ZERO TRUST:
MIRACLE OR MIRAGE?

Introduction

According to a Forrester Research client survey, 84% of respondents believe the network perimeter is no longer defensible.[1] It's no surprise when considering the technological changes with the digital transformation. The wide-scale adoption of hybrid clouds, subscription-based cloud services, ubiquity of user-owned devices, among other initiatives have blurred the conventional network perimeter. Once considered durable, traditional InfoSec's "trust but verify" has faded.

Digital technology has revolutionized business processes, customer experiences, and given you a foundation for future growth. But, it has also altered the security landscape. Established networks and assorted best-of-breed security are tested tens of thousands of times a day. Ransomware alone will reach $10 billion in 2019. The annual cost of cybercrime damages is expected to hit $5 trillion by 2020.[2]

Today's high-velocity cyberattacks are no longer wanton. They're targeted. Well-heeled cybercriminals strike selectively to steal the crown jewels at the heart of the digital expansion: your data.

In this paper, we'll explore the zero trust security model. Is it viable for organizations to adopt? Can zero trust be the new formula to turn back the clock where good did overcome evil?

[1] "Future-proof Your Business With Zero Trust," Webinar with Chase Cunningham and Paul McKay, Forrester Research

[2] "Cyber Security Statistics for 2019," Cyber Defense Magazine, March 21, 2019

What is Zero Trust?

No organization fights sophisticated cyber threats with weak defenses, and expects to win. Although cyber security technology continues to make tremendous strides, the balance of power has tipped to well-funded cybercriminal and nation-state syndicates. A recent UN report indicated North Korea hackers launched 35 large-scale attacks against financial institutions and cryptocurrency exchanges in 17 countries. Allegedly, the estimated $2 billion take will go to fund the development of WMDs (Weapons of Mass Destruction).[3]

Enter the zero trust security model approach. Widely recognized by its "never trust, always verify security" paradigm, Forrester analyst Dr. Chase Cunningham describes zero trust this way,

> "Zero Trust is strategically focused on addressing lateral threat movement within the infrastructure by leveraging micro segmentation and granular enforcement, based on user context, data access controls, application security, and the device posture.[4]"

Rather than user access granted by the network, Forrester's core principle[5] states access to services should be granted based upon:

- What you know
- What we know about the entity
- What we know about your authorization to access each service

Forrester recommends these five steps to building a zero trust network:[6]

[3] "UN probing 35 North Korean cyberattacks in 17 countries, by Edith M Lederer, ABC News, August 12, 2019

[4] "Forrester's Five Steps to a Zero Trust Network," by Dr. Chase Cunningham, Forrester Research, October 1, 2018

- Identify your sensitive data
- Map the data flows of your sensitive data
- Architect your zero trust microperimeters
- Continuously monitor with security analytics
- Embrace security automation and orchestration

Zero trust pros and cons have been mulled over by security practitioners for a decade. Recently, it has gained traction. A Forbes Insight survey of 1,000 security practitioners and executives found 66% of respondents said they have zero trust policies in place for application behavior, devices, and access.[7] It's a good start. Interest in zero trust is growing. Plug in "zero trust security" in Google Trends and you'll see searches reached peak levels in June 2019.

Cunningham has also acknowledged a few years ago that zero trust was a concept, but now, it's a combination of concept, theory, and technology to achieve an outcome."[8]

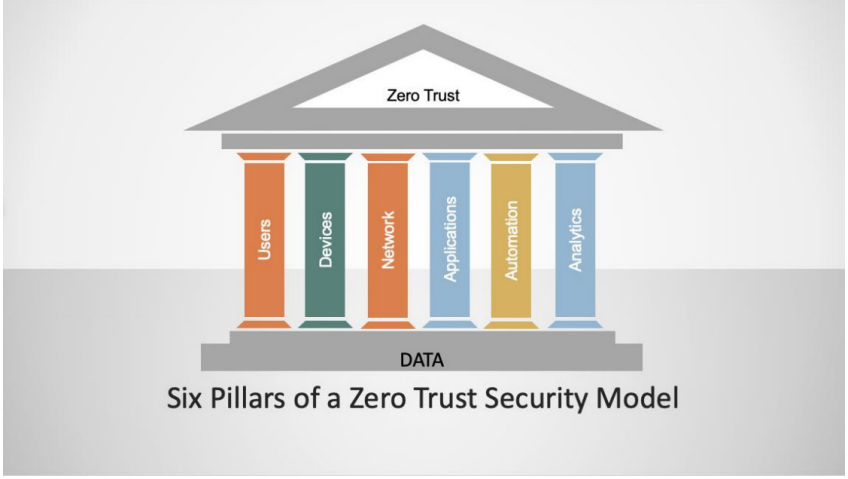

Figure 1. Pillars of Zero Trust Security

[5] "Future-proof Your Business With Zero Trust," Webinar with Chase Cunningham and Paul McKay, Forrester Research

[6] Ibid

[7] "Zero Trust: The Modern Approach to Cybersecurity," Forbes Insights, June 12, 2019

[8] "Nothing personal: Zero Trust meant to stop cyber breaches before they start," by Amelia Brust, Federal News Network, April 9, 2019

The Zero Trust Security Model

The Forrester Zero Trust Security Model (see below) re-structures security thinking, concepts, and the technology apparatus needed to meet the fluid changes of a digitally centric world.

Zero trust balances secure user access to data and apps with the ability to monitor shifts in your internal landscape. The model specifies six pillars that need to be integrated to protect cyber assets. Here are four best practices to consider when creating a perimeter-free, zero trust environment:

MICRO-SEGMENTATION

This calls for the compartmentalization of different parts of a network. Security perimeters over small zones, or isolated areas, are used to separate network access. Users with access to one zone are prohibited from accessing other zones unless granted authorization. Micro-segmentation reduces human error and internal threats to a specific segment.

APPLICATION BEHAVIOR AND VISIBILITY

Allows for the detection of anomalous activity, issues system alerts, and makes it easier to prevent a breach in access or data. This element of zero trust allows security systems to identify potential internal threats and fix them before they can inflict damage.

MULTIFACTOR AUTHENTICATION (MFA)

This approach improves on traditional user access security perimeter by requiring a second method of user authentication in addition to password validation. It verifies the identity of a user with all attempted logins. A numeric code sent to the user's device, a security question, and biometrics are examples.

LEAST PRIVILEGE

This practice functions as a need-to-know security measure, granting only the amount of access needed for a user to execute their role or purpose. Similar to micro-segmentation, least privilege reduces the risk of rogue access or data infecting the whole system by reducing the perimeter of each device or user.

The focus on users, their access, and validating system access is fundamental to the Zero Trust Security Model. Insider transgressions, by accident or deliberate action, are a huge threat, crippling many businesses. A recent Verizon report found 57% of data breaches involved insiders and 61% did not possess high levels of access.[9]

[9] "Insider Threat Report," Verizon, 2019

Zero Trust eXtended (ZTX)

More recently, Forrester introduced Zero Trust eXtended, or ZTX, an application and data-focused version of Zero Trust. The ZTX framework allows architects to map technologies and solutions to the framework's six pillars as described below:[10]

- **Network**—What does the technology do to enable the principles of network isolation, segmentation, and ultimately security?
- **Data**—What does the technology do that enables data categorization, schemas, isolation, encryption, and control?
- **Workforce**—How does the solution work to secure the humans that are using the network and business infrastructure, and does the solution reduce the threat that users create?
- **Workload**—Does the solution or technology secure areas such as cloud networks, apps, and anything else that a business or organization uses to make the business operate technically?
- **Automation and Orchestration**—How does the technology or solution automate and orchestrate zero trust principles and empower the business to have more powerful control of disparate systems?
- **Visibility and Analytics**—Does the technology or solution provide useful analytics and data points and eliminate dark corners of systems and infrastructure?

Cunningham relates, "A system, tool, or technology must have considerable and specific technical capabilities in at least 3 pillars of the framework and a powerful API integration capability to be considered a ZTX platform."[11]

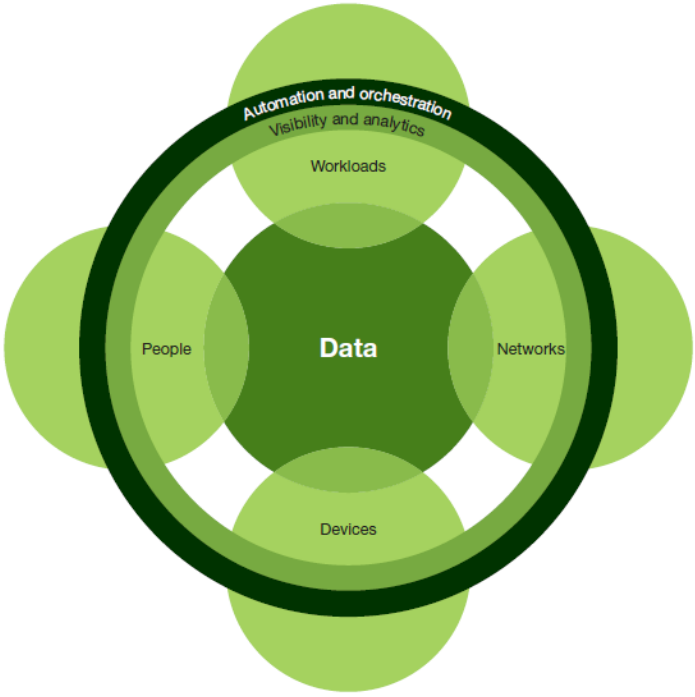

Figure 2. Zero Trust eXtended

[10] "What ZTX means for vendors and users," by Chase Cunningham, Forrester, January 23, 2018

Google BeyondCorp: Zero Trust-like Security

It's been five years since Google published "BeyondCorp: A New Approach to Enterprise Security." This document outlined Google's zero trust-like security model for its own internal use. It included the removal of VPNs, replacement of device inventories with a centralized system, and an extensive overhaul of the HR system to analyze employees' job function, and "cross-referencing this information against workflow qualification" required for network access. Google required that only devices procured and actively managed by the enterprise could access corporate applications. In short, personal devices are not allowed to access Google assets.[12]

Conclusion

If you're weighing the pros and cons of the Zero Trust Model, Forrester's recommendations from a published report nearly a decade ago still rings true:[13]

- Change how you think about trust.
- Break away from the three-tiered hierarchical networking model.
- Set up recurring meetings with your counterparts in networking.
- Grill your network and security vendors about zero trust.
- Include zero trust architectural requirements in every networking or security RFP.

Check Point Software offers Absolute Zero Trust Security with Check Point Infinity, a practical, holistic approach to zero trust implementation with a single consolidated zero trust security architecture. Click here to get started with the Check Point Zero Trust implementation.

[11] "What ZTX means for vendors and users," by Chase Cunningham, Forrester, January 23, 2018

[12] "Pros and cons of a Zero Trust security framework," by Christine Wong, ExpertIP, September 20, 2018

[13] "Build Security into Your Network's DNA: The Zero Trust Network Architecture," by John Kindervag, Forrester Research, November 5, 2010

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com