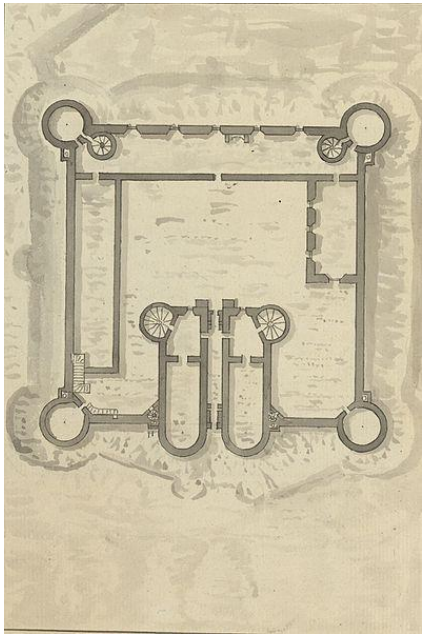
Security Architecture in the Age of Covid

March 22, 2023

Traditional Security Architectures



Traditional network security follow a **“moat and castle”** model, consisting of gateway devices at the perimeter, creating “a sort of crunchy shell around a soft, chewy center.”[1]

This model was flawed almost from the beginning, but became increasingly problematic as more and more “holes” were necessary in the firewall to allow business to function.

Firewall segmentation is still important, but the traditional model is no longer valid.

1- Bill Cheswick, https://cheswick.com/ches/papers/gateway.pdf

Problems

- Focus on perimeter & prevention was too often at the exclusion of other detective & reactive controls (“We have firewalls!”)
  - “Trusted” network contain malicious insiders and systems that have already been compromised
    - Unencrypted data in transit was a problem & a blessing, as we’ll see later.
  - The need for connection to the internet via email (and eventually web) meant that attackers already had routes through the castle walls
  - Unpatched security vulnerabilities, flat networks and implicit trust of internal systems provides the attacker an open field once they’ve breached the gates
    - Remember when we were afraid to patch?
      - **NT4 SP4 forever!**

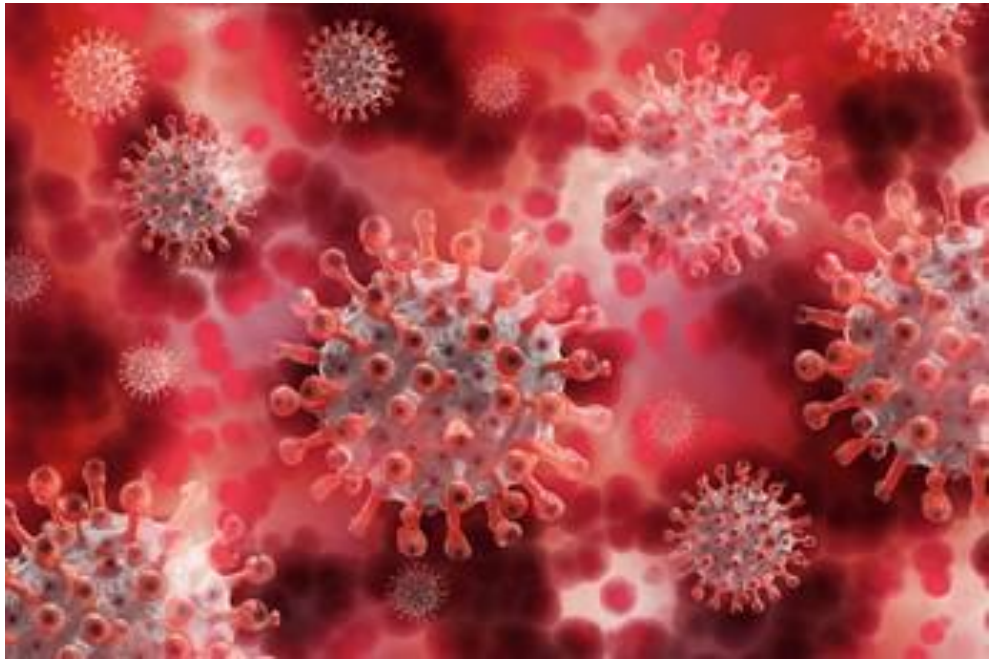
Problems (continued)

- Cloud implementations and cloud services (IaaS, PaaS, SaaS) mean that your enterprise data is no longer inside your perimeter
  - An attacker can compromise your data in the cloud and exfiltrate it without ever touching your perimeter. If your detection controls are all inside the firewall, you may never know its happening.
  - If someone in your company has a corporate credit card, they can stand up a cloud. You may not know about it until your compromised (or they need to open firewall rules)
    - They may not know it's cloud
    - Services exist to help find these
- Internet of Things
  - Devices within your network, needing network access, needing internet access that never did before, often with poor security configurations by default.
  - Business units not used to reaching out to IT need to have Security teams involved. However you may not find out until they try to attach them to the network.

And then one more Problem

December 31, 2019

The World Health Organization (WHO) Country Office in China is informed of several cases of a pneumonia of unknown etiology (cause) with symptoms including shortness of breath and fever occurring in Wuhan, China. All initial cases seem connected to the Huanan Seafood Wholesale Market.



https://www.cdc.gov/museum/timeline/covid19.html#:~:text=December%2031%2C%202019,fever%20occurring%20in%20Wuhan%2C%20China

Covid Response

- Employees who didn’t absolutely have to work in the office started working from home
- Meetings, conferences & in-person training was changed to online only, or were simply canceled
- IT infrastructure that was designed to support a fraction of employees working from home suddenly had to support the majority of, or all employees working remotely.

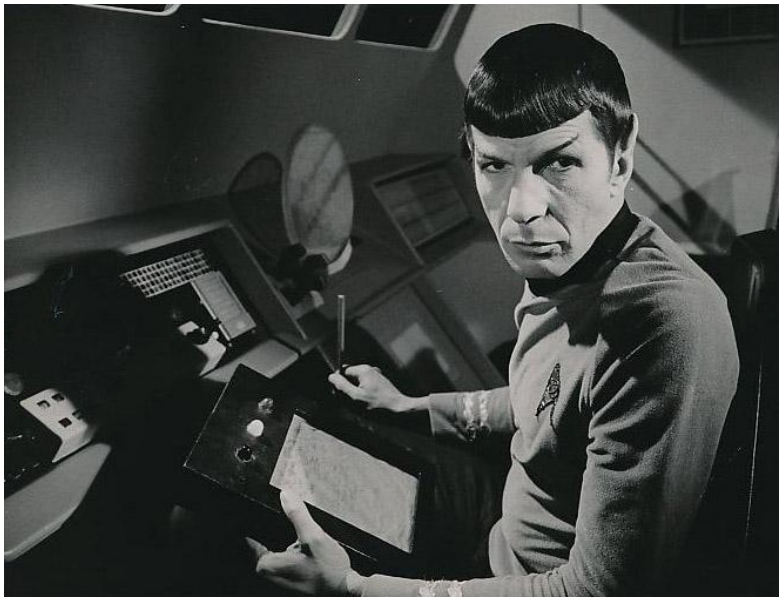
Cut to today, attempts to bring employees back to the office and go back to status quo ante have largely failed. **At a previous employer, when employees were polled regarding their opinion as to what they’d do if they had to go back to the office, more than half responded that they’d start looking for another job.**

Time Based Security

P(t)>D(t)+R(t)

- **P(t)** - the time it takes for an attacker to overcome prevention controls.
- **D(t)** - the time it takes for a defenders detection controls and processes to detect the attack.
- **R(t)** - the time it takes for a defenders response/reaction controls and process to take effect.

But how do you determine P(t)?



- Hard to quantify. Attackers don't make it easy!
- Zero days, Nation States will always be an issue depending on your industry
    - Remember you may just be a vector to attack someone else
- Practically speaking, Purple team exercises (not Red team penetration testing) are a good way to determine P(t).
- Crowdstrike recommends following the 1-10-60 rule, one minute to detect, investigate within 10 minutes and isolate/remediation within 60[1]
  More on this later!

1-https://www.crowdstrike.com/cybersecurity-101/lateral-movement/#:~:text=Top%20private%2Dsector%20companies%20strive,the%20problem%20within%2060%20minutes

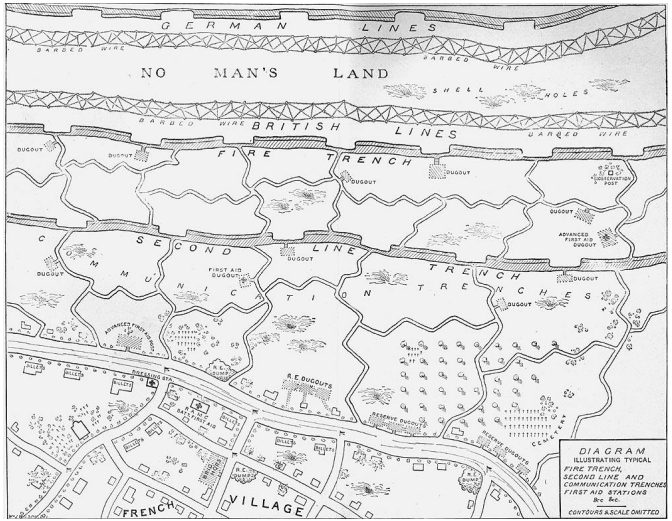
P(t): Temet Nosce

- Know Thyself[1], temet nosce is the Latin, gnothi seauton in Greek. Plato writes that Socrates attributed this saying to one of the Seven Sages of Greece. However it has been attributed to various philosophers throughout history.
- Be able to take and maintain an accurate inventory of systems on your network.
- Endpoint Detection & Response agents can be very helpful with this.
- If you don't have a commercial product open source tools such as OSQuery can be used.
- Inventory your network and segregate based on criticality. See what compliance requirements you have (HIPAA, PCI, etc.) as you've probably already done some of this.

1- https://en.wikipedia.org/wiki/Know_thyself

2- Image by Clemens Schmillen - Derived from this file:, CC BY-SA 4. https://commons.wikimedia.org/w/index.php?curid=68429623

P(t): Segmentation & Tiered Networks



- Defense in depth rather than castle walls.
  - Moats and walls are still useful if they delay & frustrate the attacker.
  - Think tiered security rather than perimeter.
  - Bring firewalls inside and know where your critical systems are (Temet Nosce).
- Private VLANS can frustrate lateral movement.
  - The wired equivalent to wireless station isolation.
  - Complicates lateral movement for the attacker.
- Proxies
  - A system that brokers traffic between two systems. **More on this later.**
- Network Access Control
  - You will still have on-premise resources.

P(t): Remote Users

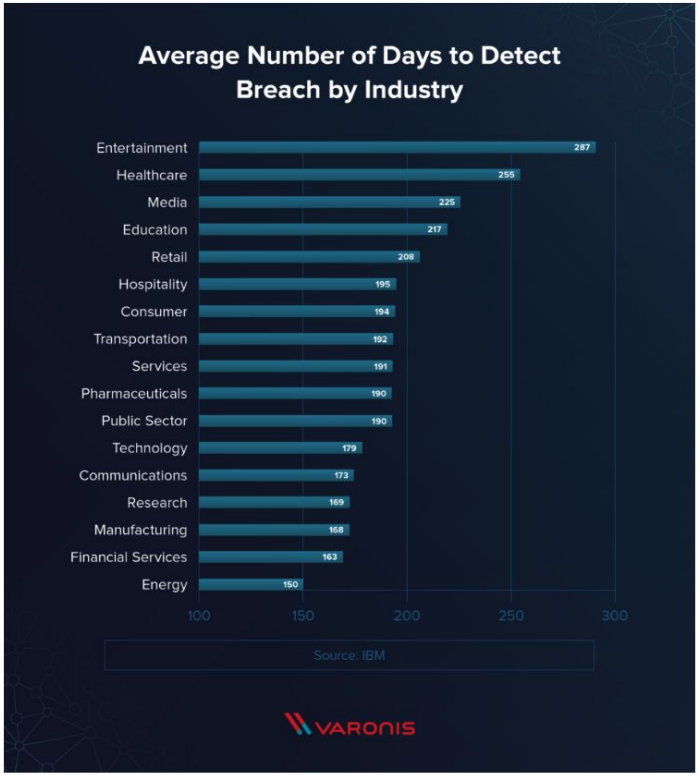
- Multi-factor Authentication! You need to have it in place and it needs to be pervasive.
  - There are no trusted networks
- Try to bring your resources back inside:
  - Consider implementing a Secure Access Service Edge (SASE) Solution
  - Consider implementing a virtual desktop solution
    - Azure Virtual Desktop, AWS Workspaces, Citrix still out there?
- Step up your VPN
  - It can do more than just authenticate and encrypt traffic.
- Local Firewall
  - For prevention but for detection later as well

P(t): Cloud Security

- Your cloud solutions have native security controls, learn and leverage them
  - AWS has gotten a lot better in the past five years.
- Microsoft is spending $B's on Cybersecurity & has build & purchased some impressive security controls
  - As of last year some of these tools didn't play well with each other & Microsoft keeps renaming things!
- Consider a Cloud Access Security Broker
  - This can be complicated, historically large public Cloud Service Providers (CSP's) didn't play well together or with CASB's
  - Some CSP's have their own CASB solutions, see previous bullet
- Implement MFA! Worth mentioning again, particularly for accessing cloud services (this means email and cloud storage as well)
  - Otherwise only a single password is between your company and data being exfiltrated from email and cloud storage

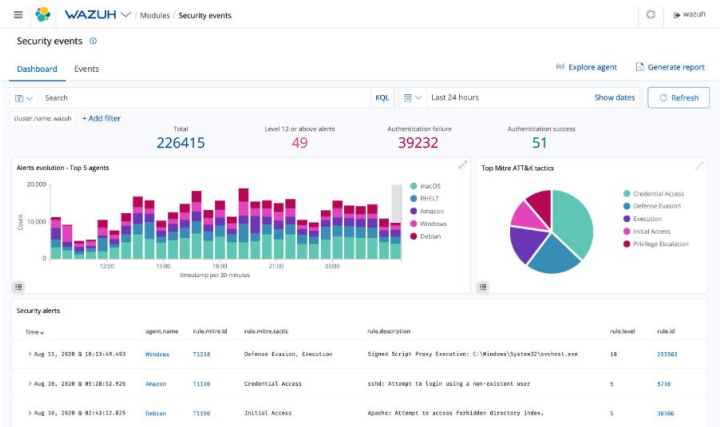
D(t): Time required to Detect

- Crowdstrike recommends the 1-10-60 rule.
- According to Varonis it takes on average 150 to 287 days to detect a breach, depending on the industry.
- **So there is a bit of a disconnect.**
- Why?
  - False negatives
  - Alert fatigue
  - Lack of a mature security organization
  - **Blind spots in detection**



https://www.varonis.com/blog/data-breach-response-times#:~:text=On%20average%2C%20companies%20take%20about,a%20breach%20according%20to%20IBM

Detection: On-Prem Security



- **Yes, your usual controls are important**
  - Network Intrusion Detection
    - Snort & Suricata
  - Network Security Monitoring
    - Network Metadata, SFlow
  - NGFWs
    - SSL Decrypt? Politically difficult but without it your NGFW a& NIDS are largely blind.
  - SIEM
    - Centralized log management. If you have any compliance requirements you likely have a SIEM
    - All of these controls are presentations on their own, but particularly SIEM, it is central to all of your controls.

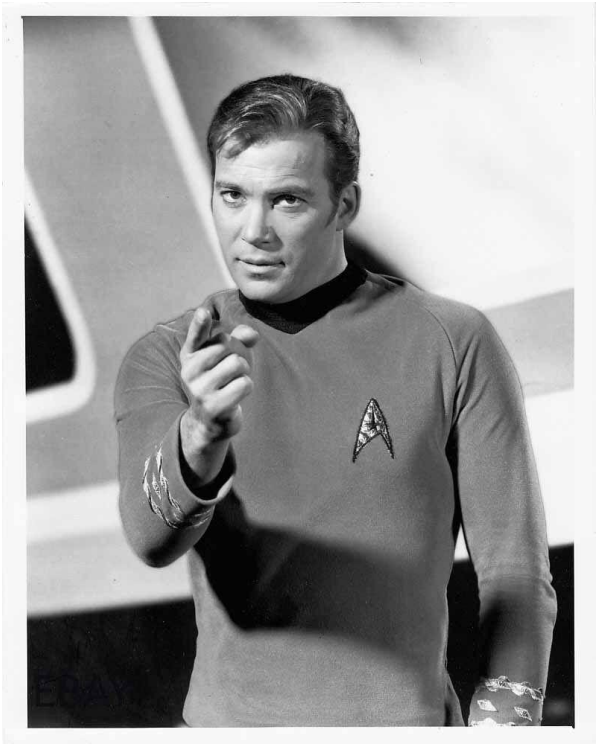
Detection: On-Prem Security

- Web Application Firewalls
  - It's not a firewall! WAF's are an App Proxy that generally follow the OWASP Top Ten to provide protection & **detection**.
  - Thought of as a prevent control, but is a strong detect control as well
  - If you can't get a commercial solution ModSecurity is an open-source alternative
- Web Proxy
  - Reverse Proxy: Service is protected by forcing connections through a proxy. WAF is a form of this
  - Forward Proxy: Systems request access through a proxy to a resource.
  - Provides protection for email traffic as well as spam control
- HoneyPots, Canaries & Tripwires
  - Tools to delay and confuse attackers on your enterprise while enabling detection

But what about the remote endpoints!

D(t): Remote Access & Cloud

- Endpoint Detection & Response: more than ever this may be your first line of defense
  - You'll see it again under Response
  - Be able to remote quarantine devices and test this
- Make sure Cloud Services can log security events to your SIEM
  - AWS VPC Flow Logs, Azure Monitoring, CSP's provide logging solutions
- Build automation to respond quickly to know attacks.
- Configure auditing on endpoints and tune! If you capture everything storage costs will break your budget, if you don't capture enough you'll be blind again.



D(t): Provide Employee Cybersecurity training

- Your employees can be a detection resource.
  - Stop thinking of them as problems and start teaching them how detect malicious activity, both in the office and at home.
- Where possible provide training specific to their role in the organization.
  - If you have PCI Compliance concerns you may be required to do this.
- Get beyond annual “checkbox” training.
  - Vendors provide “gamified” training.
  - You can create your own games as well (with prizes!) .
  - There is a Cybersecurity Awareness Month, use it to your advantage.
  - Cultivate Security Champions within your organization.

https://www.cisa.gov/cybersecurity-awareness-month#:~:text=Since%202004%2C%20the%20President%20of.confidential%20data%20become%20more%20commonplace

R(t): Time to Respond/React

- **Or, you've detected suspicious/malicious activity, now what?**
  - Automate wherever possible!
  - Known bad attacks should be blocked.
  - Your security solutions (EDR, NIDS, FW, DLP, etc.) generally have automated response built in as well as integration into ticket management systems (Jira, etc.) and notification (email, text, Slack, etc.) as well as automating response.
  - You can automate notification before response to make sure a human presses the button
  - You can build this into a Security Orchestration and Automation Solution (SOAR)

R(t): Remote Users

- VPN solution that supports Dynamic Access Control.
  - If the endpoint trustworthiness changes the VPN should alert & respond
    - Hosts that drop below a trust level must be quarantined, blocked or at least moved to a limited access network to get themselves fixed
    - Easier to deploy on the VPN than on the local network.
  - Can VPN solution inforce security policies? Do you have a device management system that can enforce security policies?
    - Microsoft's solution as of a year ago was weaker for remote hosts than internal network hosts. 3rd party tools aren't always better. You can implement startup and shutdown scripts as a workaround
- Extended Detection & Response (XDR),
  - Your EDR provider likely has a solution already
  - (Again) Test your ability to remotely quarantine a system
- If the host is a VDI you can quarantine it in the cloud
  - Standing up a VDI environment can allow you to enforce policy on endpoints like they were in the office
- Be able to automate the (relatively) easy stuff!

BYOD: Bring your Own Device

- **I'm giving BYOD a short shrift:** It's problematic from a security perspective as your enterprise data is now on employee personal devices
  - If someone tells you they have a solution that equals on-prem or a corporate device they are trying to sell you something, however do implement a Mobile Device Management (MDM) solution.
  - As Work from Home continues more corporations are going to start looking at having employees use their personal devices rather than provide them one
  - Is Virtual Desktop an option? Try to keep the data inside the perimeter even if the host is not.
  - Whatever you decide to do work with your legal department.
    - **Some of the controls you may want to implement might be illegal on an employees personal device**

A few more things

Post Covide Zero Trust

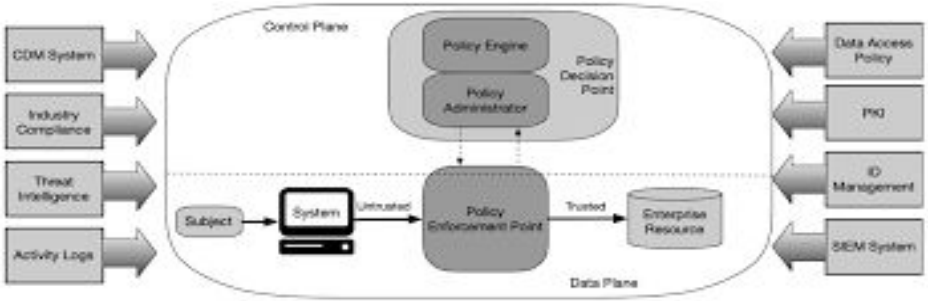
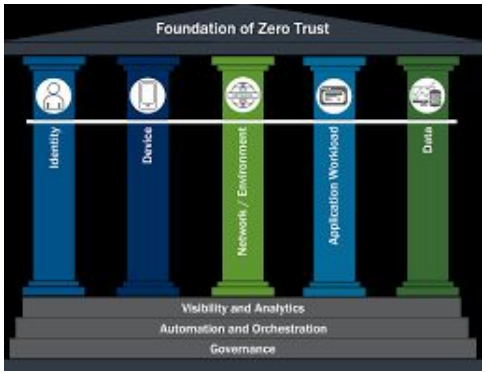


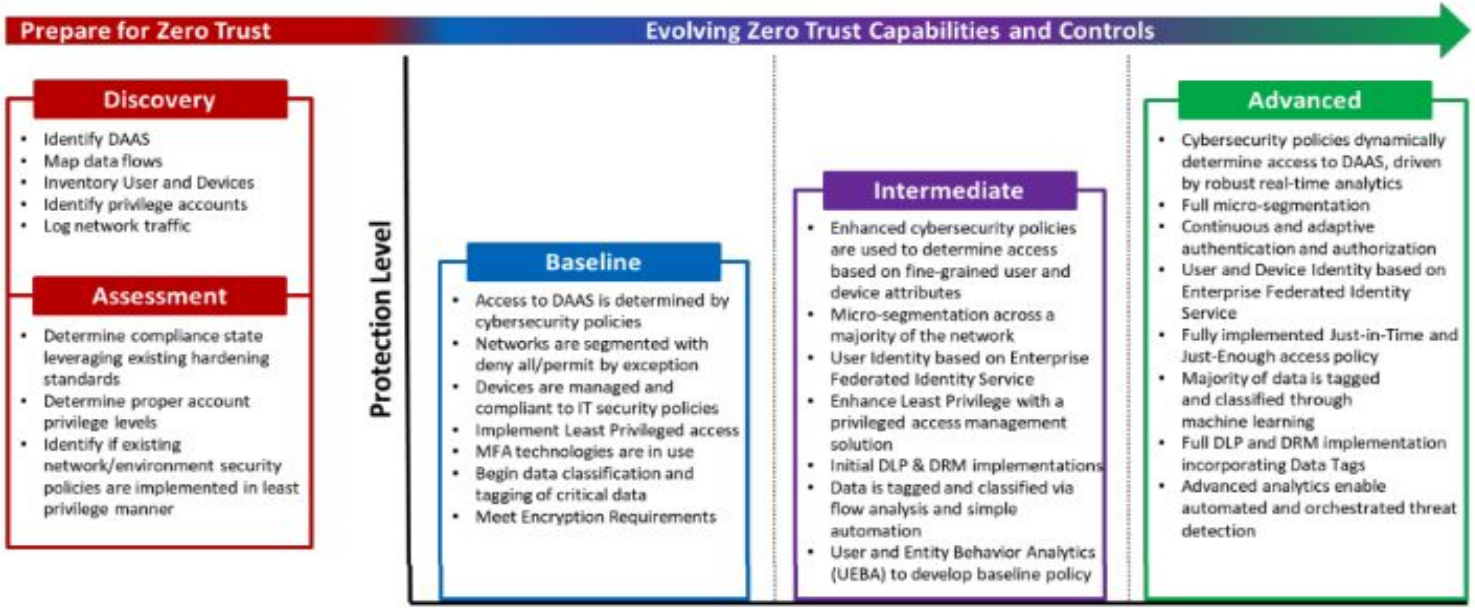
Figure 2: Core Zero Trust Logical Components



- Zero Trust has a Data-Centric focus
- Zero Trust should be considered a journey and philosophy as well as an architecture (“eating the elephant”). **If you are 70% successfully implemented you’re doing great!**
- Test & develop with systems that can support ZT, but build out from crown jewels (temet nosce)
- Follow NIST & DISA guidance for building **Zero Trust, it is not a product that can be purchased!**

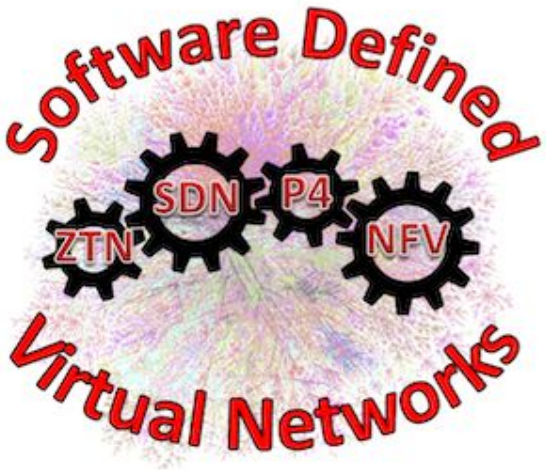
Remember, you’re already compromised!

Zero Trust Roadmap



Software Defined Wide Area Network (SD-WAN)

- SD-WAN lets you abstract the physical layer of the network
  - You're "internal network' connection could be over the internet
  - Look for security solution that complements SD-WAN, or comes with it.
- Not all solutions are created equal. Some provide excellent security and can help you "extend your perimeter" to your remote users
  - Zscaler & Palo Alto provide solutions in this space, but do your research
  - Check with your solution provider
  - **Extend your perimeter back to your remote hosts?**



https://www.nist.gov/programs-projects/software-defined-virtual-networks

The Last Battle[1]

- It’s a story about the Battle of Castle Itter, perhaps the last battle of WW2
- The Allied commander on site, Captain Lee, had to defend the castle against Nazi SS forces with one tank & 36 personnel consisting of U.S. Soldiers, German POW’s & eventually the French captives they were protecting
- He didn’t have to hold the castle against the Nazis, he just had to hold out long enough until reinforcements arrive

1- By Stephen Harding: https://www.amazon.com/Last-Battle-German-Soldiers-Joined/dp/0306822962/ref=sr_1_1?crid=1OSKA9UNGO2LM&keywords=the+last+battle+stephen+harding&qid=1678835058&sprefix=The+last+battle%2Caps%2C497&sr=8-1

Questions?