LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

Zero Trust in Healthcare

10/01/2020

Report #: 202010011030

Agenda

- What is Zero Trust?
- Why implement Zero Trust?
- What does Zero Trust involve?
- What are the benefits of Zero Trust?
- How to begin with Zero Trust

Slides Key:

Non-Technical: managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

What is Zero Trust?

- Created in 2010 by John Kindervag (Forrester)
- Shift from castle and moat security model to zero trust approach in order to address current IT environments and workplaces
- None of the following should ever be trusted by default, regardless of the location each is operating from, either inside or outside the security perimeter:
  - Devices
  - Users
  - Workloads
  - Systems
- Every device should be treated as a threat vector
- Anything that cannot be verified is denied access

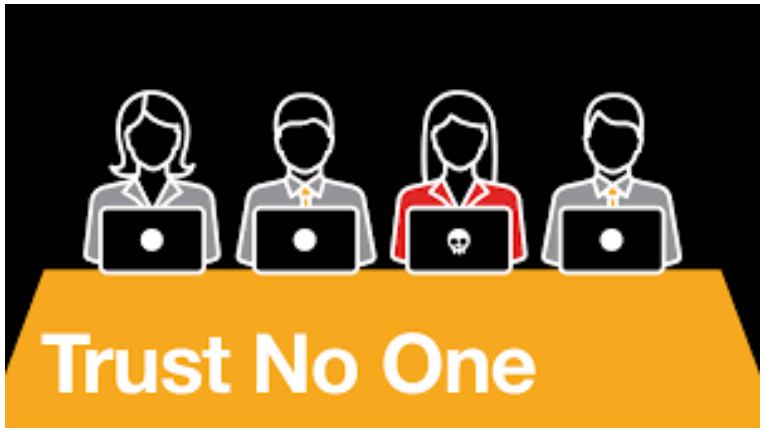

Image source: crowe.com

Image source: cloudflare.com

What is Zero Trust? (cont.)

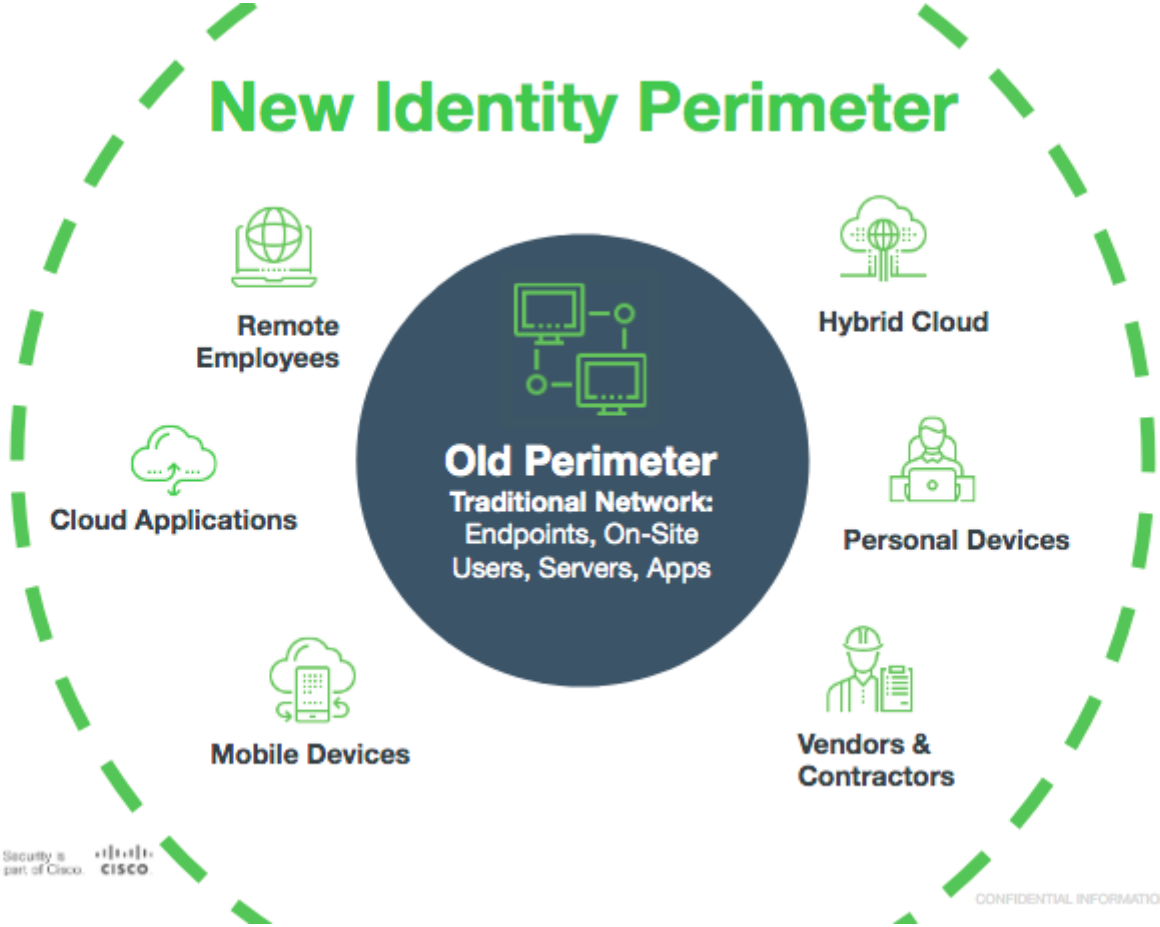

Image source: duo.com

Why Implement Zero Trust?

- Given the interconnected nature of the future with IoMT devices, augmented reality, robotics and more, it is clear that the current perimeter-based security model that most healthcare organizations use will no longer be effective. To stay ahead of these trends, healthcare organizations must continue to invest in the basics while making a fundamental shift from the castle-and-moat approach to a Zero Trust model.

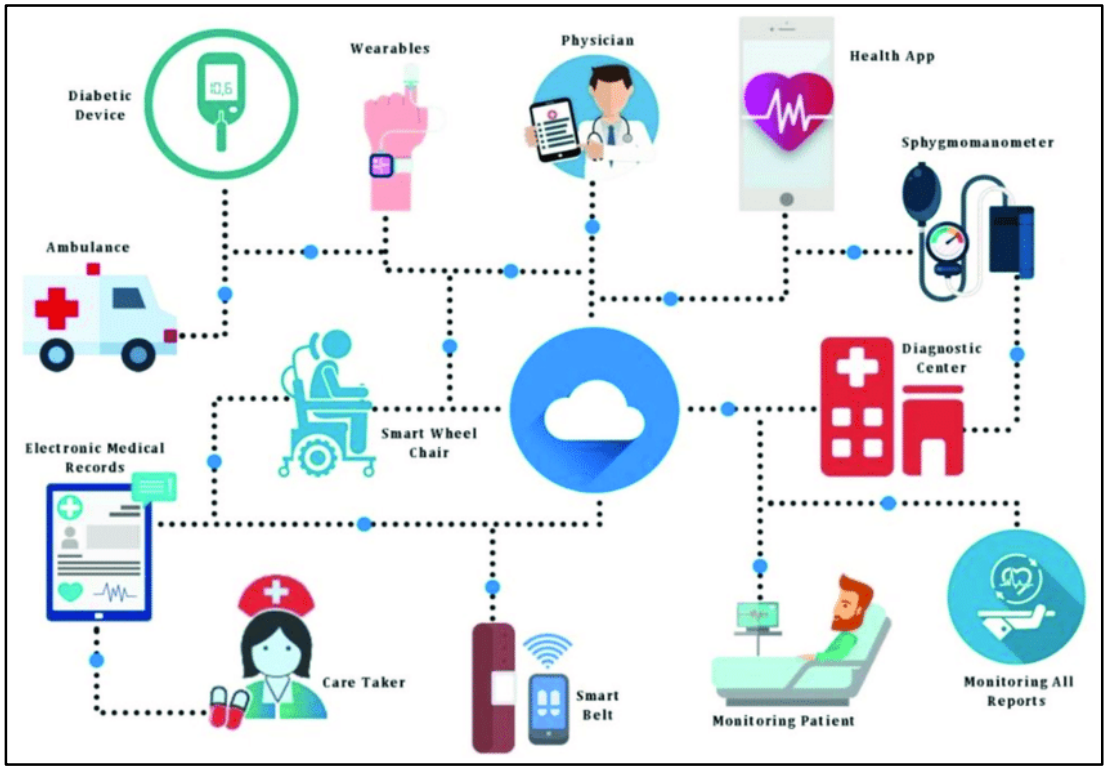

Image source: researchgate.com

What does Zero Trust Involve?

- According to Checkpoint, zero-trust security isn't accomplished by deploying a single tool or platform. The approach usually involves technologies from an array of categories including:

1. Device security
2. Network security
3. Data security
4. Workload security
5. Identity and access management
6. Visibility tools
7. Orchestration platforms

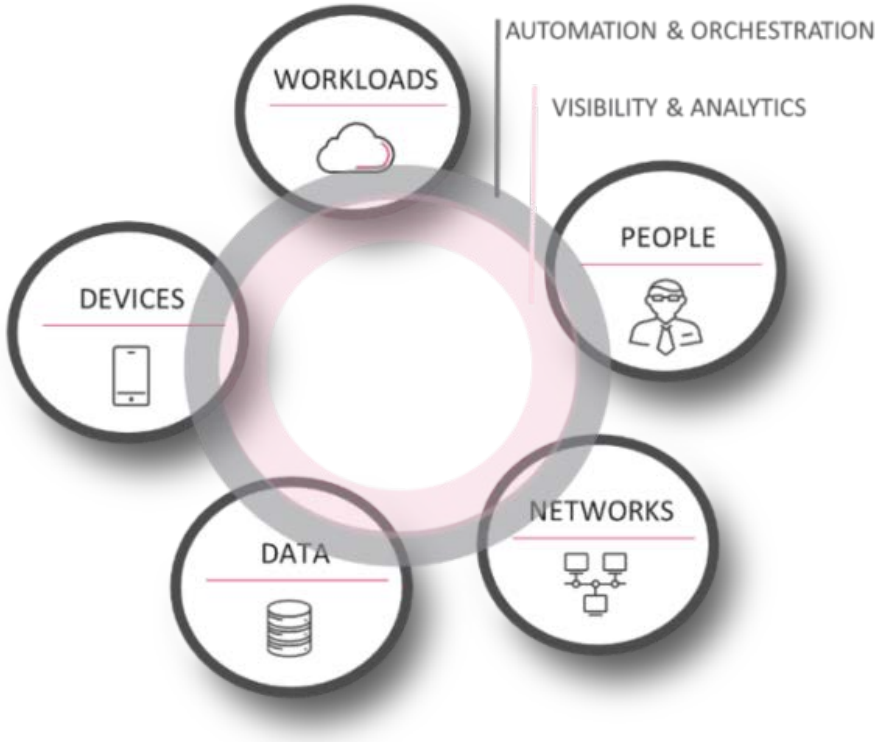

Image source: checkpoint.com

What Are the Benefits of Zero Trust?

- A Zero Trust model can help healthcare organizations provision access in a more effective manner by focusing on data, workloads and identity.

- ✓ Data-centric
- ✓ Workload-first
- ✓ Identity-aware
- ✓ Visibility
- ✓ Reinforces security orchestration and automation

Image source: visionsecuritytechnologies.com

Source: https://securityintelligence.com/posts/safeguarding-healthcare-for-the-future-with-zero-trust-security/

How to Begin with Zero Trust

- Software Defined Perimeter (SDP)
  - Hide Internet-connected infrastructure (servers, routers, etc.) so that external parties and attackers cannot see it, whether it is hosted on-premises or in the cloud
  - Base the network perimeter on software instead of hardware
  - Network layer vs. application layer
  - Device + user authentication
  - Increased security and flexibility

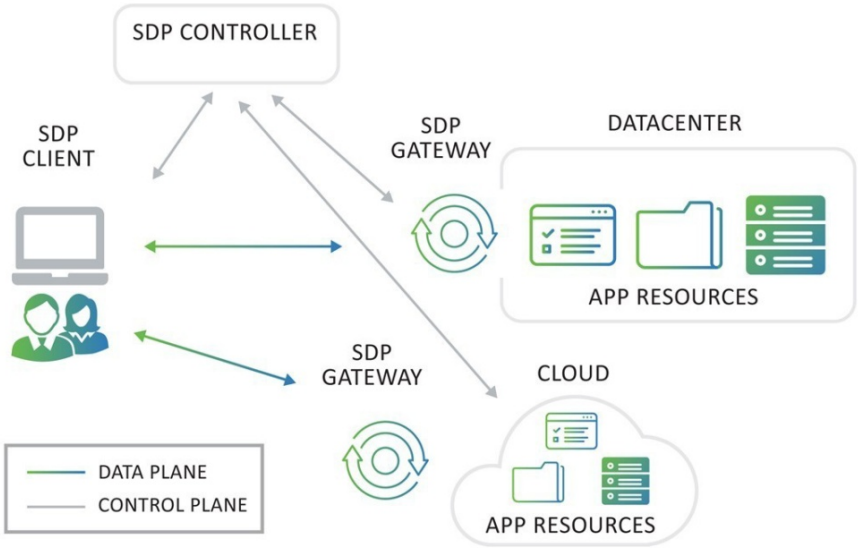

Image source: networkworld.com

How to Begin with Zero Trust (cont.)

- Mesh VPNs
  - Peer-to-Peer (P2P) architecture
  - Less expensive & easier to scale
  - Device identity checks at protocol level
  - User identity checks
  - Encrypted traffic

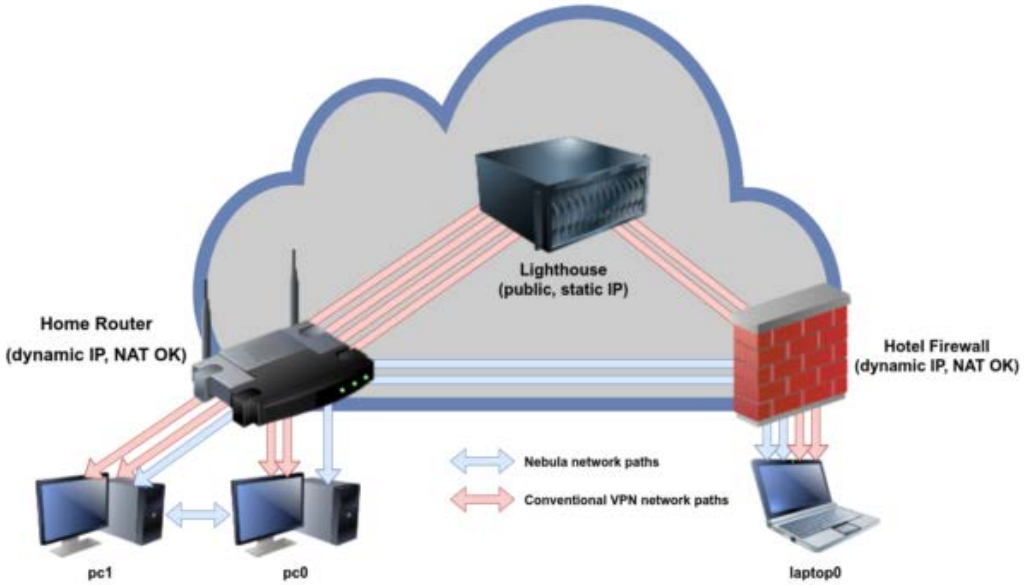

Image source: arstechnica.com

How to Begin with Zero Trust (cont.)

- Modern Network Access Control (NAC)
  - Identify every device/user on the network before granting access
  - Require continuous monitoring of the network & devices
  - Assess posture and compliance
  - Enforce access control

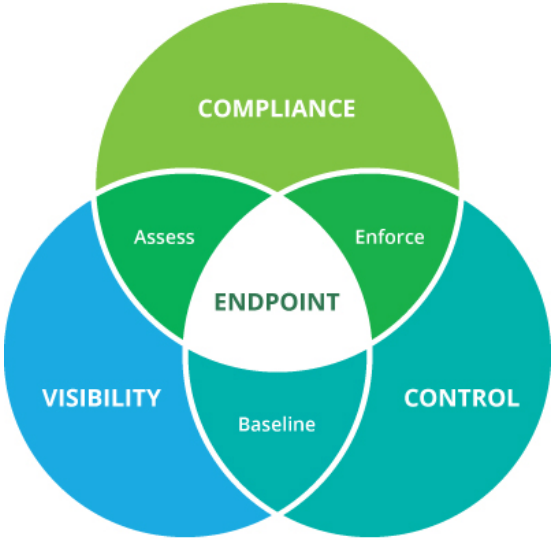

Image source: genians.com

Conclusion

- Don’t trust anyone!
- Deny all access until network can authorize users/devices
- Complete Zero Trust should secure devices, networks, data, workloads, and leverage IAM, visibility tools, automation & orchestration platforms

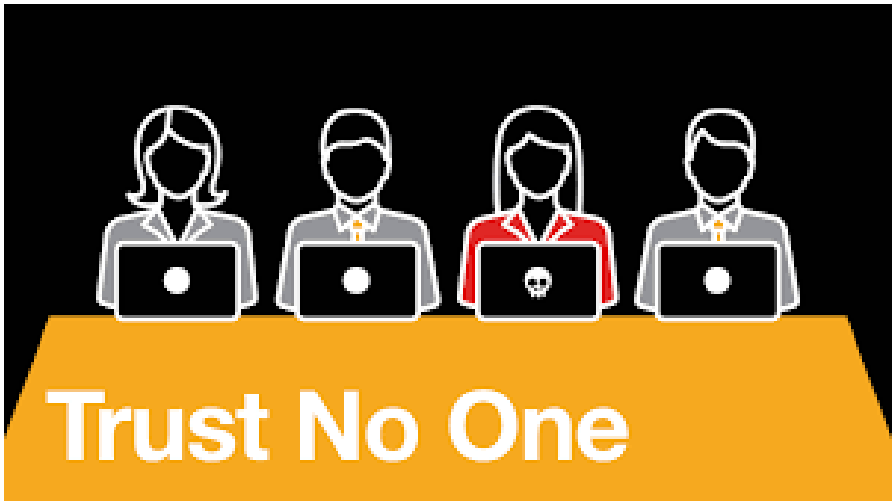

Image source: crowe.com

Reference Materials

References

- Nathan Eddy, Health systems adopt zero trust approach to secure networks, devices (11 March 2020)
  - https://www.healthcareitnews.com/news/health-systems-adopt-zero-trust-approach-secure-networks-devices
- Cloudflare, Zero Trust Security | What's a Zero Trust Network?
  - https://www.cloudflare.com/learning/security/glossary/what-is-zero-trust/
- Lucian Constantin, Mesh VPNs explained: Another step toward zero-trust networking (16 September 2020)
  - https://www.csoonline.com/article/3575088/mesh-vpns-explained-another-step-toward-zero-trust-networking.html
- Eitan Bremler, Zero Trust Can Fix Healthcare's Security Problem (16 February 2020)
  - https://securityboulevard.com/2020/02/zero-trust-can-fix-healthcares-security-problem/
- DXC, Why a zero trust security model makes sense in healthcare (20 November 2019)
  - https://blogs.dxc.technology/2019/11/20/why-a-zero-trust-security-model-makes-sense-in-healthcare/
- Heather Seftel-Kirk, Understanding Zero Trust and the Unique Opportunity it Presents for Federal Healthcare (4 February 2020)
  - https://www.fedhealthit.com/2020/02/understanding-zero-trust-and-the-unique-opportunity-it-presents-for-federal-healthcare/
- Aaditya Bhagra, Safeguarding Healthcare for the Future With Zero Trust Security (11 March 2020)
  - https://securityintelligence.com/posts/safeguarding-healthcare-for-the-future-with-zero-trust-security/

References

- NCCOE, Zero Trust Architecture
  - https://www.nccoe.nist.gov/projects/building-blocks/zero-trust-architecture
- Chris Gerritz, 5 considerations for building a zero trust IT environment (2 March 2020)
  - https://www.helpnetsecurity.com/2020/03/02/building-zero-trust/
- Thu T. Pham, An Overview of Zero Trust Architecture, According to NIST (7 January 2020)
  - https://blogs.cisco.com/security/an-overview-of-zero-trust-architecture-according-to-nist
- CheckPoint, Video: What is Zero Trust Security? (21 November 2019)
  - https://youtu.be/1D5mg9an19o
- Forrester, The Zero Trust Security Playbook For 2020
  - https://www.forrester.com/playbook/The+Zero+Trust+Security+Playbook+For+2020/-/E-PLA300#
- Cloudflare, What is a software-defined perimeter? | SDP vs. VPN
  - https://www.cloudflare.com/learning/access-management/software-defined-perimeter/
- Duo, Zero Trust Evaluation Guide: Securing the Modern Workforce (20 April 2019)
  - https://duo.com/blog/zero-trust-evaluation-guide-securing-the-modern-workforce
- US Food and Drug Administration (FDA), Cybersecurity with Medical Devices
  - https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity

References

- Nathan Eddy, Health systems adopt zero trust approach to secure networks, devices (11 March 2020)
  - https://www.healthcareitnews.com/news/health-systems-adopt-zero-trust-approach-secure-networks-devices
- Nathan Siegel, Zero Trust a Frontline Defense Against Healthcare Attacks (25 February 2020)
  - https://www.perimeter81.com/blog/zero-trust/zero-trust-a-frontline-defense-against-healthcare-attacks/
- Louis Columbus, How To Protect Healthcare Records In A Zero Trust World (16 December 2018)
  - https://www.forbes.com/sites/louiscolumbus/2018/12/16/how-to-protect-healthcare-records-in-a-zero-trust-world/
- Gigamon, White Paper: Your Guide to Zero Trust for Healthcare
  - https://www.gigamon.com/resources/resource-library/white-paper/wp-zerotrust-healthcare.html
- Palo Alto Networks, What is Zero Trust?
  - https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture
- Tony Kueh, A Practical Guide to Zero-Trust Security (15 January 2020)
  - https://threatpost.com/practical-guide-zero-trust-security/151912/
- Tommy Peterson, How Hospitals Can Establish a Zero Trust Security Model
  - https://healthtechmagazine.net/article/2020/07/how-hospitals-can-establish-zero-trust-security-model

Questions

Questions

Upcoming Briefs

- TrueFighter and RDP Access (10/8)
- Using Honeypots for Network Intrusion Detection (10/15)

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to **HC3@HHS.GOV** or call us Monday-Friday, between 9am-5pm (EST), at **(202) 691-2110.**

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback. If you wish to provide feedback please complete the HC3 Customer Feedback Survey.

HC3 Customer Feedback

Disclaimer

These recommendations are advisory and are not to be considered as Federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. HHS does not endorse any specific person, entity, product, service, or enterprise.

About Us

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

Sector & Victim Notifications

Directed communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft and general notifications to the HPH about currently impacting threats via the HHS OIG

White Papers

Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings & Webinar

Briefing document and presentation that provides actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic or want to join our listserv? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday-Friday, between 9am-5pm (EST), at (202) 691-2110.
Visit us at: www.HHS.Gov/HC3

Contact

www.HHS.GOV/HC3

(202) 691-2110

HC3@HHS.GOV