Why We Need To Apply Zero Trust To Applications

Forbes Technology Council

Sameer Malhotra
FORBES COUNCILS MEMBER

Sameer Malhotra is co-founder and CEO of TrueFort, a former Wall Street tech exec and an expert in IT infrastructure and cyber security.

While the term "zero trust" is often used in cybersecurity circles, the phrase has different meanings to different IT professionals. For some, it is an end-state. For others, it is a set of guiding principles or a framework to apply when augmenting security

Zero trust evolved from the concept of applying specific best practices to network access. These best practices included assigning the least amount of rights to users that would allow them to do their jobs or validating user accounts and applying policies based upon specific criteria. Ultimately, those practices for securing the network layer became somewhat synonymous with the term "zero trust."

However, networks are not the only IT elements vulnerable to attacks and compromises. Many other IT stack components are quickly becoming attack vectors just waiting for a zero-day exploit to compromise them. That raises the question: Can zero trust be implemented in other parts of the enterprise security estate? The answer is a resounding yes—yet perhaps not in exactly the same way.

For example, take enterprise applications, which are a top attack vector for unauthorized access by data-seeking hackers. Applications are normally accessed after a user is authenticated to the network. Yet network user authentication alone does not offer full protection against today's range of threats. Enterprise applications are susceptible to numerous other attacks such as SQL or code injection, lateral movement, API weaknesses and many more. Simply put, just because you are using a zero-trust solution for network access does not mean enterprise applications are properly protected.

However, extending zero trust to application environments proves to be somewhat more complex than applying it to the network. Applications and their workloads are more numerous, dynamic and complex than networks.

They perform many different functions and have dependencies on data sources and potentially other applications. In other words, applications are not always static and can take on numerous different roles depending upon the use case.

Protecting applications means rethinking how they are accessed and how they communicate with each other, share data and authenticate users. In fact, applying zero trust to application environments often requires thinking a little differently. Instead of looking at applications strictly from a code vulnerability perspective, cybersecurity pros need to understand the acceptable behavior of the applications and, ideally, assign a behavior-based security identity to them that determines their entitlements.

Accordingly, establishing application-centric zero trust means first analyzing each application's behavior to verify it is only performing appropriate functions and only interacting with the needed binaries and data sources. This analysis can be used to build a library of behavioral parameters for each application and, subsequently, establish a security identity for it.

In this context, applications have their own trust footprint, and permissions can be limited to only what is necessary for the app to function (zero trust). Any type of attack, such as code injection, will fall out of the normal range of behavior and trigger an alert or shut down the application session to block any unauthorized activity or access to restricted resources.

TO GET STARTED WITH APPLICATION-CENTRIC ZERO TRUST, YOU'LL NEED TO:

- Discover and catalog all of your applications.
- Monitor their behavior over time to create a baseline of expected and authorized activity.
- Eliminate any security risks identified as part of the behavior profiling process (i.e., unnecessary permissions, excessive entitlements, risky dependencies, etc.).
- Create security policies that enforce a zero-trust stance on application activity so only authorized behavior is allowed.
- Push out alerts to control points when a policy is violated so corrective action can be triggered to remediate threats.

Ultimately, cybersecurity professionals want to protect not only the network but also data, identities and applications to reduce the attack surface. By applying the concepts of zero trust to applications, cybersecurity teams can achieve the goal of more fully protecting the enterprise from risks, preventing brand damage and avoiding business interruption.

By applying the concepts of zero trust to applications, cybersecurity teams can achieve the goal of more fully protecting the enterprise from risks, preventing brand damage and avoiding business interruption.

ABOUT TRUEFORT

TrueFort reduces business risk for security-focused enterprises striving for zero or lean trust application environments. Our innovative and uniquely application-centric Fortress platform delivers comprehensive realtime cloud-to-the-ground insight, protection and automated response with patented machine intelligence and a single or bring-your-own agent. Fortress overcomes the application security blindspots inherent in legacy infrastructure-centric tools, providing unparalleled visibility and protection for applications in on-prem, hybrid and cloud environments and for security teams across the enterprise. Fortress speeds response times, minimizes the blast radius of compromises, prioritizes resources, and enhances application risk posture.

TRUEFORT

3 West 18th Street
Weehawken, NJ, 07086
United States of America

+1 201 766 2023
sales@truefort.com

TRUEFORT.COM