DELL Technologies

PRODUCTS AND OPERATIONS
OFFICE OF THE CHIEF TECHNOLOGY OFFICER

How will Zero Trust help my business?

Herb Kelsey
Federal CTO

Copyright © 2023 Dell Inc. or its subsidiaries. All Rights Reserved. Dell Technologies, Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

Table of Contents

Introduction **3**

Benefits of using Zero Trust **3**

1. Prevent unauthorized access 3
2. Curb freedom of movement 4
3. Reduce the blast radius 4
4. Avoid too many on-ramps 4
5. Safeguard against compromised technology 5
6. Eliminate operational risk 5
7. Enhance response effectiveness 5

Dell Technologies can be the industry's Zero Trust integrator **5**

Copyright © 2023 Dell Inc. or its subsidiaries. All Rights Reserved. Dell Technologies, Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

Introduction

Cyberattacks pose immense financial and third-party liability risks as more organizations enable remote work, interact with consumers on their personal devices, and expand their compute and capabilities off-premises. It is in the news, on the rise,[1] and having an increasing economic and societal impact.[2] Within the public sector, governments are also looking for ways to protect their critical infrastructure, such as fuel and water sources, from cyberattacks, as these could become national security risks. The world is increasingly fighting digital wars.

Meanwhile, Zero Trust is gaining renown as a solution for many cybersecurity concerns. It is a compelling proposition, considering an advanced Zero Trust solution aims to automate an organization's security and orchestrate an effective response as soon as systems are attacked. It can even work for businesses that do not have significant in-house cybersecurity expertise. It will also make it harder for anyone, whether they are hackers or employees of the company, to:

- Access the IT systems without permission
- Cause damage to the systems
- Steal valuable data
- Negatively impact the revenue derived from customers interacting with the system

The challenge, however, lies in implementing an advanced Zero Trust solution. Although highly effective, it is currently unavailable for purchase as a ready-to-deploy solution. An advanced Zero Trust architecture requires over 30 different technologies and a capable systems integrator to build and configure it. Moreover, organizations already invested in Secure Development Lifecycle (SDL) programs, a secure software release process, and a myriad of cybersecurity tools wonder—what will be different this time?

Benefits of using Zero Trust

Most importantly, though, there is a lack of clarity among organizations on how Zero Trust will benefit them or what significant changes will occur due to its implementation. Dell Technologies is releasing a two-part series to demystify some of the ambiguities surrounding Zero Trust. These papers will help organizations understand how Zero Trust will benefit their business and how Dell Technologies can help enterprises avoid an endless journey by developing an advanced level, validated Zero Trust solution. In this paper, we will discuss the **seven most critical security concerns** and the **benefits of using Zero Trust** to address them:

Prevent unauthorized access

Hackers prefer not to waste time attempting to defeat security controls, as it is difficult. They would rather spend their time stealing login information, which is much easier. Hackers, as the saying goes, do not break in, they log in. APIs, or application programming interfaces, are another way to access an organization's systems; it is how businesses and hardware systems communicate with each other. API access requires credentials, which can be easily stolen and misused. This aspect, called machine-to-machine, Internet of Things (IoT), or event-driven architectures (EDA), is critical as more and more of a system is accessed by other systems. in a Zero Trust environment, API and user access to the systems can be restricted through the use of **multifactor authentication (MFA)**.

[1] Why ransomware attacks are on the rise — and what can be done to stop them, Lynsey Jeffery and Vignesh Ramachandran, PBS News Hour, July 8, 2021, https://www.pbs.org/newshour/nation/why-ransomware-attacks-are-on-the-rise-and-what-can-be-done-to-stop-them

[2] The biggest cyber attacks of 2022, Patrick O'Connor, BCS, The Chartered Institute for IT, September 26, 2022, https://www.bcs.org/articles-opinion-and-research/the-biggest-cyber-attacks-of-2022/

 Copyright © 2023 Dell Inc. or its subsidiaries. All Rights Reserved. Dell Technologies, Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

Curb freedom of movement

Once hackers have gained access to the system, they can often obtain the ability to go anywhere on the network. They use this freedom of movement to hide malware within the system. This approach allows them to attack the system and gain access to increasingly more data. The term for this approach is privilege escalation. Hackers can use several tools to transform a simple set of credentials into superuser credentials. Consider the difference between stealing the key to a single room or the primary key to the entire hotel. An advanced Zero Trust system focuses on **privileged access management** to control how access is granted, how the privileges are used, and how it is revoked when abused.

Reduce the blast radius

Depending on how far it can spread within an organization, cyberattacks can have significant operational and financial consequences as data is stolen, destroyed, or held for payment. Zero Trust focuses on minimizing the impact of a threat or how much an unauthorized user or malware can affect. Several technologies can help with this, but the most important is **microsegmentation**.[3] The idea is as follows: for each authorized user to access the application or data they

requested, a Zero Trust solution automatically creates a **custom network** (using microsegmentation). Consider everyone has their own lane on a highway. This approach limits the blast radius of the attack as the network itself isolates system access to a specific user, application, and data. When the user switches tasks, the isolated network is removed, and a new one is formed. If a hacker attempts to do damage, it will be confined to this microsegment and not spill over to the rest of the enterprise. **Hardly anything can be tampered** with, and **only limited data can be extracted or held hostage**. It is tough to paralyze the entire organization in an advanced Zero Trust system.

Avoid too many on-ramps

The on-ramps must be monitored to control who enters a superhighway. The more on-ramps there are, the more difficult it is to track entry. In the world of cybersecurity, having too many entry points is called an "increased attack surface." Examples include:

- Working remotely from home
- Interacting with customers through an app on their phone
- Connecting distant devices to the main office for remote maintenance

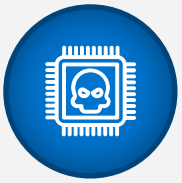
With each of these instances, the number of places a hacker can access the system and cause damage continues to increase. Why? There is less control over the security of remote or noncontrollable devices used in a Bring Your Own Device (BYOD) environment. Why does it matter? **Hackers target vulnerabilities in misconfigured or outdated devices**.

Before allowing a device to connect to an enterprise's network, Zero Trust ensures that it is in a known good state. It is like a "No shirt, No shoes, No service" policy. Before a remote employee's laptop connects to the enterprise network, a Zero Trust implementation will check that it is running the correct operating system version. Or that a remote wind turbine is running the proper software patch level before connecting to the network. People refer to this as **comply to connect**.

---

[3] Microsegmentation definition, Chuck Moozakis, TechTarget, https://www.techtarget.com/searchnetworking/definition/microsegmentation

4 Copyright © 2023 Dell Inc. or its subsidiaries. All Rights Reserved. Dell Technologies, Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.



Safeguard against compromised technology

Advanced hackers will go beyond using poorly configured devices. If possible, they will embed flaws in hardware and software for later use. This is a type of **advanced persistent threat (APT)**, where the threat is embedded in hardware and software even before the user receives it.

An advanced Zero Trust solution can help ensure the integrity of the system's components. For example, a server in the system could be checked to ensure that no component changed from when it was manufactured to when it was installed and running in the environment. This is known as **secure component verification**.[4]

The reliability of the server's boot sequence is also critical.[5] This is a common point of entry for hackers into the systems. To secure and protect these startup or boot sequences from tampering, organizations will need the ability to customize and control them. Zero Trust also employs methods to **safeguard the software's integrity**. The goal is to ensure that the system components are not compromised before use by verifying the **supply chain integrity**.

Eliminate operational risk

Several cybersecurity issues pose operational risks. Systems that have not been updated. Systems using older versions of software with known issues. Updating systems, software, and hardware configurations take time. Things can be overlooked when done manually because everyone is human. Zero Trust emphasizes **continuous monitoring** and **scoring the operational risk** in a system. It emphasizes **automation of updates and maintenance** to reduce risk to the overall operations.

Enhance response effectiveness

Current computer systems are complex; they handle millions of daily transactions involving thousands of devices. Organizations have just as many customers who do business using their own devices. This creates massive amounts of data for highly trained cyber specialists to review and analyze. Cyberattacks occur quickly and always at inconvenient times, with increasing financial impact.

As a result, responding quickly and returning to normal operations is critical. An advanced Zero Trust solution constantly **analyzes both good and bad system behavior**. It uses data from the system to build artificial intelligence and machine learning models that can help respond faster to a cyberattack to increase the completeness of responses. The goal is not to overlook anything, whether it is the users, the devices, the internal equipment, the API access points, or the equipment's integrity. An advanced Zero Trust solution aims to **automate and orchestrate the security response** as quickly as the systems can be attacked.

Dell Technologies can be the industry's Zero Trust integrator

Once organizations see how Zero Trust tackles some of the most challenging cybersecurity concerns, they can take the first steps toward implementing the solution. It is a journey, no doubt, but one with a definite destination. To reach that destination of an advanced level of Zero Trust maturity, the system should support the 45 capabilities with a validated implementation of the 152 activities and associated controls as outlined by the U.S. DoD and NIST. Dell is committed to being the industry's foremost Zero Trust integrator and developing the solution at the Zero Trust Center of Excellence. The validated solution will ease the integration burden, reduce the long-term costs of managing version changes and updates, and manage the supply chain across multiple vendors. In part two, we will cover how enterprises can avoid an endless journey and the value of the validated Zero Trust solution developed by Dell Technologies.

---

[4] Dell Technologies Secured Component Verification, https://www.dell.com/en-us/dt/solutions/openmanage/secure-component-authentication.htm

[5] UEFI Secure Boot Customization, Cybersecurity Technical Report, National Security Agency, September 2020, https://media.defense.gov/2020/Sep/15/2002497594/-1/-1/0/CTR-UEFI-Secure-Boot-Customization-UOO168873-20.PDF

5 Copyright © 2023 Dell Inc. or its subsidiaries. All Rights Reserved. Dell Technologies, Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.