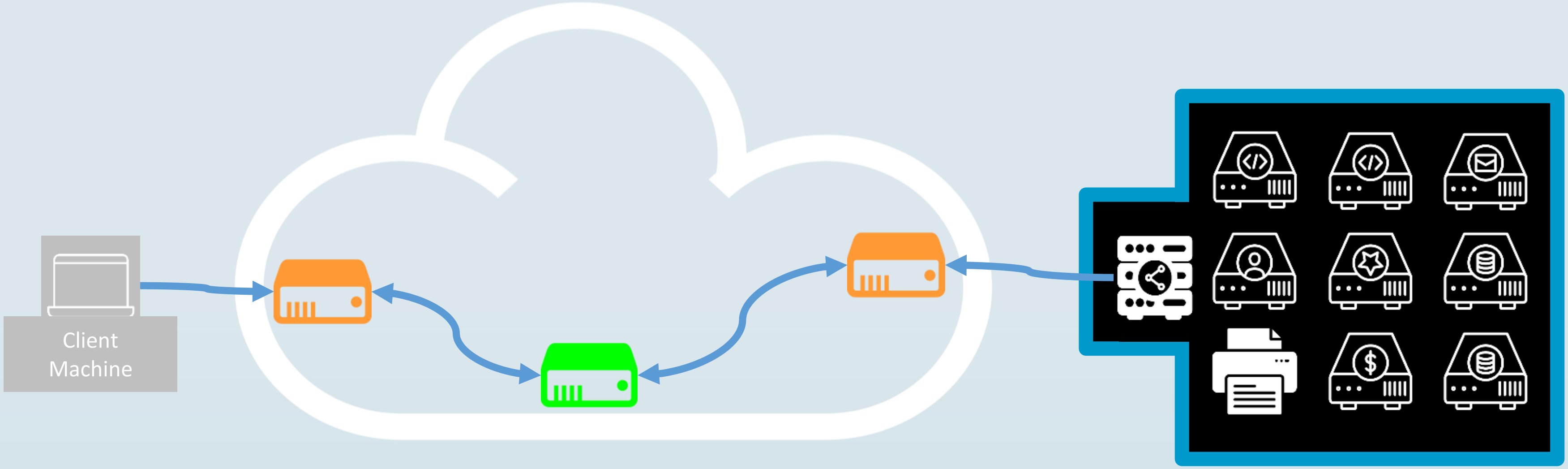
Identity Aware Proxy (IAP)



User	Role(s)
bob	dev,boston
joe	sales,london

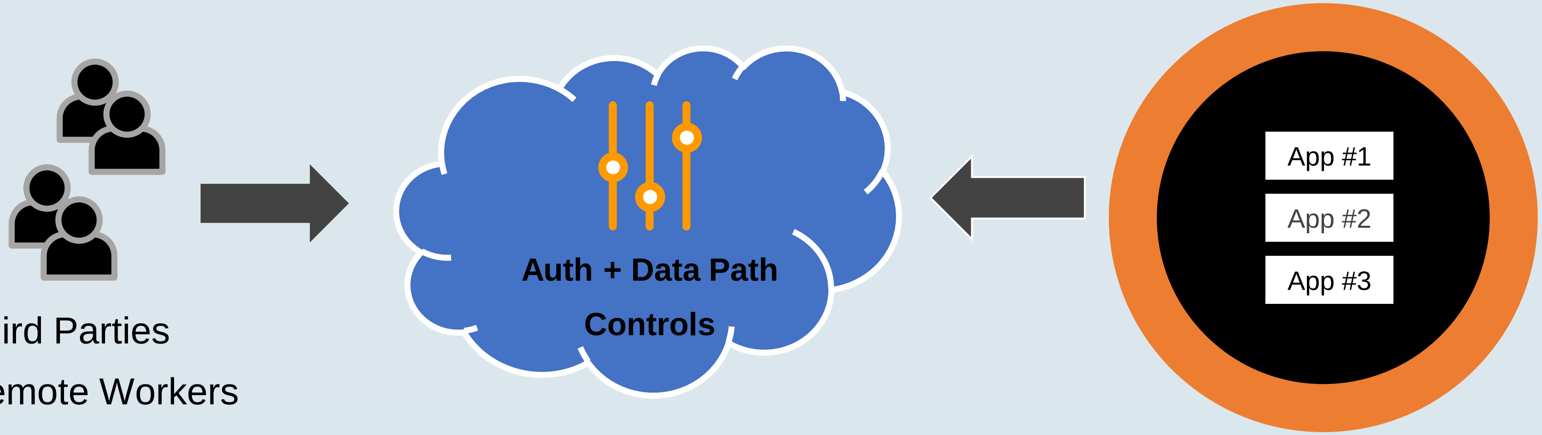
Machine	Data
123	Current OS With Patches
123	Updated endpoint protection
123	Score: 85

Identity Aware Proxy (IAP)



Injecting WAF, DLP,
or other content aware
Filtering, Authentication + 2FA, etc.

Benefits



Auth + Data Path Controls

App #1

App #2

App #3

Third Parties

Remote Workers

Remote sites

No network connectivity - Least privilege per app

No company owned devices to third parties

No security appliance stack in cloud infrastructure

The Internet as Corporate Network

No Inside

No VPN

No Passwords

Every app seems like SaaS

Every office is a hotspot

Summary

- Zero Trust is a journey.
- Managed services and partnerships will be key.
- Your partners, plans, and integrators must be able to *phase* this in.
- Mixing of strategies can have value. For example, Micro-Segmentation *within* an Identity aware Proxy approach (IAP). These Micro-Perimeter can prevent lateral movement.

ISSA

Information Systems Security Association International

www.issa.org

QUESTIONS?