Strengthen Your Security with Zero Trust

Protecting your business from cyberthreats requires a comprehensive, multilayered approach. Zero trust principles enforce a *never trust, verify everything* strategy as a key element of defense. Taking the right measures to secure your data and systems can help protect against malicious online activity.

Zero trust operates on the philosophy that any attempt to access critical data must be verified and authorized, regardless of where it originates. Even if a hacker succeeds in accessing a system, zero trust can prevent their ability to cause significant damage. It decreases the attack surface through segmenting and limiting access, preventing attackers from moving laterally in the network. Zero trust can help reduce cybersecurity costs by strengthening compliance with data security regulations.

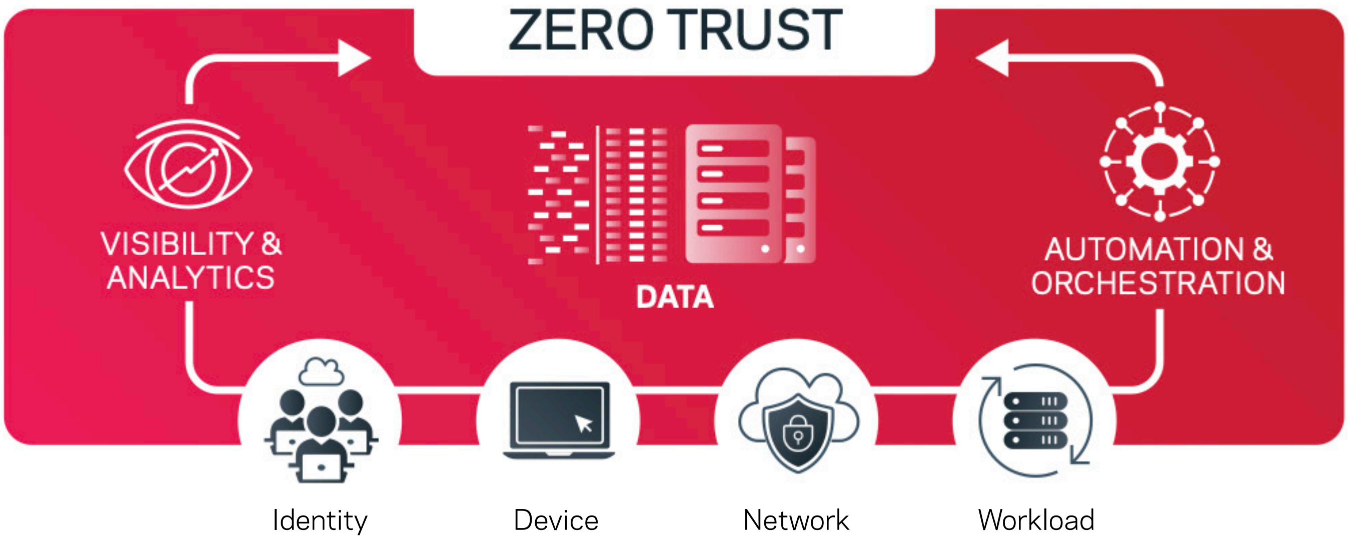
Zero trust is not a quick fix. Securing your data requires consistent effort. With proper integration and diligence, you can protect against malicious attackers and limit the amount of damage that can be inflicted if they manage to breach your defenses. Use this approach across your infrastructure to guard your data, no matter where it resides.

Roadblocks to Zero Trust

It is common to be anxious about how to deploy a zero trust architecture. Your organization wants to limit disruption, maintain productivity, and keep a solid ROI. You may be discouraged from implementing and integrating new architecture.

Change in Thinking

The first thing to consider is the pathway to cyber resiliency. Backup and recovery is a team sport. For zero trust to be successful, the entire company must align. Corporate culture, company processes, employee education, and a security mindset must be paramount through your entire organization for zero trust to work.



Ongoing Investment

Zero trust is a complex model that requires significant effort. Implementation can be expensive, especially if you need to upgrade technology. It requires a change in the way your organization thinks about security and is challenging from a typical perimeter-based security model. Implementation and management may be costly up front, because your workforce will need to build and apply new skills. You also might have to upgrade legacy technology, which may require a budget you weren't prepared to spend.

Zero trust bolsters networks and safeguards against malicious hackers. Restricting access to critical data, applications, infrastructures, and your network makes it difficult for attackers to shift and move laterally within the network. With improved visibility into potential threats, you can reduce your response time to threats. As your security posture strengthens, you can reduce the impact of a breach and improve the efficacy of your response, which will decrease the financial impact of downtime.

Risk Mitigation

Use zero trust principles to ensure your data is secure. Start by creating layers of checks such as authentication, authorization, and constant verification. AI-powered tools watch for unusual activity, while AES encryption helps protect the data in transit and at rest. These steps are necessary to stop attackers from gaining access using stolen passwords.

Reduced Reliance on Human Interaction

Preventing data loss and securing valuable resources is the goal of a strong zero trust architecture. This comprehensive approach includes ongoing observation, authentication, and re-verification to ensure that all resources remain secure.

Infrastructures are diverse. Tasks such as anomaly detection and malware scanning become tedious and overwhelming if they depend on significant staff monitoring. Hackers come in quietly: The first indicators of their presence may be odd behavioral patterns or the number of changed files in a backup. If unauthorized users access critical data, machine learning and AI can alert IT staff to the indicators for closer inspection to isolate and take action.

Increased Efficiency

As your zero trust security model matures, the more effectively you can support regulatory compliance efforts. You can increase efficiency by automating security tasks. Automation, in turn, can reduce spending related to compliance tasks and processes. Meanwhile, increasing data visibility will produce greater insights and simplify audits of your data.

Launching a Zero Trust Strategy

While there is no *off-the-shelf* zero trust product, there are concrete steps that you can take.

Veritas provides solutions to help you identify and categorize the importance of essential data, processes, and services. Ensure that you use zero trust principles across your entire infrastructure, including hybrid environments. You should fill your zero trust strategy with technologies and solutions that are secure by default. We also help you ease the transition for IT teams struggling to support updates and changes by helping automate inefficient processes and strengthening systems in place.

The CISA Zero Trust Maturity Model provides a practical phased strategy for implementing zero trust. It allows you to allocate resources efficiently, minimize disruptions, and ensure ongoing progress by dividing the implementation process into multiple phases. By harnessing the power of maturity models such as the one from CISA, you can:

1. **Measure Security Posture:** Assess your current security posture and identify potential weaknesses.
2. **Set Clear Objectives:** Create achievable goals and establish a practical timeline for implementation.
3. **Prioritize Investments:** Allocate resources effectively by focusing on critical aspects of zero trust security.
4. **Monitor Progress:** Use actionable metrics to track progress and quantify successes.
5. **Foster Continuous Growth:** Encourage ongoing assessment, adaptation, and education to stay ahead of evolving threats.

Be sure to reinforce zero trust policies and safeguards throughout the project. Start your plan and policies for successful implementation with a segmented network and a unified platform. Construct data flows that you can strictly monitor and protect vulnerable gateways and access points. Compile reports that pinpoint behaviors that need optimization.

Prevent Data Loss

Insights: A secure environment requires you to understand your current security posture. Identify what assets are sensitive and what you need to protect. Good insights will show you where and what users are trying to access, and whether they have permission. Conduct a comprehensive assessment of your organization’s security posture, policies, processes, and technology to find gaps and prioritize remediation based on risk and objectives.

Integration: Solutions with built-in integrated and automated orchestration and management give you better visibility and control over analytics of user behavior and traffic. With SIEM/SOAR, you can show potential threats and investigate security incidents to strengthen security posture. You can also automate security tasks for more efficient threat hunting and incident response on backups. Integrated AES-encryption and STIG-hardened appliances also improve security posture and reduce risk. Create and outline the steps needed for comprehensive protection, and identify if you need partners to reach your goal.

Isolation: The zero trust model requires critical isolation with identity and access management (IAM) to protect micro-segmented areas of your network. Micro-segmentation divides the network into discrete sections and makes it difficult for attackers to shift and migrate around. With proper authentication and authorization in place, you can guard against unauthorized access and accidental disclosure of critical data.

Strengthen Cyberdefenses

Intelligence: Continually scan your network, devices, and applications to detect anomalies. Immediately restrict access when irregularities arise, then set up an automated process to track patterns for further investigation. Keep a close watch on the metrics that matter most, so you can stay ahead of security threats.

Immutability: If bad actors infiltrate the system, immutable vaults reduce the risk of contamination of critical systems and data. Incorporating immutable storage into your environment ensures that you have a clean copy of data to recover from, in case of a cyberattack. Additionally, immutable storage can improve your regulatory compliance.

Have Confident Recovery

Bolster your data security and combat cyberthreats with Veritas. Our comprehensive suite of tools is designed to provide intuitive solutions to meet the unique needs of your organization, automating manual processes and enhancing operational efficiency. Arm yourself with the confidence to take proactive steps against cyberattacks and safeguard your organization’s future. Veritas makes it simple — eliminate guesswork and protect against vulnerabilities.

Creating a zero trust security plan may seem difficult. It’s an approach that involves verifying trustworthiness step-by-step, instead of giving people and processes immediate access. Although it’s complex, following the right strategy and tips can help you set up a strong cybersecurity shield. Invest in zero trust security to strengthen systems and gain peace of mind.

Veritas provides a path to reduce the complexity and cost of building a strong zero trust posture. We engineer everything on an intrinsically strong foundation. Our products and solutions embody multiple layers of zero trust checks and balances, while adhering to zero trust principles. We offer easy-to-integrate solutions that will significantly boost operational efficiency and comprehensive resiliency. Our goal is to remove manual processes and guesswork, while equipping you with the tools to close potential gaps.

Our cutting-edge technology combines automation, machine learning, and AI to boost your resilience, while offering comprehensive insight and data analysis to find optimization and development opportunities.

Don't leave your company vulnerable. Get started with this Seven Step Checklist to improve your security posture, and share these actionable tips with your team. Visit our cloud data security page for more ways to strengthen your cybersecurity strategy.

About Veritas

Veritas Technologies is the leader in secure multi-cloud data management. Over 80,000 customers—including 91% of the Fortune 100—rely on Veritas to help ensure the protection, recoverability and compliance of their data. Veritas has a reputation for reliability at scale, which delivers the resilience its customers need against the disruptions threatened by cyberattacks, like ransomware. No other vendor is able to match the ability of Veritas to execute, with support for 800+ data sources, 100+ operating systems and 1,400+ storage targets through a single, unified approach. Powered by Cloud Scale Technology, Veritas is delivering today on its strategy for Autonomous Data Management that reduces operational overhead while delivering greater value. Learn more at www.veritas.com. Follow us on X at @veritastechllc.

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

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