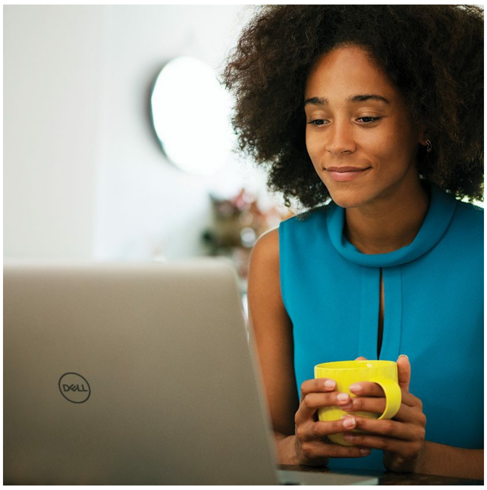


CYBER SECURITY

Using a Zero-Trust Model to Secure a Distributed, Remote Workforce

The recent influx of remote work has challenged traditional security priorities, with employees accessing data from so many multiple locations. Network-based security alone cannot keep up, but a “zero trust” approach might be the answer.
September 8, 2020 | 5 min read

By Rodika Tollefson, Contributor

Today’s workplace is sharply different from a decade or two ago. In many organizations, employees can get their work done from anywhere—and never have to come to the office. This mobile and distributed workforce has prompted businesses to rethink many things, including their cybersecurity, which traditionally focused on securing the corporate perimeter.

The recent influx of remote work has challenged security priorities even more. As more employees access corporate resources and sensitive data from home and other mobile or remote locations, network-based security by itself can’t hold up to the new risks and vulnerabilities.

One approach that helps secure users, assets, and resources—rather than network access—is “zero trust.” It’s a concept built around the idea that intruders are already in the network and no connection can be trusted, even if it originates inside the perimeter.

The main principles of zero trust center around continuous, dynamic authentication and authorization. Essentially, never trust, always verify.

“The world has changed and the environment has changed, and there’s a new paradigm—to focus on securing resources instead of the network,” says Russ Berkoff, president of StealthPath Inc., a cybersecurity company that offers a zero-trust assessment platform and endpoint security. “And COVID-19 has accelerated the need for a dynamic, zero-trust approach that allows companies to protect themselves on multiple dimensions.”

> “The world has changed and the environment has changed, and there’s a new paradigm—to focus on securing resources instead of the network.”
>
> —Russ Berkoff, president, StealthPath Inc.

The Concept of Zero Trust

The idea of zero trust is not new—a Forrester Research analyst coined the phrase a decade ago. Even so, the term is still evolving. Various vendors have different approaches, which vary from using microsegmentation (dividing data centers and cloud environments into zones) or software-defined network perimeters to endpoint agents or gateways.

The National Institute of Standards and Technology (NIST), which creates voluntary, industrywide standards for cybersecurity measures, published a zero-trust framework in August 2020. According to the NIST, the zero-trust principles “are designed to prevent data breaches and limit internal lateral movement.”

The NIST describes zero trust as a set of paradigms that “move network defenses from static, network-based perimeters to focus on users, assets, and resources.” Whether internal or external, no connection is implicitly trusted and must be continuously authenticated and authorized before access to an IT resource is granted.

The work-from-home movement is renewing interest in the model. Especially since a recent Gartner poll found that nearly half of employees will likely remain remote at least part of the time after COVID-19, compared to 30 percent before the pandemic.

“The pandemic has accelerated the push for remote work, and with that you have to make sure endpoints are secure,” says Kathleen Moriarty, security innovations principal with Dell Technologies. “And remote work naturally falls into zero-trust models because each user has to strongly authenticate back to applications.”

Security experts like Moriarty and Berkoff find that zero trust is especially helpful within the context of the “kill chain,” which has become a common term in the industry. The kill-chain framework, created by Lockheed Martin, describes the phases of an advanced persistent threat attack and how the adversary gains lateral movement.

“Once you have zero trust with granular controls, you can detect anomalies,” Moriarty says. “With the kill chain, you want to detect anomalies as early as possible and as quickly as possible [so you can contain the damage]—and the tenets of zero trust help to enable detection early in the kill chain.”

Zero-Trust Architecture

A zero-trust architecture includes both logical and infrastructure components—which ones you use, however, depend on the deployed approach. Logical components may include policy engines and policy enforcement points, threat intelligence, and identity management. Servers, routers, appliances, and other hardware make up the infrastructure components.

Let’s say a user requires access to a resource: The system needs to ensure that not only the user is authentic but the request is also valid.

“The authentication piece is: *Are they allowed to be here?* And the authorization part is: *Are they allowed to be doing this?* And you’re verifying that continuously,” Berkoff says. “This allows you to provide a defense-in-depth posture that thwarts the threat within the kill chain and before it can execute.”

For the process to work, you would need to set up and maintain risk-based, dynamic policies for accessing the resource, and the zero-trust architecture would ensure these policies are consistently and correctly enforced.

Moriarty explains that the components (or modules) of the architecture are isolated from each other, so you can set up controls for each. In the infrastructure, for example, controls would verify the firmware and hardware at system boot, then move on to the operating system, patches and updates, applications, and microservices. Additionally, communication between the components would be continuously authenticated, preventing lateral movement for an intruder already inside the network.

“The attacker would have to survive the re-authentication on any particular module, and as they leap from one module to another, also survive the re-authentication process,” she explains. “You have to make survivability very difficult—it’s about increasing the cost to the attacker.”

> “The attacker would have to survive the re-authentication on any particular module, and as they leap from one module to another, also survive the re-authentication process.”
>
> —Kathleen Moriarty, security innovations principal, Dell Technologies

Implementing Zero Trust

Christopher Gerg with the incident response and forensics company Tetra Defense says zero trust is effective because “it puts the security close to the thing you’re securing.” Since there’s no out-of-the-box solution, one approach he suggests is to start by introducing some of the core concepts of the zero-trust architecture into your existing environment.

“Microsegmentation is a good start—making it so that workstations and services can only talk to the networks and devices that are necessary for business and nothing more. Workstations can’t talk to other workstations and services are only available at the workstations that need access,” says Gerg, who’s Tetra’s chief information security officer and vice president of cyber risk management.

Gerg also recommends using a mechanism for distributing secure configurations to all devices and ensuring the configurations are in place and unchanged. Additionally, he advises adopting robust verification from a “single source of truth, using multifactor authentication, to ensure that people are actually who they say they are.” This is often in the form of something the user knows (e.g. mother’s maiden name), something the user has (e.g. a unique key or mobile phone with a code), or something the user “is” (e.g. facial recognition or fingerprint scan).

“If a threat actor cannot verify the second factor of authentication, then the account remains locked and a potential attack is prevented,” Gerg says.

Moriarty notes that there’s no single answer for everyone. Since many organizations already use some of the zero-trust principles, she recommends first reviewing the current architecture.

“Their first move should be guided by a reasonable transition strategy,” she says. “For some, this means microsegmentation. For others, it may be identity- or network-focused. In the long term, zero trust becomes pervasive.”

She believes that as the concept of zero trust matures, the market and vendor solutions will evolve. In a few years, she says more vendors will deploy infrastructure with zero-trust principles built-in, such as root of trust technology for boot and runtime. That means the focus will shift from endpoints—because they will be more secure—into approaches such as confidential computing (the ability to isolate data, functions, or applications from the operating environment).

In the meantime, the adoption of zero trust is not without its challenges. Berkoff believes one of the biggest hurdles is the paradigm shift among CISOs and CSOs. They would have to go back to the drawing board and re-examine their strategies and security models.

“They’ve been reporting ‘green lights’ all the time, and now all of a sudden you’ve got a model that’s going to show you’re not really green—you’re yellow or even red,” he says. “But the complexity of all the tools they’re using is leaving huge gaps in security, and that’s where zero trust can come in. Zero trust, if it’s done correctly, is disruptive—it should disrupt the activities of the bad guys.”

Subscribe to our weekly email newsletter

Join the Dell Technologies community

Sign Up

Topics in this episode:

Cyber Security , Remote Work

YOU MAY ALSO LIKE

RESEARCH & INSIGHTS

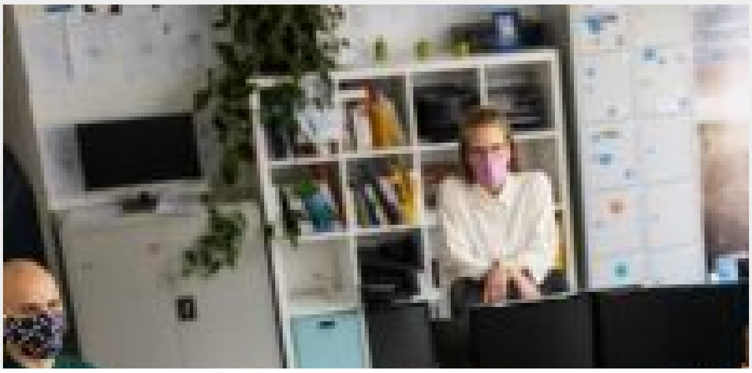
Taking the Pulse: Data Management

Sep 24, 2020 | 5 min read

RESEARCH & INSIGHTS

Four Ways to Build an AI-First Culture

Sep 17, 2020 | 4 min read



ORGANIZATIONAL CULTURE

How Europe Is Leading the Way Back to the Office

Sep 10, 2020 | 5 min read