www.valoremreply.com

REPLY VALOREM

A Guide to the ZERO TRUST SECURITY JOURNEY

PRINCIPLES AND STRATEGIES
TO HELP YOU PREVENT RISK AND PROTECT YOUR DATA

The proliferation of cloud applications, continued move to hybrid, remote work for millions of workers, and frontline enablement initiatives are redefining security boundaries for enterprises today. Rather than manage a small number of devices on a corporate perimeter and protecting network access with VPNs, IT teams are now faced with a much more complex task: managing both home and corporate networks, cloud apps, and multiple devices.

At the same time, cyberattacks and data breaches are becoming more common and more sophisticated, making security a bigger challenge than ever. According to the ***Identity Theft Resource Center (ITRC)*** [i], more than 1,291 data breach incidents were reported through September 30, 2021, a number that was 17 percent higher than all disclosed breaches in 2020. Ransomware attacks, meanwhile, hit 37 percent of businesses in 2021 [ii], and phishing incidents nearly doubled in frequency from 2019 to 2020.

For enterprises, the consequences of these attacks can be devastating. Security firm McAfee reported that the global cost of cybercrime was nearly $1 trillion in 2020[iii]. Companies on the receiving end of cyberattacks also suffer damage to their brands and potentially lost customers.

3 KEYS TO MOVING BEYOND **"CASTLE AND MOAT"** IT SECURITY

valoremreply.com +1 (855) 864-9929 info@valorem.com

3 KEYS TO MOVING BEYOND "CASTLE AND MOAT" IT SECURITY

Some organizations are fighting back against cybercrime by implementing a zero trust security model. Zero trust refers to a perimeterless security approach that stipulates that no devices should be trusted.

However, adopting a zero trust model can be challenging in traditional IT, where security is built for a world with clear boundaries between the inside and outside of the network. This "castle and moat" approach, used by organizations that have not yet started a zero trust journey, relies on on-premises identity features with static rules and some single sign-on (SSO) capabilities. Organizations using the castle and moat model have limited visibility into device compliance, cloud environments, and logins. The result is a flat network infrastructure characterized by broad risk exposure.

A zero trust framework that includes cloud-based identity solutions, multi-factor authentication, and cross-environment SSO is more suitable for today's workplaces. To successfully adopt this kind of zero trust framework, organizations should follow these principles:

VERIFY EXPLICITLY

Always perform identity verification and authorization based on all available data points, including user identity, location, equipment health, service or workload, data classification, and exceptions.

USE LEAST-PRIVILEGED ACCESS

Restrict user access through timely and appropriate access (JIT/JEA), risk-based adaptive policies, and data protection to help protect data and productivity.

ASSUME BREACH

Minimize blast radius and segment access, verify end-to-end encryption, and use analytics to gain visibility, drive threat detection, and improve defenses.

SIX PILLARS
OF ZERO TRUST

A zero trust IT security model should be part of an integrated approach that includes the entire end-to-end digital estate. This is accomplished by following these six IT security pillars:

Identity

Because of the proliferation of devices, it is essential to verify that only the employees and devices that have been granted access to corporate resources can access them.

Endpoints

With a broader range of endpoints to manage, organizations need to assess the security compliance of all hardware, including IoT systems on the edge of the network.

Applications

IT teams need to ensure reliable access to all applications, including on-premises and cloud-based apps, while also maintaining access control.

Infrastructure

Increasingly complex IT infrastructures include physical and virtual servers and containers and microservices, making permissions management and configuration critical.

Data

Data must be protected at all times, and organizations need to classify, label, and protect their data, wherever it resides, to stop inappropriate sharing and insider risks.

Network

Organizations often lack adequate network security perimeters and threat protection tools. Moving beyond traditional network security can be a way to solve the problem.

3 TIPS TO ACCELERATE YOUR ZERO TRUST JOURNEY

Fully implementing a zero trust framework requires the adoption of all of the above guiding principles and pillars. However, getting there does not happen overnight. It is a unique journey for each organization, depending on your specific needs and current state. Here are some recommendations to make that journey as smooth and painless as possible:

PROTECT AGAINST ACTIVE THREATS

Stopping active threats is an important first step in the journey. This includes taking steps to prevent zero-day threats, which haven't been seen before, as well as stopping ransomware, intrusions, and data leaks.

UTILIZE SECURITY FULLY

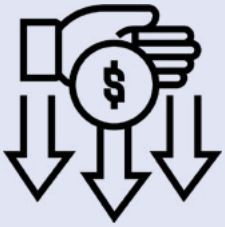
A full analysis of your IT environment can often reveal what's missing from your security approach. Does your organization have shadow IT, involving the use of systems or applications without IT approval? Is frontline enablement a key company initiative? Consider the risk involved.

SECURITY PROCESSES ENSURE SECURITY PREPAREDNESS

How easy is it for your organization to manage IT? More specifically, how easy is it to comply and prove compliance and identify the root cause of security problems? To simplify management and compliance, make sure you have strong governance, legal compliance, and escalation preparedness

MAKING SECURITY
EFFICIENT AND COST-EFFECTIVE

Implementing zero trust throughout your organization should ultimately make security management more efficient and cost-effective. This is accomplished through:



Consolidating security solutions, which reduces TCO by eliminating hardware, licensing costs, and other fees.

Using security data more effectively, which increases overall security.

Enabling automation and orchestration through technologies that increase both speed and compliance.

OUR APPROACH TO ZERO TRUST

Security is a core tenant of Valorem's approach to digital transformation and innovation. Our strategy for implementing a zero trust framework is designed to enable and empower our clients. We provide a customized zero trust security solution for each client, and we are committed to meeting organizations where they are in their journey, while helping them progress through that journey. Using detailed analysis, clear recommendations, and a strategic roadmap, we help organizations solve their most complex security challenges and prepare to face evolving threats head on.

Our process always follows these steps:

1	**UNDERSTAND**	We gather data to learn about the current state of your IT security capabilities and discover where you are on the zero trust journey.
2	**ANALYZE**	Based on our learnings from the first step in the process, we develop insights and identify opportunities to make improvements to your security approach.
3	**RECOMMEND**	By prioritizing remediation items and longer-term implementation goals within the context of your business goals, we can recommend the most effective next steps.
4	**ACCELERATE**	We help you follow through on the remediation tasks we have identified and then help implement new security features, eliminating third-party tools where possible.

Based on extensive experience and deep cloud security expertise, our experts have developed a security service framework that can be customized to your current state and help you reach the next phase of your zero trust journey more quickly and efficiently. A typical journey may include an executive strategy and road mapping workshop, a proof of concept, pilot project, and ultimately full deployment of your custom zero trust solution.

MICROSOFT 365
ZERO TRUST SOLUTIONS

We use leading-edge Microsoft solutions to help organizations build foundational zero trust security capabilities. These solutions include:

MICROSOFT 365 E5

Microsoft 365 E5 integrates best-in-class productivity apps with advanced security, compliance, voice, and analytics to help prevent cyberattacks and protect and govern data.

AZURE ACTIVE DIRECTORY

Microsoft Azure Active Directory (Azure AD) is an enterprise identity service that offers SSO and multi-factor authentication to help protect users from 99.9 percent of attacks.

MICROSOFT DEFENDER FOR ENDPOINT

Microsoft Defender for Endpoint provides endpoint security for Windows, Linux, Android, and macOS to help rapidly prevent attacks.

MICROSOFT ENDPOINT MANAGER

Microsoft Endpoint Manager combines services such as Microsoft Intune, Configuration Manager, and Windows Autopilot to help keep data secure, both in the cloud and on-premises.

MICROSOFT DEFENDER FOR CLOUD APPS

Microsoft Defender for Cloud Apps is a comprehensive solution that increases visibility into cloud apps and services by enabling you to control and limit access while enforcing compliance requirements on cloud data.

MICROSOFT SENTINEL

Microsoft Sentinel is a cloud-native security information and event management (SIEM) solution that delivers intelligent security analytics and threat intelligence across the enterprise.

ACCELERATE YOUR JOURNEY TO ZERO TRUST SECURITY

Implementing a zero trust framework is a journey, requiring a process that includes guiding principles, detailed analysis, clear recommendations, and a strategic roadmap. No matter where you are in your zero trust journey, we can help you advance your security posture, reduce risk and make your environment more secure.

Using the right combination of tools for your unique environment, we help you harden security by taking an integrated and holistic approach to protecting your digital assets. Our offerings include:

CLOUD SECURITY SOLUTION ACCELERATOR

We engage clients to rapidly adopt the latest Microsoft security technologies by using trial licenses to leverage data in their actual environment.

Request more information here.

SECURITY ASSESSMENT

We evaluate security readiness, identify potential risks and make recommendations for modern security solutions. Our assessments include product and licensing recommendations for solutions such as Microsoft 365 E5 and Microsoft Endpoint Manager. .

Request more information here.

MANAGE AND INVESTIGATE RISK

We support clients as they manage and investigate risk by implementing threat management tools like Microsoft Defender and Microsoft Sentinel.

Request more information here.

PROTECT SENSITIVE DATA

We help clients protect their most sensitive data by implementing sensitive data policies, encryption, usage, and user policy understanding. We build a roadmap for Microsoft Information Protection implementation and execute and support deployment and training.

MODERNIZE SECURITY AND ESTABLISH A ZERO TRUST FOUNDATION

By building a modern security and identity infrastructure, we help clients create aa foundation for zero trust. This includes migrating to Azure Active Directory and implementing Privileged Identity and Access Management and Conditional Access.

Request more information here.

i *Number of Data Breaches in 2021 Surpasses All of 2020. ITRC, 2020.*
ii *Ransomware Statistics, Trends, and Facts for 2020 and Beyond. Cloudwards, 2020.*
iii *The Hidden Costs of Cybercrime. McAfee, 2021.*

Our experts can help you to **Guide to the Zero Trust Security Journey**

Click here to learn more!

valoremreply.com +1 (855) 864-9929 info@valorem.com