CYBERSEC 2021
臺灣資安大會

ORGANIZED BY iThome

資訊架構的零信任革命

MAY 4-6 臺北南港展覽二館

$ ls

1. **What Zero Trust?**

2. Why Zero Trust?

3. How Zero Trust?

4. Why not Zero Trust?

TRUST:redefined

信任重構

What is TRUST?

Q1: 我是金城武，這是我的名片，你信任我嗎?

A1: 我是誰? 是誰說我是誰?
要看雙證件才(就)可信嗎?

[驗證身分]

What is TRUST?

Q2: (公司內)可以幫我開一下門嗎?

A2: 大門警衛放進來的，
邊界內就是安全的?
業務部找的廠商可以進機房?

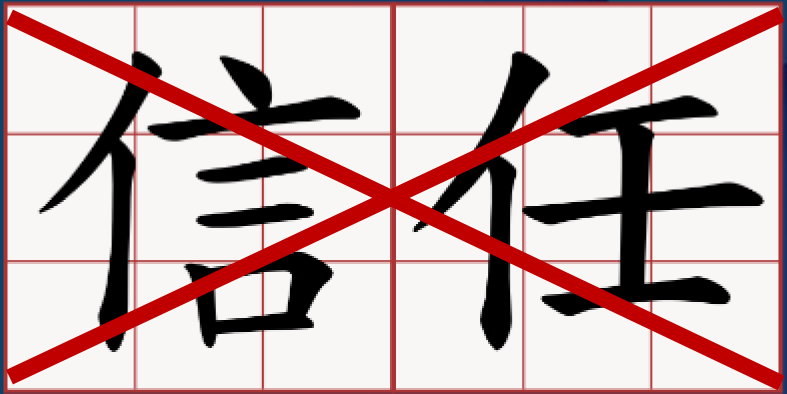
[網段區隔]

What is TRUST?

Q3: (在大街上)免費發放試用產品!

A3: (釣魚信件)請開啟這個附件

[不預設信任，時時驗證]



What is ZERO TRUST?

~~Trust, but Verify.~~...

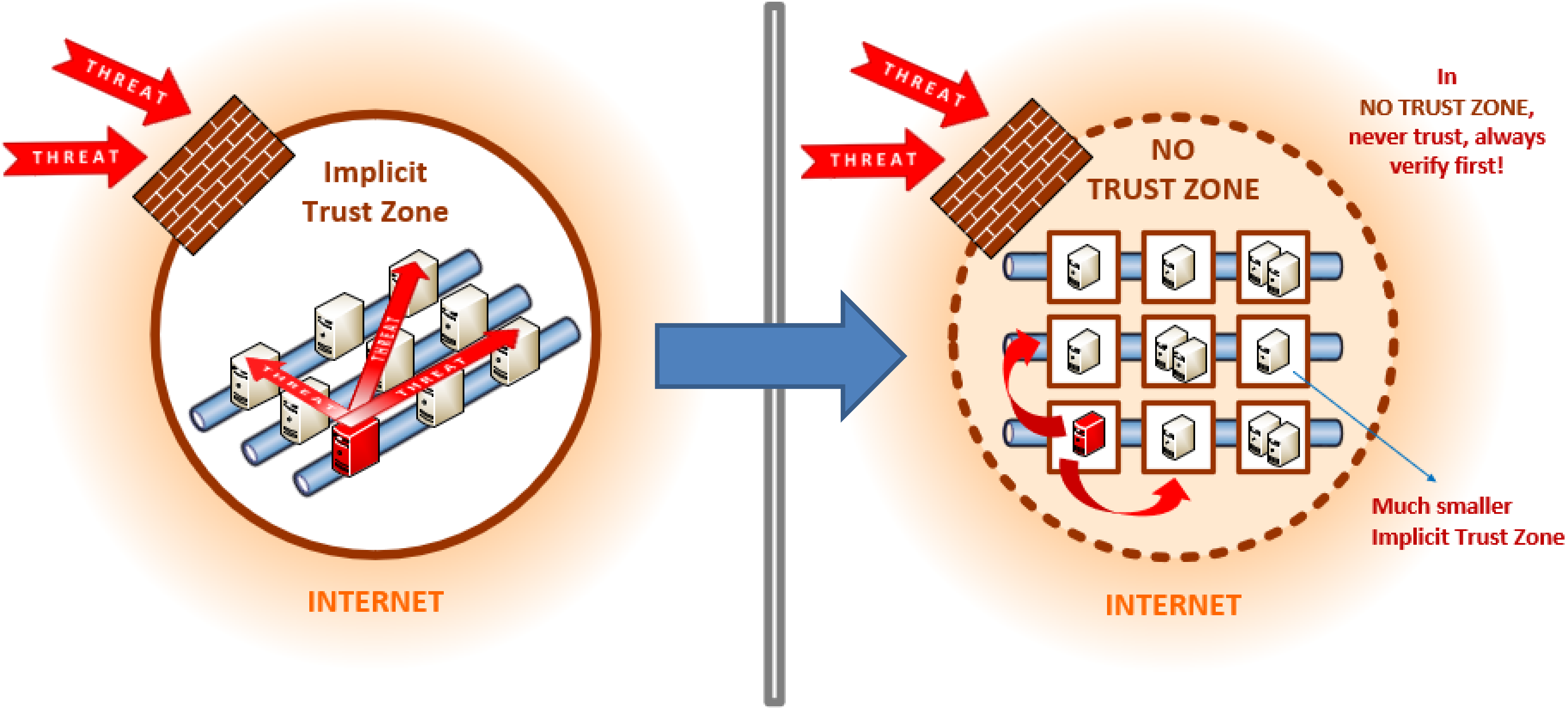
Never Trust, Always Verify!

Definition:

“Zero trust is a cybersecurity paradigm focused on resource protection and the premise that trust is never granted implicitly but must be continually evaluated. “

Traditional Single Perimeter Defense

Zero Trust Defense Focuses on Resource Protection



In NO TRUST ZONE, never trust, always verify first!

Much smaller Implicit Trust Zone

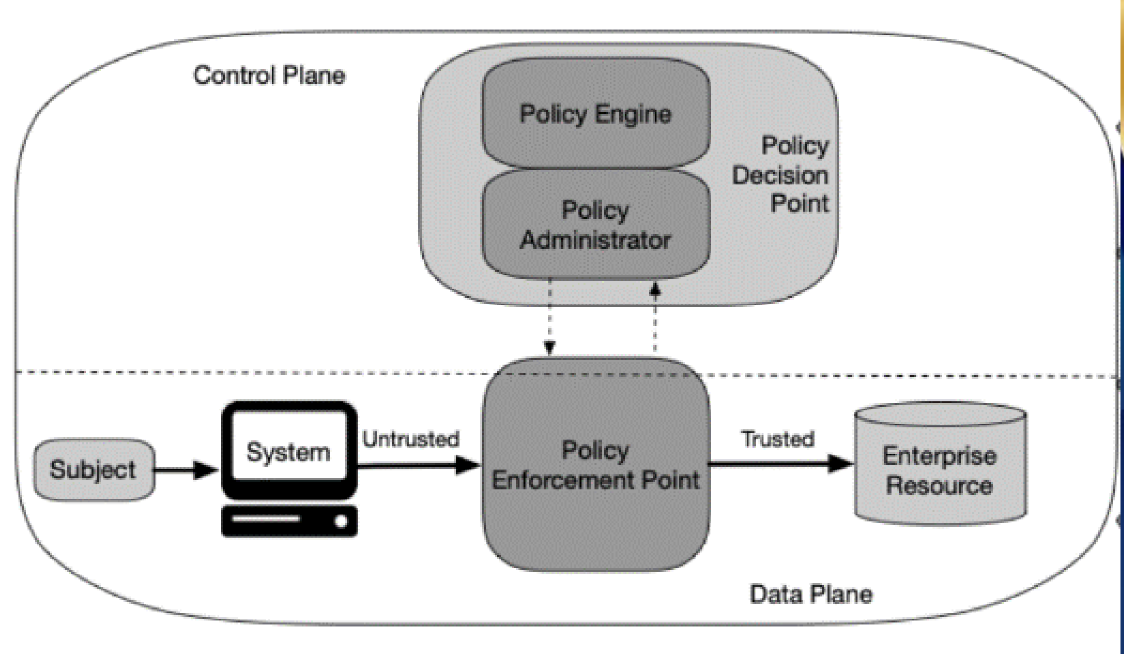
https://www.nist.gov/blogs/taking-measure/zero-trust-cybersecurity-never-trust-always-verify

Zero Trust Components

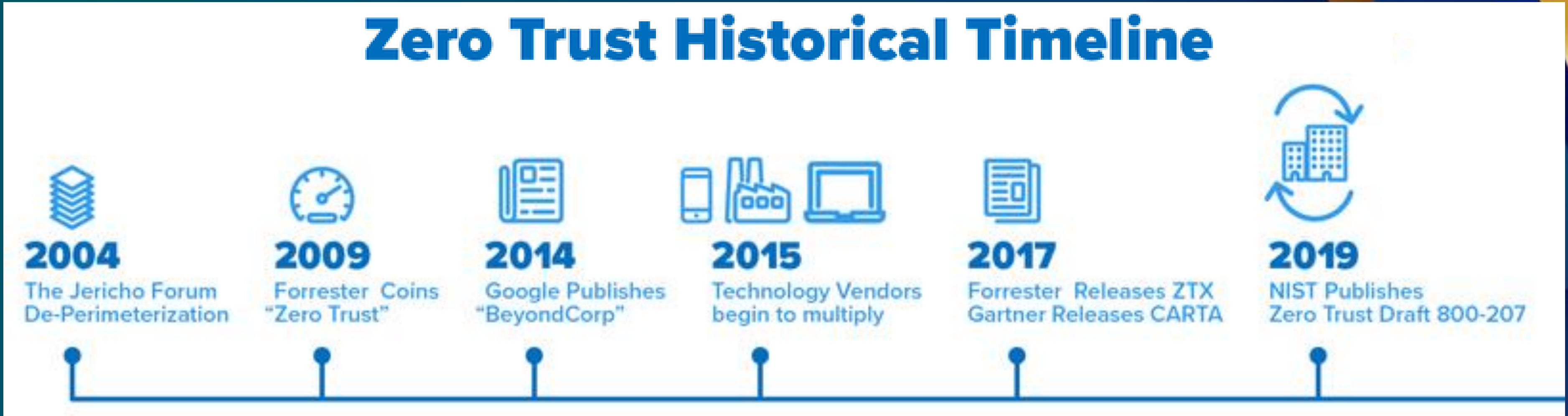
PE: decision to grant access

PA: establish access

PEP: enable, monitor and terminate connections



Zero Trust is New!



Zero Trust Historical Timeline

2004
The Jericho Forum
De-Perimeterization

2009
Forrester Coins
"Zero Trust"

2014
Google Publishes
"BeyondCorp"

2015
Technology Vendors
begin to multiply

2017
Forrester Releases ZTX
Gartner Releases CARTA

2019
NIST Publishes
Zero Trust Draft 800-207

https://www.wwt.com/article/what-is-zero-trust

$ ls

1. What Zero Trust?

2. **Why Zero Trust?**

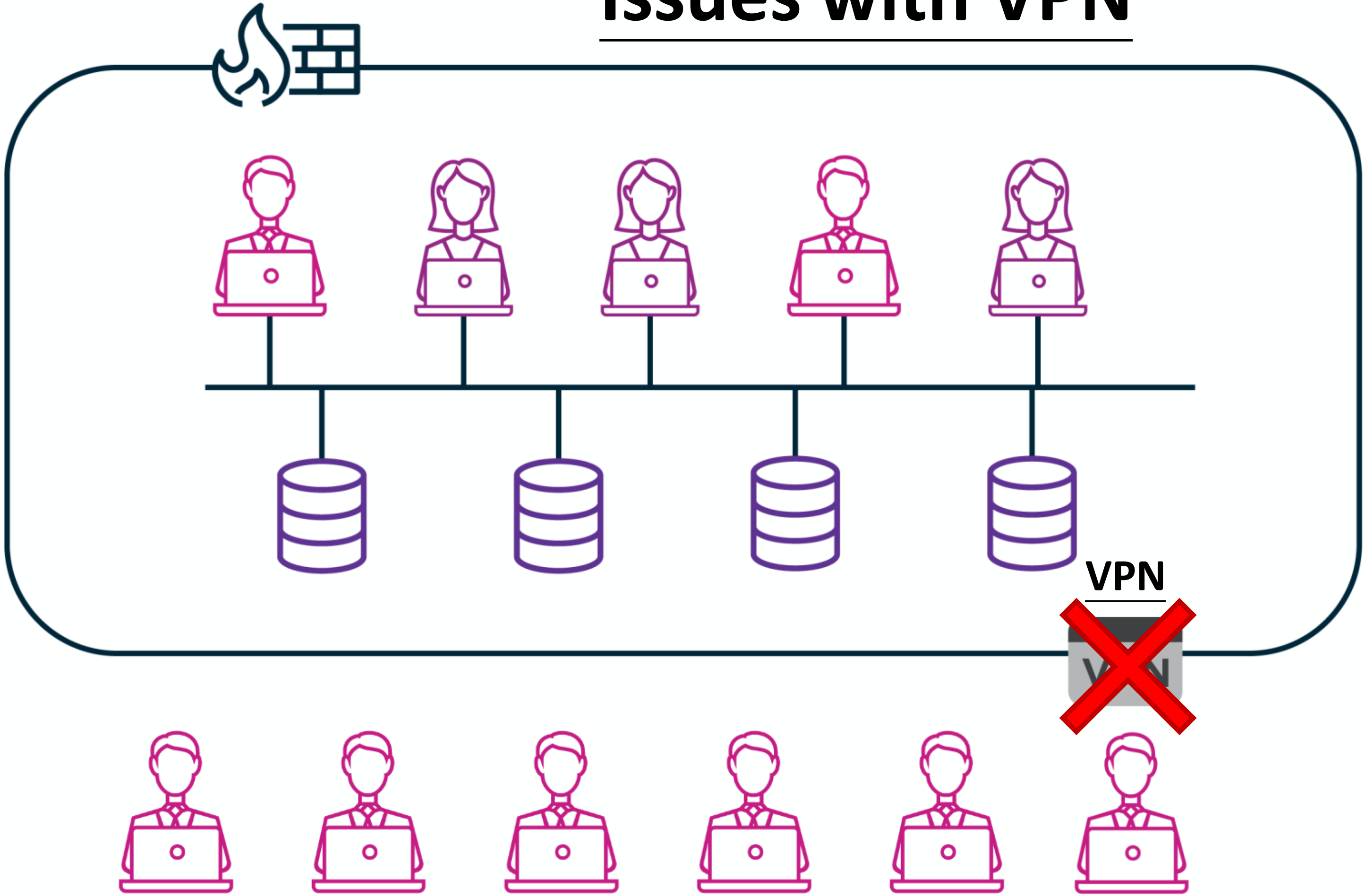
3. How Zero Trust?

4. Why not Zero Trust?

Work From Home under COVID-19

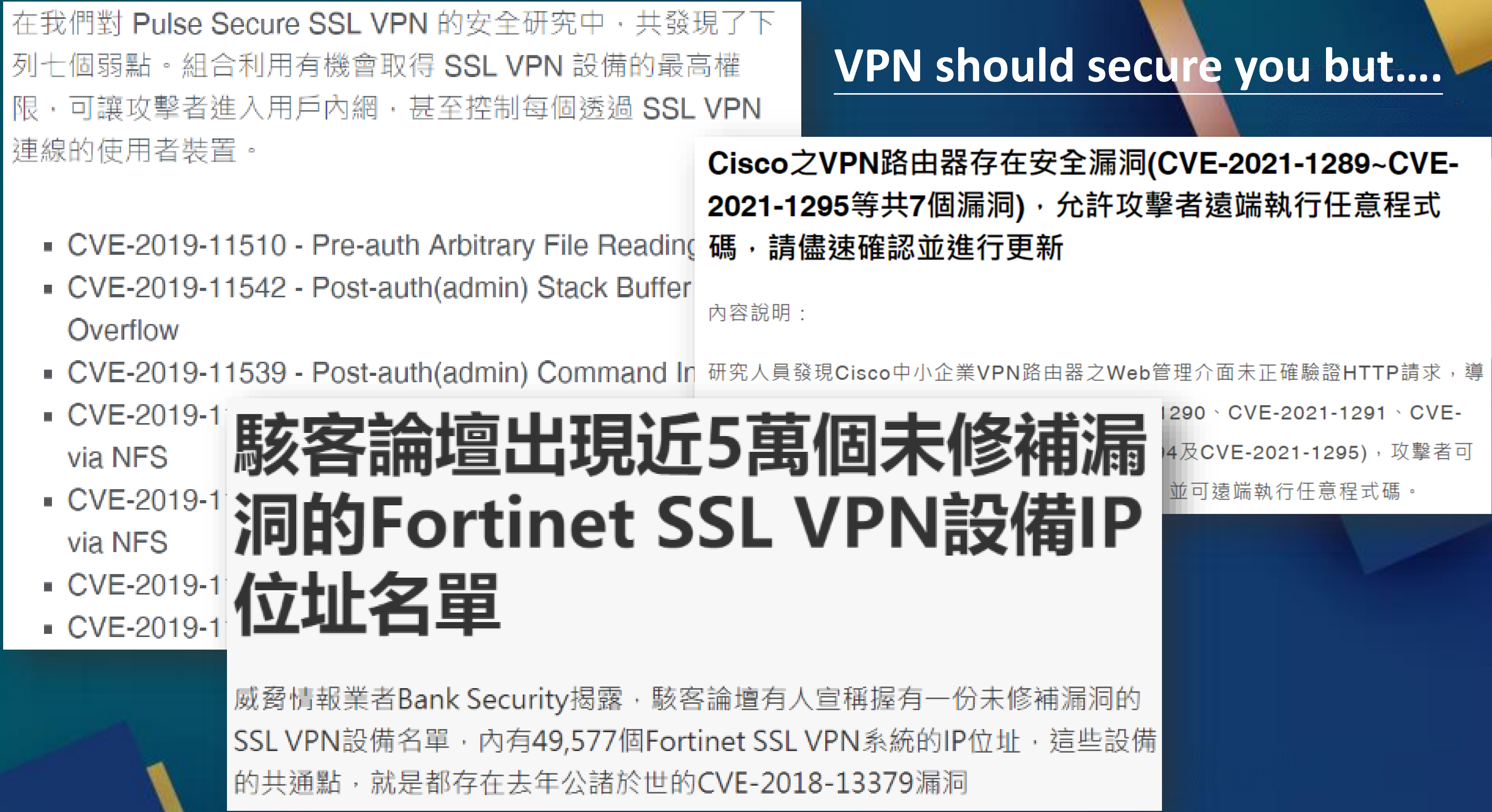
https://www.sourcingspeak.com/security-risk-work-from-home-wfh-covid-19/

Issues with VPN



https://www.appgate.com/blog/what-is-a-software-defined-perimeter

VPN should secure you but....



在我們對 Pulse Secure SSL VPN 的安全研究中，共發現了下列七個弱點。組合利用有機會取得 SSL VPN 設備的最高權限，可讓攻擊者進入用戶內網，甚至控制每個透過 SSL VPN 連線的使用者裝置。

- CVE-2019-11510 - Pre-auth Arbitrary File Reading
- CVE-2019-11542 - Post-auth(admin) Stack Buffer Overflow
- CVE-2019-11539 - Post-auth(admin) Command In
- CVE-2019-1
  via NFS
- CVE-2019-1
  via NFS
- CVE-2019-1
- CVE-2019-1

Cisco之VPN路由器存在安全漏洞(CVE-2021-1289~CVE-2021-1295等共7個漏洞)，允許攻擊者遠端執行任意程式碼，請儘速確認並進行更新

內容說明：

研究人員發現Cisco中小企業VPN路由器之Web管理介面未正確驗證HTTP請求，導

1290、CVE-2021-1291、CVE-

4及CVE-2021-1295)，攻擊者可

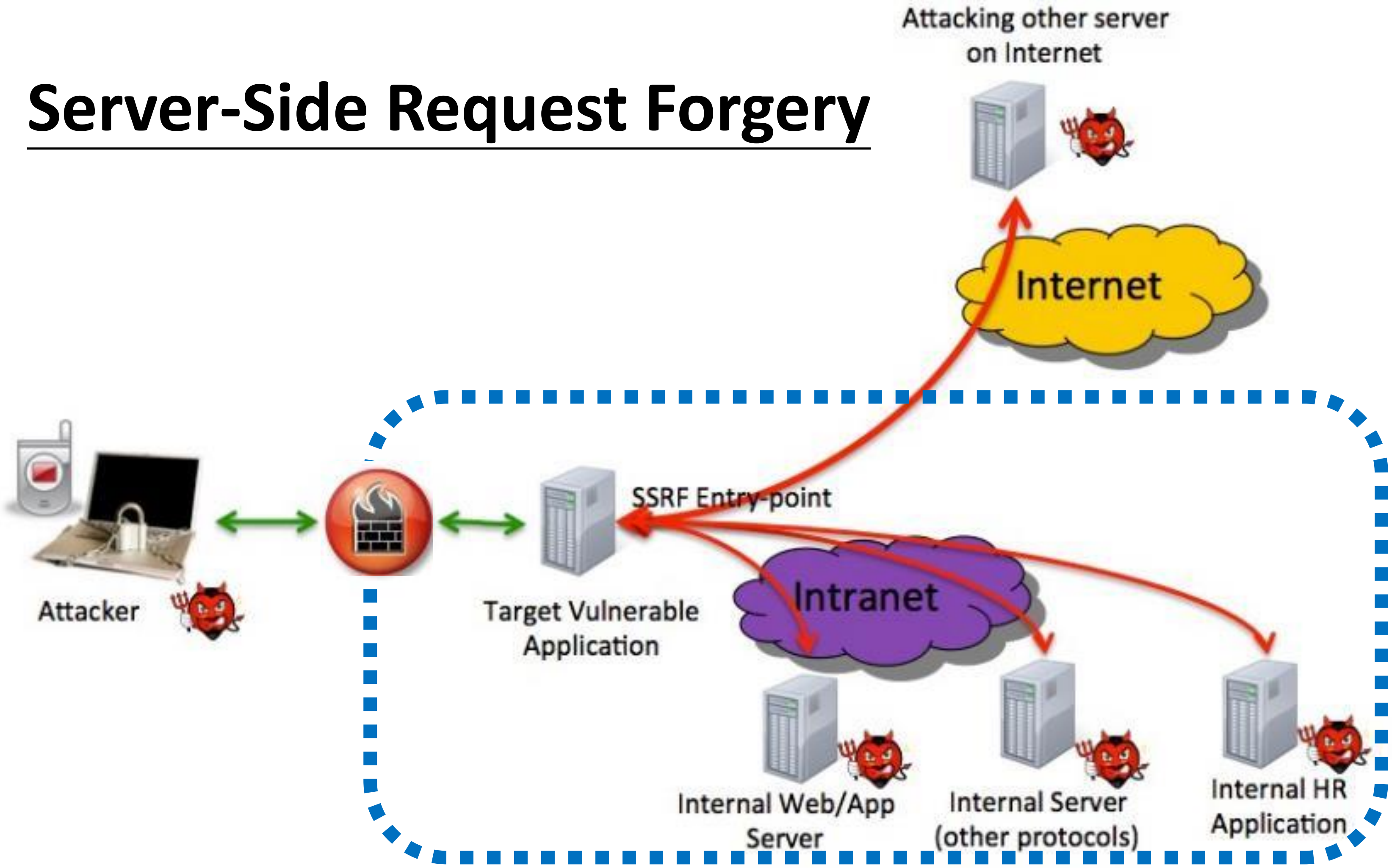
並可遠端執行任意程式碼。

駭客論壇出現近5萬個未修補漏洞的Fortinet SSL VPN設備IP位址名單

威脅情報業者Bank Security揭露，駭客論壇有人宣稱握有一份未修補漏洞的SSL VPN設備名單，內有49,577個Fortinet SSL VPN系統的IP位址，這些設備的共通點，就是都存在去年公諸於世的CVE-2018-13379漏洞

Perimeter Defense Fails

Server-Side Request Forgery


Attacking other server on Internet
Internet
Attacker
SSRF Entry-point
Target Vulnerable Application
Intranet
Internal Web/App Server
Internal Server (other protocols)
Internal HR Application

http://blog.blueinfy.com/2017/12/server-side-request-forgery-ssrf-attack.html

$ ls

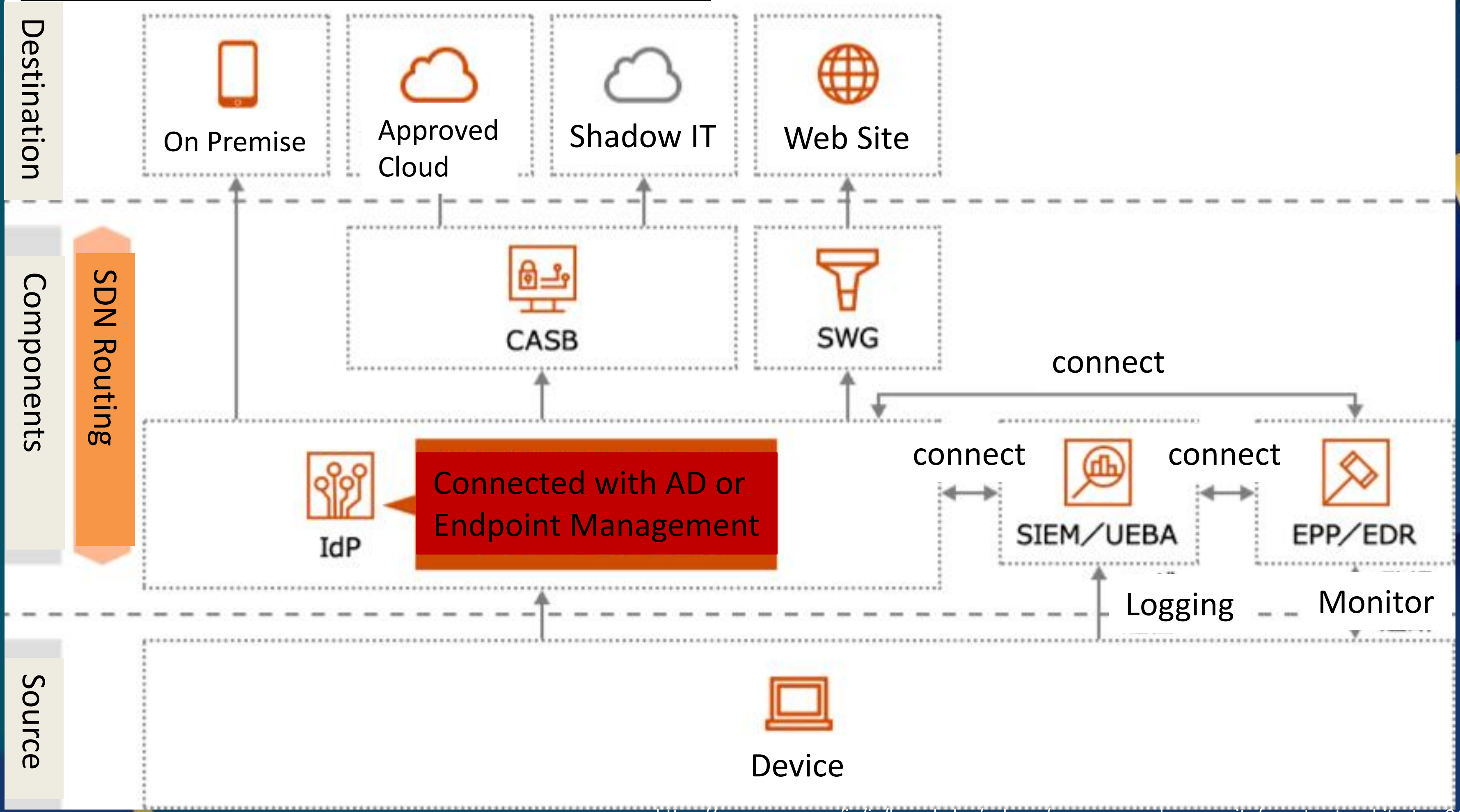
1. What Zero Trust?

2. Why Zero Trust?

3. How Zero Trust?

4. Why not Zero Trust?

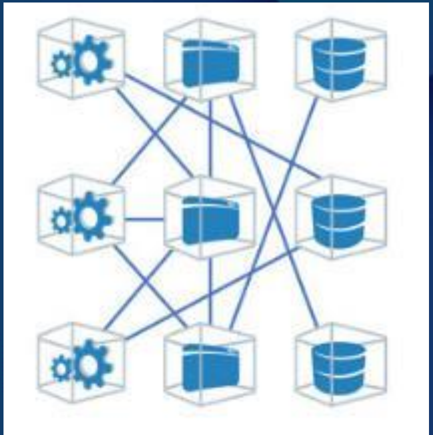
Zero Trust Architecture Implementation Sample



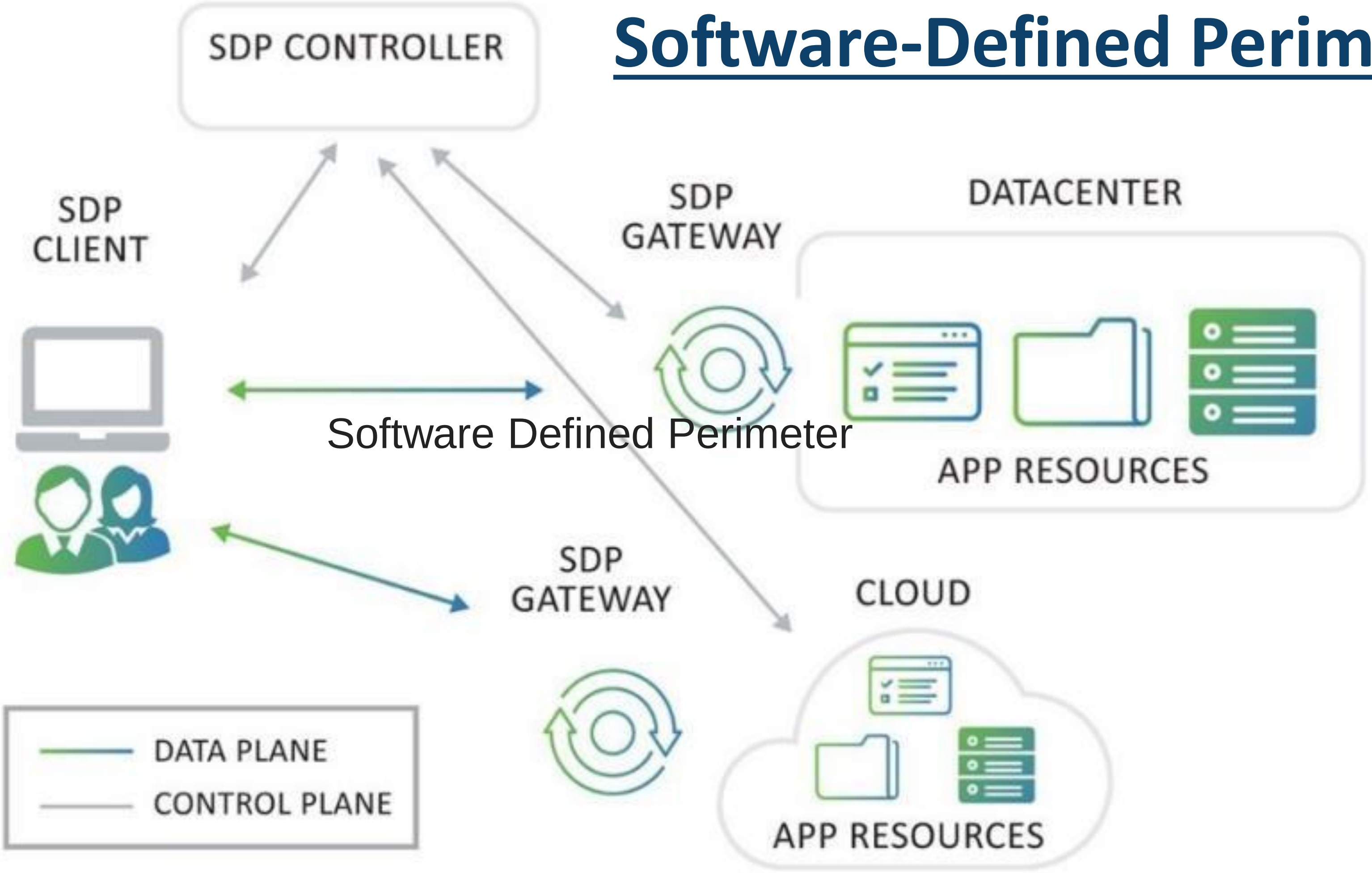
https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/zero-trust-architecture04.html

3 Main Technologies for Zero Trust

- Software-Defined Perimeter (SDP)
- Identity and Access Management (IAM)
- Micro-Segmentation (MSG)



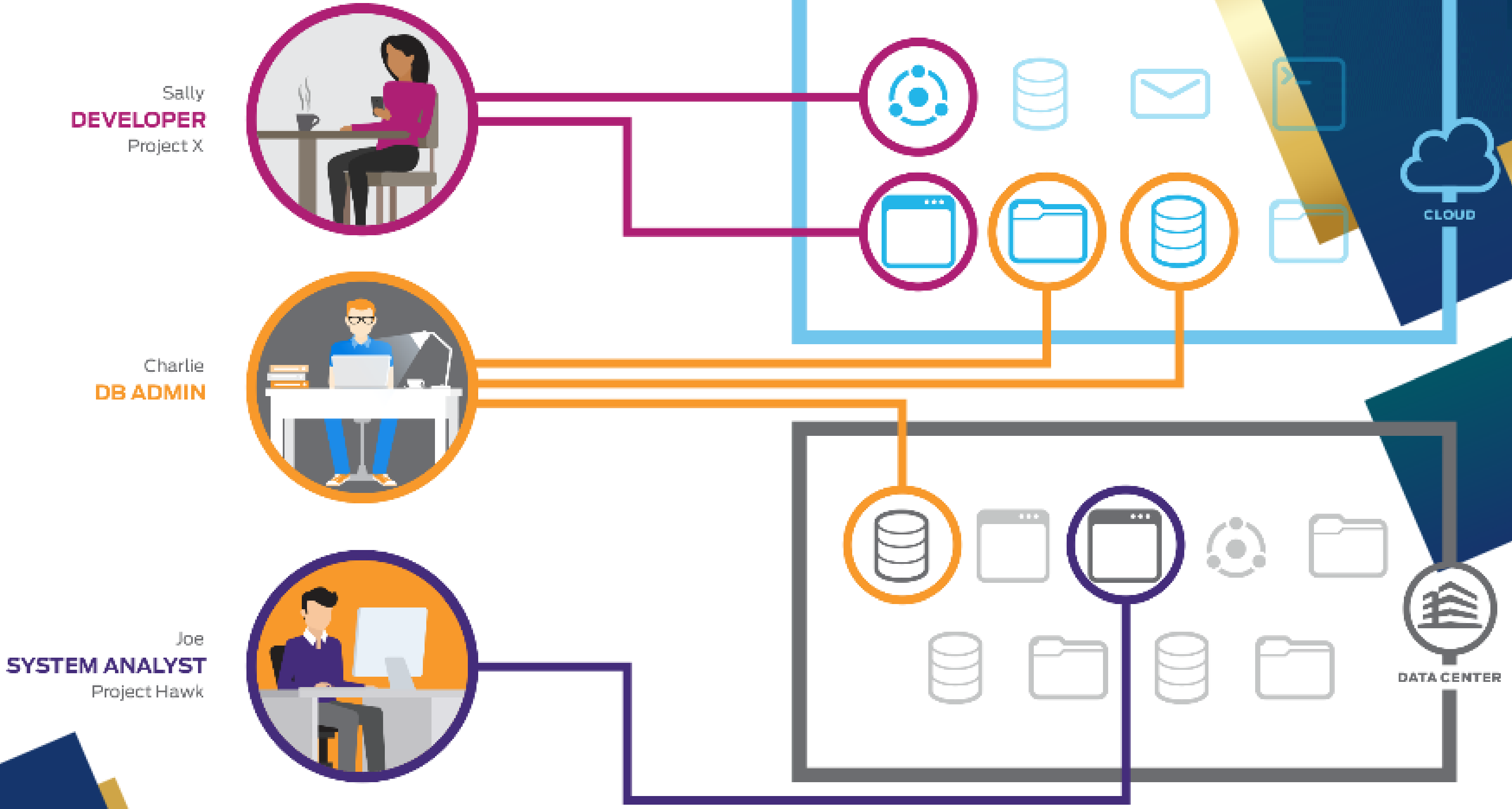
Software-Defined Perimeter



Software Defined Perimeter

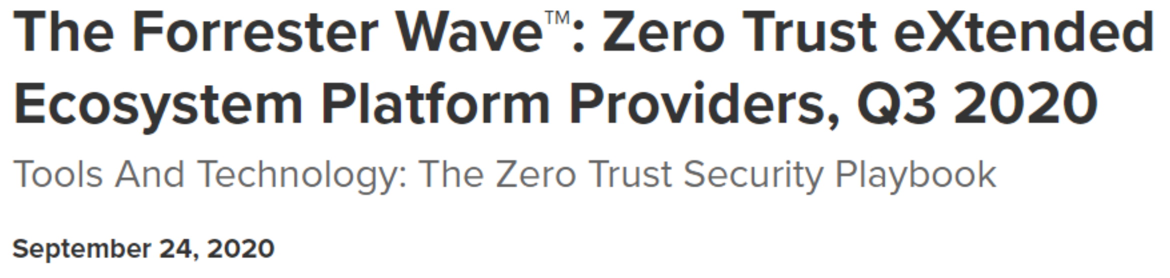
https://www.appgate.com/blog/what-is-a-software-defined-perimeter

Software-Defined Perimeter



https://www.appgate.com/blog/what-is-a-software-defined-perimeter

How to Zero Trust?

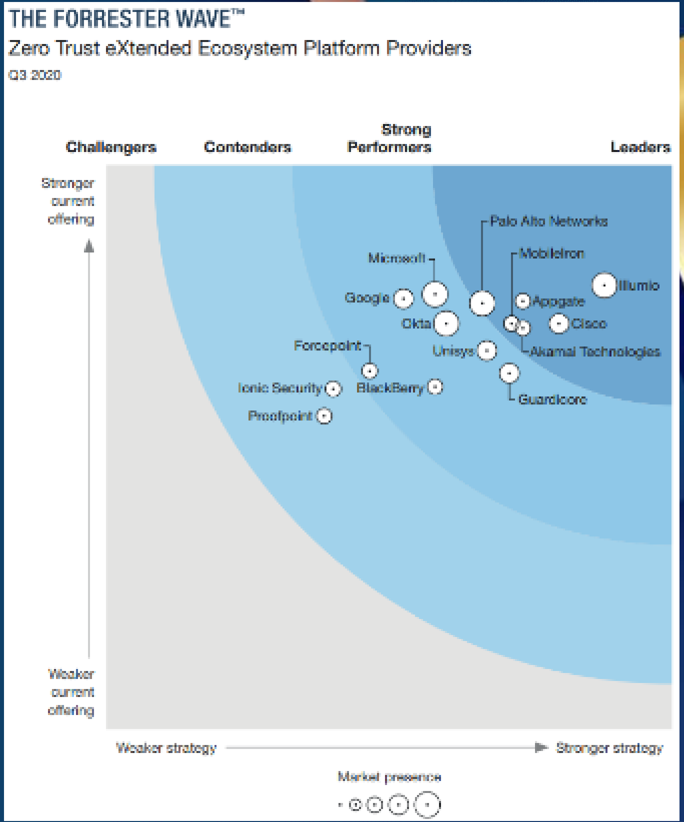


The Forrester Wave™: Zero Trust eXtended Ecosystem Platform Providers, Q3 2020

Tools And Technology: The Zero Trust Security Playbook

September 24, 2020

Akamai, Appgate, BlackBerry, Cisco, Forcepoint, Google, Guardicore, Illumio, Ionic Security, Microsoft, MobileIron, Okta, Palo Alto, Proofpoint, and Unisys

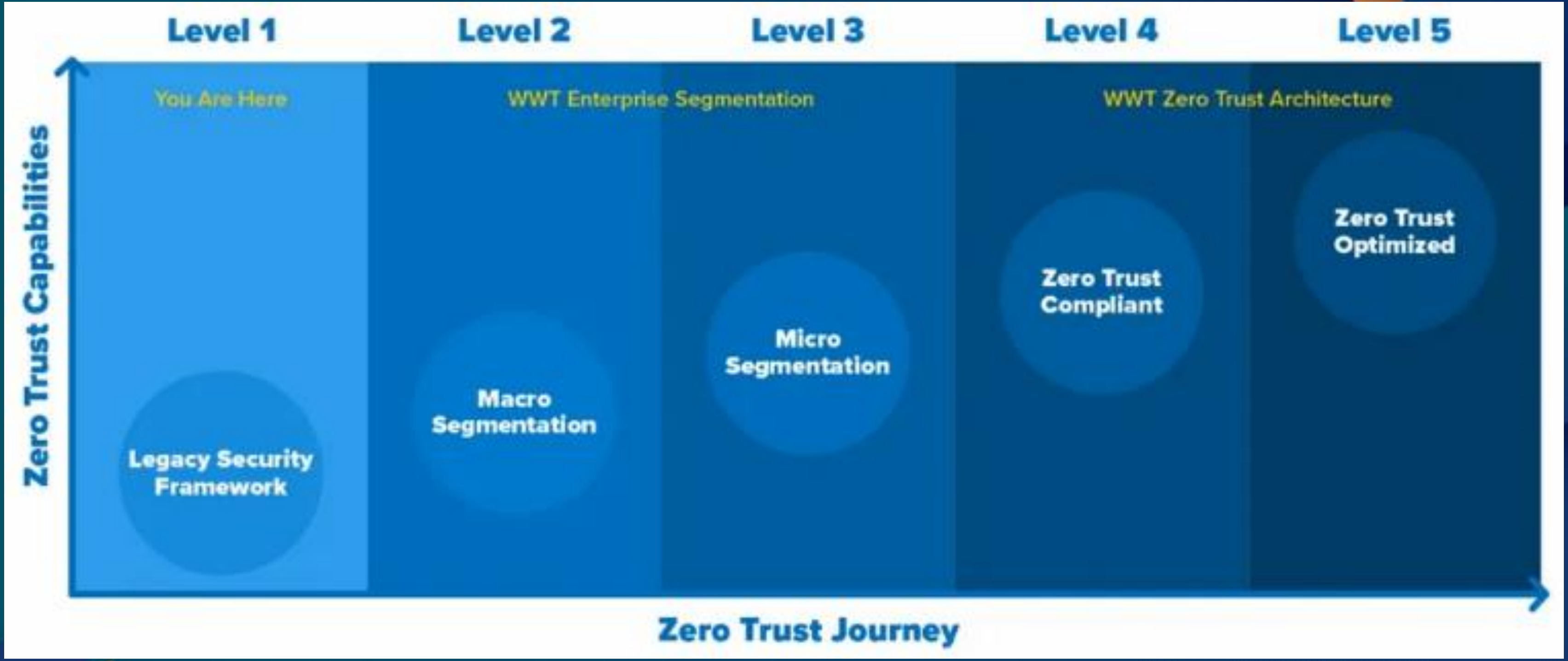

THE FORRESTER WAVE™

Zero Trust eXtended Ecosystem Platform Providers

Q3 2020

https://www.forrester.com/report/The+Forrester+Wave+Zero+Trust+eXtended+Ecosystem+Platform+Providers+Q3+2020/-/E-RES157494

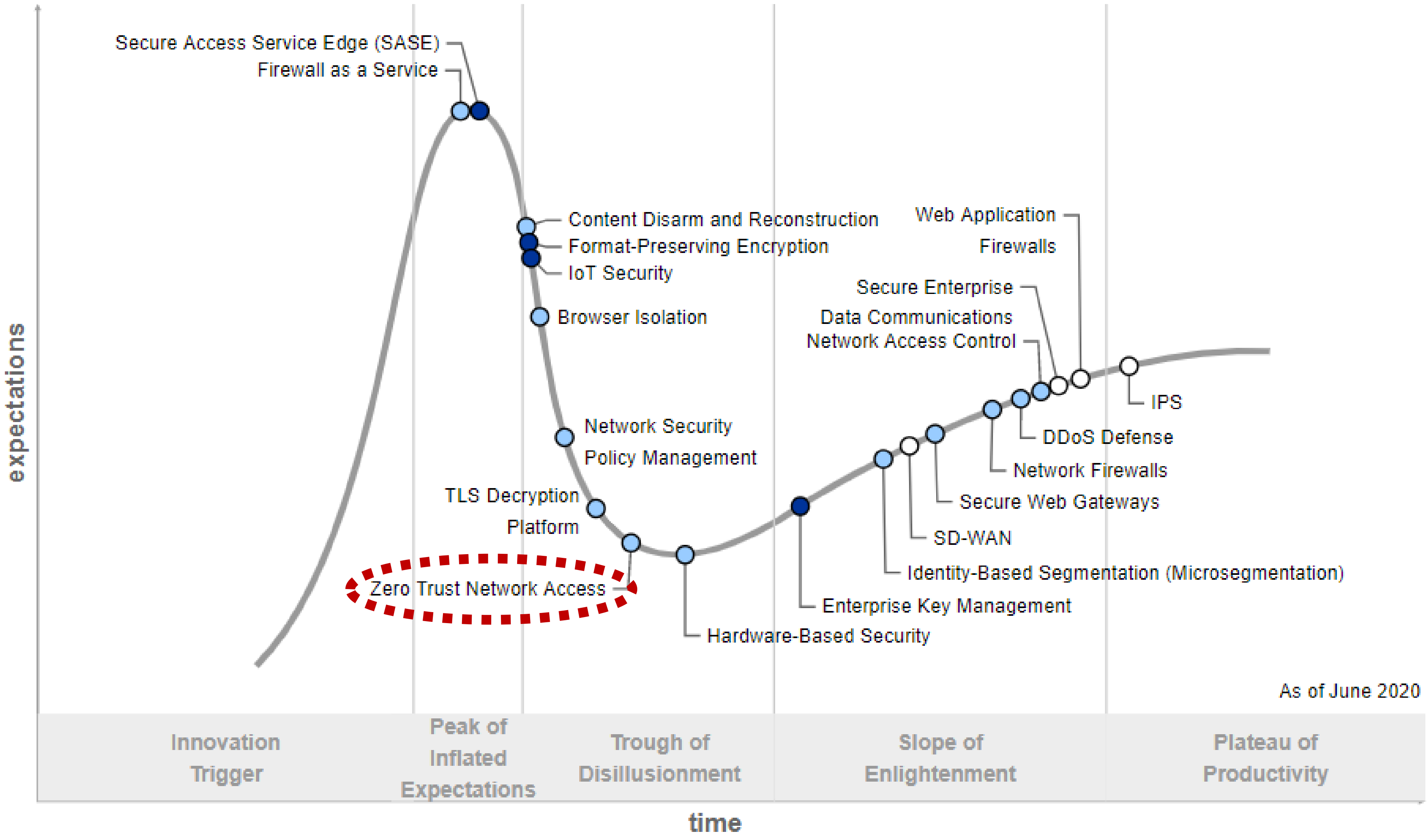
Zero Trust Step by Step



https://www.wwt.com/article/what-is-zero-trust

$ ls

1. What Zero Trust?
2. Why Zero Trust?
3. How Zero Trust?
4. Why not Zero Trust?



As of June 2020

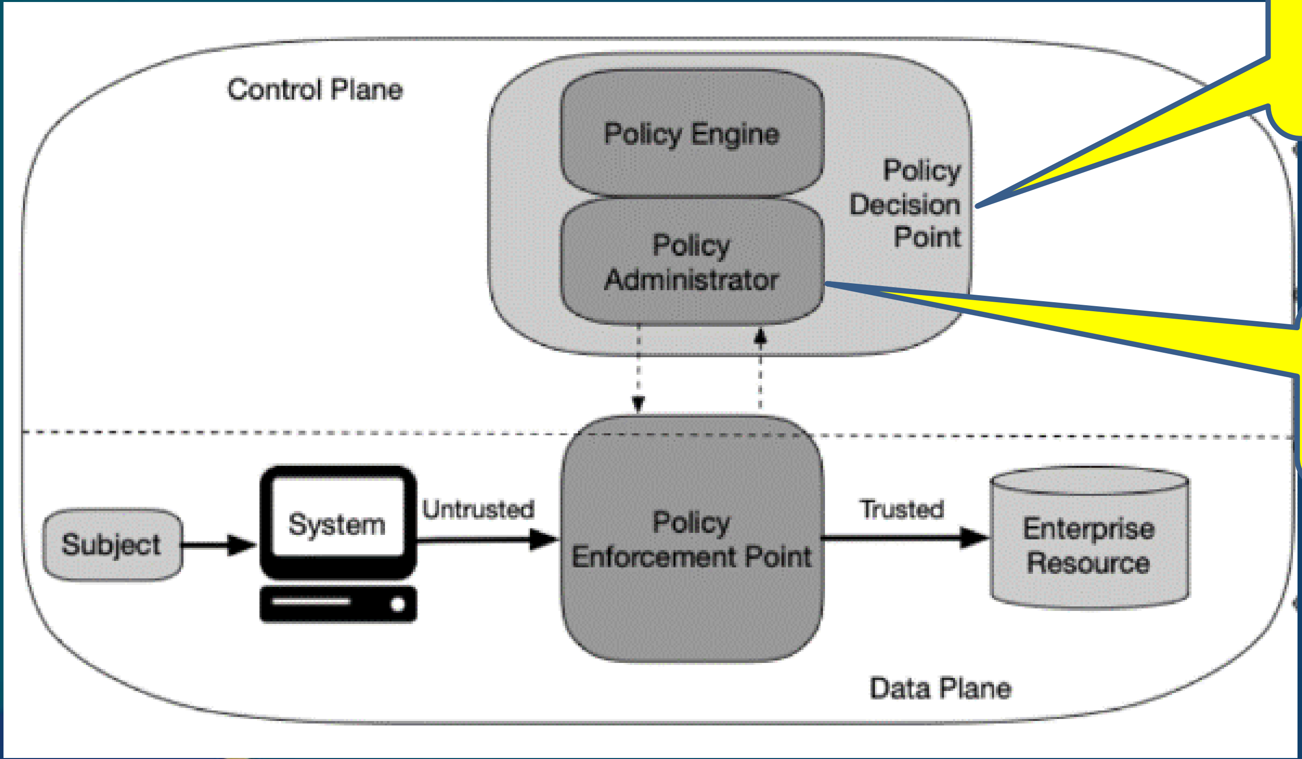
Issues on Zero Trust (1/2)

Legacy Systems

Lack of Regulation

Network Visibility

Issues on Zero Trust (2/2)



Single Point of Failure

Vulnerable to DoS Attack

Takeaways

1. Zero Trust is going to mature in 2-5 yrs
2. COVID-19, Remote Work, Cloud are pushing
3. Not easy to shift thoroughly at once
4. Can enhance components step by step

Thank you!