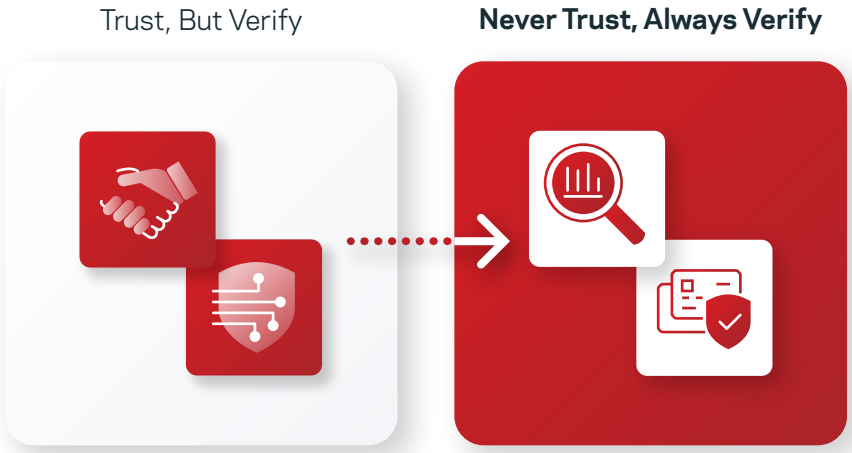
Zero Trust Fundamentals

In our industry, a large amount of confusion has developed around the definition of Zero Trust, what it is and what it isn't. Problematic misconceptions—like that Zero Trust can be bought with a single product—are spreading wildly, which can lead to serious vulnerabilities and consequences for ransomware resiliency.

What does Zero Trust really mean?

Let's start by pulling the textbook definition. The Zero Trust security model—also known as Zero Trust Architecture, ZTA, or ZTNA—describes a "never trust, always verify" approach to the design and implementation of IT systems. The Zero Trust model was coined by Forrester Researcher, John Kindervag, in 2010 as a significant departure from the traditional security practice of "trust, but verify."



Expanding further, Zero Trust is an approach, meaning that it is not just one single thing or a feature. It is a practice, framework, mindset, or philosophy that encompasses not trusting any devices—or users—by default, even if they're inside the corporate network. This concept can include a large number of technologies, products, practices, and features that are built not only into the products but also into the culture and processes of a company. A Zero Trust strategy is based on continuous evaluation and verification of network access, ensuring that access is secure and authorized, every time and for every single access. We are talking about more than just users, but devices and workloads too.

But Zero Trust is much more than the IT team or an IT charter. For a Zero Trust approach to be successful, the entire company must be aligned. Corporate culture, company-wide processes, employee education, and a security mindset must be paramount throughout the entire organization for Zero Trust to work.

Security teams across the organization must agree on priorities and align on access policies. Every single connection across the business—from data, to users and devices, to applications, workloads, and networks—must be architected according to the Zero Trust strategy, with the ability to evolve and refine as needed. That means there must be an organization-wide commitment. A Zero Trust architecture can include everything from identity and access management, data, and encryption to devices, workloads, networks, and endpoints, but also includes monitoring with analytics and visibility as well as new technologies like artificial intelligence (AI), machine learning (ML), automation, and orchestration. Identity access management includes multi-factor authentication (MFA), which confirms user and device identities, and dual approval confirms whether users are doing "what" they are supposed to be doing.

Why is Zero Trust such a hot topic right now?

One word: ransomware. Cybersecurity is top of mind worldwide today. With the threat of ransomware becoming more prevalent compounded by the challenges of securing a remote workforce, Zero Trust has been elevated out of the IT team and into every boardroom across the globe. Although incredibly important, frontline security tools and technologies alone are insufficient.

Adoption of a company-wide Zero Trust mindset has proved to help reduce the risk of a devastating attack. If a breach does happen, it then significantly reduces the attack surface or what is often referred to as the "blast radius" by providing multiple layers of security that minimize impact. For example, once in your systems, cybercriminals often move across your environment searching for business-critical data, confidential information, and backup systems. Building strong identity and access management controls, privilege controls, hardening, and secure hardware on Zero Trust, however, prevents access to these areas. By continuously monitoring and validating users and devices, Zero Trust flags threats immediately and stops them before they can cause maximum damage. Zero Trust is even more crucial today where environments are multi-cloud, hybrid, and multi-identity with both legacy and software as a service (SaaS) apps.

How does Veritas help?

We act as a trusted resource to help any organization on its Zero Trust journey. The Zero Trust practice has been part of our corporate culture for years—a huge advantage of having been conceived while we were still part of a security company. Everything we engineer is built on that strong security foundation. Veritas products have embodied multiple layers of Zero Trust principles for years and are architected to enhance the Zero Trust architecture for all our customers.

Check out this helpful white paper on our immutable and indelible storage titled, "Secure by Default."

Actions to take ASAP

- **Adopt immutable and indelible storage**
- **Institute identity and access management (IAM)** (MFA and role-based access control for both users and machines)
- **Encrypt data** both inflight and atrest to reduce data exfiltration leverage (use data loss prevention software)
- **Limit access to backups** (no one with access to primary data should also have access to Backups)
- **Implement security analytics** to monitor for and mitigate malicious activity

We've got your back.

The harsh reality of 2022 is that data breaches are inevitable. Adopting the Zero Trust "never trust, always verify" mantra is paramount. If you need advice or help strengthening your Zero Trust strategy or bolstering your cyber-resiliency, we can help. We get it and we are eager to partner with you. Ready to talk? Request a call from us.

About Veritas

Veritas Technologies is a global leader in data protection and availability. Over 80,000 customers—including 87 percent of the Fortune Global 500—rely on us to abstract IT complexity and simplify data management. The Veritas Enterprise Data Services Platform automates the protection and orchestrates the recovery of data everywhere it lives, ensures 24/7 availability of business-critical applications, and provides enterprises with the insights they need to comply with evolving data regulations. With a reputation for reliability at scale and a deployment model to fit any need, Veritas Enterprise Data Services Platform supports more than 800 different data sources, over 100 different operating systems, more than 1,400 storage targets, and more than 60 different cloud platforms. Learn more at www.veritas.com. Follow us on Twitter at @veritastechllc.

VERITAS

2625 Augustine Drive
Santa Clara, CA 95054
+1 (866) 837 4827
veritas.com

For global contact information visit:
veritas.com/company/contact

V1531 04/22