Zero Trust – What Is It?
Associated Best Practices and Vendors

Tony Massimini, Senior Industry Analyst

January 27, 2020

Zero Trust - Agenda

- What is a Zero Trust Network (ZTN)?
  - What is it NOT?
- Importance of ZTN
- Elements of ZTN
- Important tenets of ZTN
- Some key vendors
- Implementing Zero Trust
- ZTN with IoT, IIoT, IT/OT and utilities industry
- Conclusion and Best Practices to follow

What is Zero Trust?

- A Zero Trust Network (ZTN) is based on the basic principle of **“never trust, always verify”.**
- ZTN is a model or guiding design principle. It is an overall strategy and framework to prevent unauthorized access, contain breaches, and reduce the risk of an attacker’s lateral movement through your network.
- ZTN is a general approach for leveraging various security technologies to enable perimeter enforcement and strict access controls.
- No one is trusted by default from inside or outside the network. Verification is required from everyone and everything trying to gain access to resources on the network.
- ZTN is a comprehensive approach to securing all access across your networks, applications, and environment.
  - secure access from users, end-user devices, APIs, the Internet of Things (IoT), microservices, containers, and more.

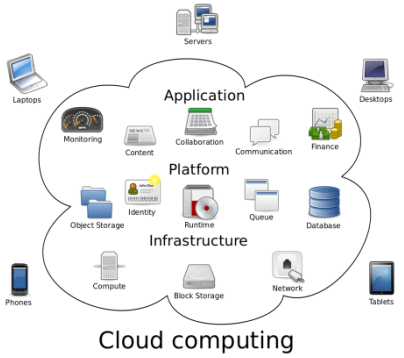
What Zero Trust is NOT

- ZTN is not a single point product that is a drop in solution to protect your castle.
  - It is an integrated ecosystem of several security solutions and tools from multiple vendors.
- ZTN is not a panacea. You need to remain vigilant. Never trust, always keep adding context and keep up-to-date who the user/device is and the defined appropriate interaction.
  - Add more authentication methods to counter credential based attacks.

- ZTN is not an overnight solution. It will take time to develop.
- ZTN is not limited to the traditional endpoints (PCs, servers, etc.). It extends to cover IoT devices.
- ZTN is not just to stop attackers at the perimeter. Traffic inside the perimeter should not be more trusted any more than outside traffic.
  - You can set how tightly access is restricted to verify access.

Importance of Zero Trust Network

- The network perimeter is no longer clearly defined. Organizations are migrating to the cloud.
  - applications and data stores are on-premises and in the cloud, with users accessing them from multiple devices and locations.
- Environments include cloud-based services, mobile workloads and a growing number of unmanaged devices.
- Increasing level of malware, cyber attacks and attack innovation
- Every device on a network is a potential attack or reconnaissance point.



Importance of Zero Trust Network

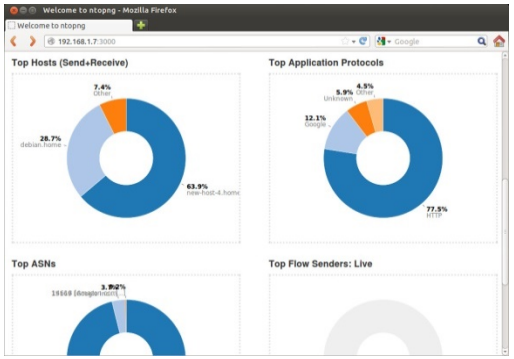
- Increasing number and diversity of endpoint devices opens up more attack vectors.
  - Different OS's, mobile, different communications standards, and legacy systems. Each have their own vulnerabilities.
- User, guest and contractor access expansion.
- Growing adoption of BYOD and IoT devices on the network.
- The growth of BYOD, guest and contractor access, and IoT has made it evident that the network is no longer composed of securely managed devices.
- Traditional security is designed to protect the perimeter, but threats can get inside the network undetected and free to move around.

Elements of Zero Trust

- The concept of a Zero Trust Architecture has been around for about a decade. Interest in ZTN picked up a little over a year ago. The momentum has been growing.
  - Cisco has seen discussions accelerate over last 12 months. Expects to see further growth in next 12 months.
- ZTN is achieved via integration, automation and orchestration of various security solutions. Security is a layered approach.
  - Need to consistently enforce policy based controls.
- Visibility into users, devices, components, and more across your entire environment.

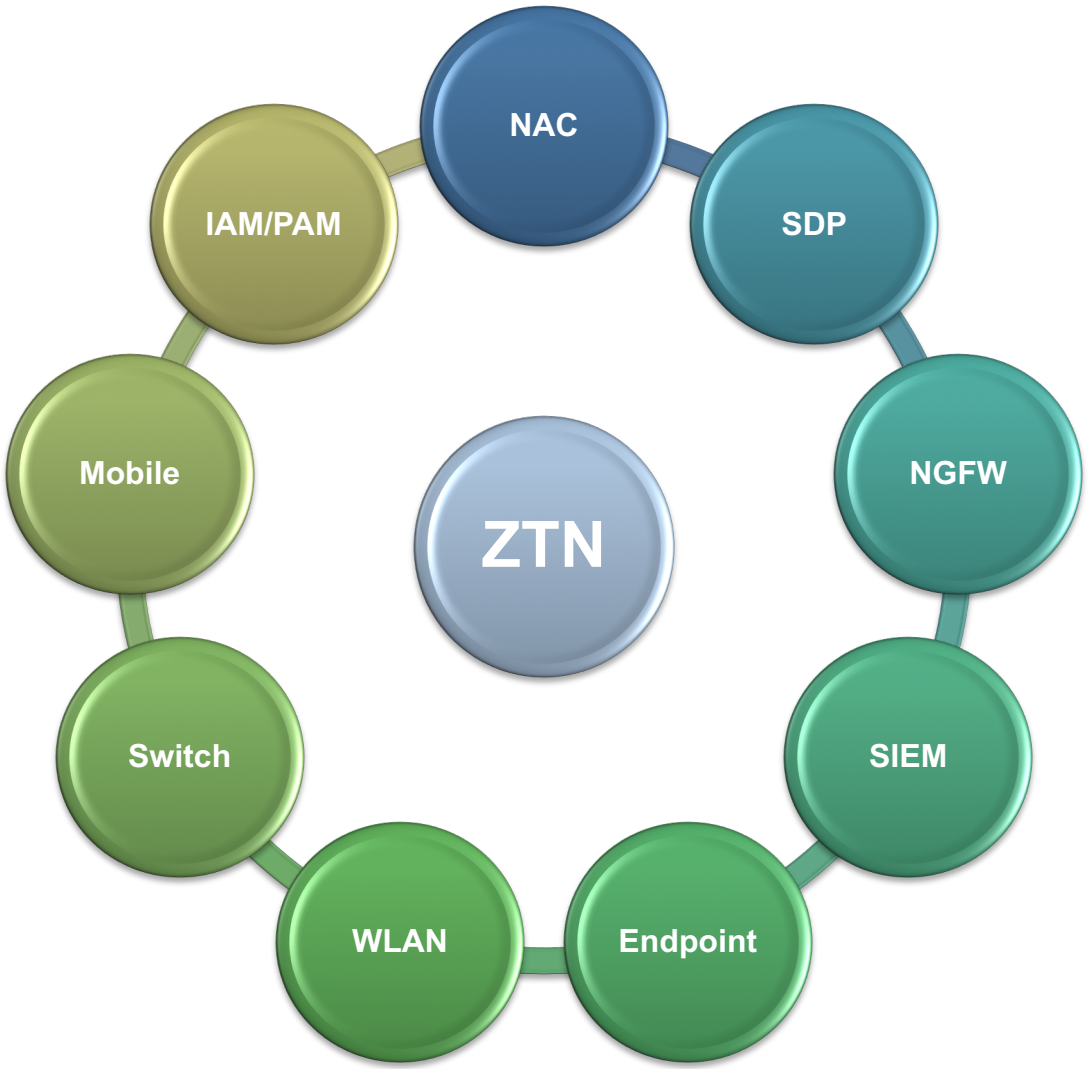
Elements of Zero Trust

- Strict identity verification process. Only authenticated and authorized users and devices can access applications and data.
- Segmentation and granular access policies for all connecting endpoints must be defined, implemented, and enforced.
- Least-privilege access: “information on a need-to-know basis”.
- All network traffic should be inspected and logged. Encryption across all communications.
- Dynamic policy, trust assignments and segmentation.



Zero Trust Network Ecosystem

- Leverage your ecosystem.
- There is no one single specific technology for ZTN.
- ZTN is a holistic approach to network security incorporating several different principles and technologies.
- Core technologies for ZTN: NAC, SDP, NGFW, SIEM, Endpoint, WLAN, Switch, Mobile and IAM/PAM.
- Other security solutions can be integrated for ZTN, i.e. email, SWG, CASB, and more



Key Tenets of Zero Trust

"Never Trust, Always Verify"

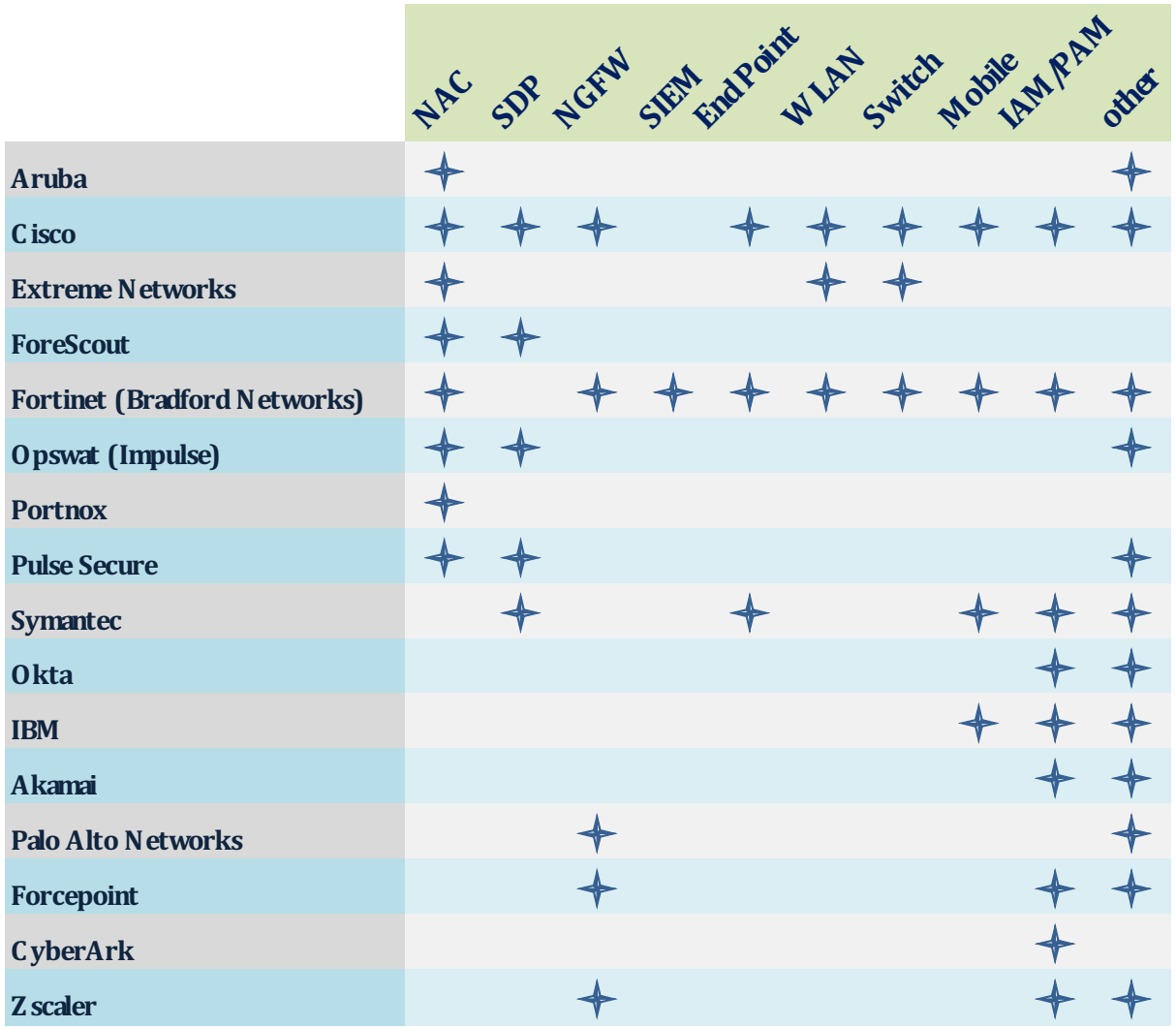
- NAC is a foundational network security defense. It provides visibility, monitoring and control. NAC orchestrates and integrates a variety of network and security infrastructure. It provides flexible endpoint policy management.
- Classification of users and endpoints is the basis of visibility and determining secure access policies.
- SDP protect users as they access workloads and applications. It is complimentary to NAC.
  - Future trend: NAC vendors expected to integrate SDP as a feature.
- IAM/PAM is crucial for strict identity verification, regardless of whether the user or device are sitting within or outside of the network perimeter.

Key Tenets of Zero Trust

- Segmentation is the practice of breaking up security perimeters into small zones to maintain separate access for separate parts of the network. Microsegmentation provides finer granularity.
  - Segmentation restricts east-west attacks.
  - Separate authorizations for each zone
- Least privilege access reduces pathways typically used by malware and attackers and reduces the chances of internal data exfiltration.
- Risk adaptive security controls - User Entity Behavior Analytics (UEBA).
- Assume that there are attackers both within and outside of the network. No users or machines should be automatically trusted.
  - Beware the insider threat.

Key Vendors Supporting ZTN

No one vendor has all the components for a complete solution.



Key Vendors Supporting ZTN

- Many vendors are promoting their ZTN capabilities via integration of their product portfolios. Most vendors offer a ZTN platform or program focusing on their specific strength.
- NAC, NGFW, SDP and IAM/PAM are the foundations for vendors.
- ZTN vendors partner with other companies for integrating technologies they do not have or which a customer has licensed. Customers are able to leverage security technologies they have purchased.
- One vendor must be the leader for a ZTN deployment. There can be only one quarterback on the field.
  - Ex. Portnox offers NAC, but partners with Palo Alto and Okta who provide ZTN platforms
- Notable acquisitions:
  - Symantec – Luminate Security for SDP (Feb. 2019)
  - Cisco – DUO Security for verification with MFA (Oct. 2018)
  - Fortinet – Bradford Networks for NAC (June 2018)
  - OPSWAT – Impulse for NAC and SDP (Dec. 2019)

Implementing Zero Trust

- Evaluate all risk factors surrounding the user/endpoint and their authenticating device.
- Determine access needs – which user or device needs access to what in your organization. Implement restrictions to secure core privileges on applications, devices and endpoints.
- Implement strong network controls that segment and isolate data and resources. This includes on-premises, web-based and cloud-based systems.
- Deploy Multi-Factor Authentication (MFA).
- Classification of users and endpoints is the basis of visibility and determining secure access policies.
  - Classification of device identity is based upon discovered characteristics such as OS, device type, and business function.

Implementing Zero Trust: Onboarding Considerations

- ZTN vendors offer automated onboarding tools.
- Ease of deployment: facilitates configuration settings, integrations and basic customization of guest, BYOD and other secure access rules.
- Important to identify and enable automatic and custom classification of both managed and unmanaged endpoint devices
- NAC uses IEEE 802.1X standard which requires an agent on the endpoint. Most IoT devices are non-802.1X compliant. NAC agentless technology is used for unmanaged devices. Different methods for profiling and verification.

Complications

- Unclassified: if classification is not possible it is “unknown”
  - Will require periodic review, assessment, classification and policy adjustment
  - Device profiles can be customized to enable similar device verification and access
- Non-compliant devices
  - Enable automated remediation prior to verification and granting access
  - Unsanctioned devices from specific manufacturers may be blacklisted

Zero Trust with IoT, IIoT, IT/OT and Utilities Industry

- An effective ZTN strategy means you must vet every device; ensure it is trustworthy; grant access; and then isolate, secure, and control every device touching the network at all times.
- According to Frost & Sullivan, there will be 45.4 billion connected devices by 2023. The high growth of IoT poses challenges to enterprise networks since these are mostly non-802.1X compliant. Some NAC vendors estimate that more than half of all endpoint devices in an organization are IoT.
- IT and OT have developed independently. Convergence offers benefits of improved efficiencies, it also exposes previously isolated systems to cyber attacks.
- NAC vendors have made implementation easier with improved tools and automation specifically addressing IT/OT convergence.
  - Ex. Cisco, ForeScout, Fortinet and Pulse Secure
- ZTN vendors are focusing on the specific needs of IoT, IIoT, and IT/OT.
- Example: OPSWAT has supported ZTN for IIoT, especially utilities.
  - Solutions include Secure Device Access, Cross-Domain Solutions , File Upload Security, Malware Analysis, and email security. Acquisition of Impulse adds NAC and SDP.

Conclusion and Best Practices to follow

- ZTN principle of “never trust, always verify” protects against lateral threat attacks
- ZTN strategy is a holistic approach. Layered security.
- Define key policies: guests, endpoint compliance, apps/resources
- Focus on core integrations: NAC, switch, wireless, NGFW, SDP, SIEM, endpoint, mobile, IAM/PAM
- Set endpoint compliance rules: cert., malware, system Scan, patches, settings
- Explore advanced features: VPN/NAC integration, mobility, threat response and UEBA
- Implement least privilege access, segmentation, MFA, and risk-adaptive security controls.
- Know what is on your network. Monitor and log the flow of data.
- Strict identity and device verification must be maintained for anyone and anything attempting to access network resources.
- Classify, verify and segregate: unknown, unmanaged and IOT devices.
- One ZTN vendor should lead your efforts to leverage and integrate your ecosystem.
- Rome was not built in a day. A global ZTN is not achieved overnight.
  - Prioritize your most sensitive assets. Implement ZTN in increments.

Thank You

Questions and Answers

About Frost & Sullivan

- Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the global 1000, emerging businesses, the public sector and the investment community.
- **Industry Research**
  - Frost & Sullivan was founded on the simple premise that research should enable decision-makers to use marketing information in more innovative and meaningful ways. With this objective in mind, the company developed a comprehensive range of research services and state-of-the-art analytical tools. Frost & Sullivan has continued to grow, adapt, and innovate to meet the challenges and opportunities of today's ever-changing business world.
- www.frost.com

Tony Massimini

Tony Massimini

Senior Industry Analyst

Frost & Sullivan
North America
Phoenix, AZ

Functional Expertise	• Over 26 years of experience in market research in the semiconductor industry. Strong technical and analytical skills. Since July 2016, covering cyber security at Frost & Sullivan. ○ Research tracking markets and technologies. Interviewing skills. Predicting industry trends and developments. ○ Executive level consulting ○ Deliver competitive analysis and consulting to clients to aid in their product development, technical and strategic marketing plans, and for due diligence in mergers and acquisitions
Industry Expertise	• Industry Principal on IT and Information Security market strategies, business opportunities, and technologies. Concentration in: ○ Secure web gateways, Email security, Endpoint security, Endpoint management, Cloud Access Security Broker (CASB) and Network Access Control (NAC).
What I bring to the Team	• Over 26 years of experience as a market analyst in Technology, Computing and Media, including primary research, interviewing, in-depth research reports, forecasting, and presentations • Industry experience and technical education and background • Broad functional expertise including analysis, sales, and consulting. Strong writing, presentation and public speaking skills. • Managed portfolio of reports and services
Career Highlights	• Founding partner for start-up marketing research firm with exceptional industry traction at Semico Research. Delivered innovative research solutions as Chief of Technology (Semico) covering MPUs, MCUs, MEMS, embedded control and IoT (1995 to 2016). Market analyst for Micro Logic service at InStat (1992 to 1995). • Applications engineer in semiconductors with VLSI Technology (acquired by NXP) and STMicroelectronics, providing hands on technical experience and customer interaction. (1986 to 1992).
Education	• Bachelor of Science Electrical Engineering from Northwestern University, Evanston, IL (USA)
Languages	• English, Italian and Spanish

Tony Massimini

Contact info:

Tony Massimini
Frost & Sullivan
Senior Industry Analyst
Information & Communication Technologies
tony.massimini@frost.com
Cell: 602-301-7485

FROST & SULLIVAN

Research • Consulting • Growth