ZOHO for Enterprise

Securing the evolving workspace through zero-trust architecture

Security series, Q3 2023

As new security threats challenge dispersed workforces, zero-trust architecture offers a way to protect vast amounts of data without becoming a roadblock to legitimate use.

Introduction

Enterprise infrastructure and security are operating in a different paradigm from even two or three years ago. Workforces are more dispersed across remote locations and satellite offices, data is more decentralized and accessed through more self-service BI tools, and bring-your-own-device (BYOD) policies are giving employees more flexibility than ever in how they interface with the tech that supports their work. Unfortunately, this opens organizations up to more dangerous security threats as cybercrime attacks become more complex and devices that employees use for work lack the security measures to hold up against them.[1]

[1] McKinsey, 2021

> “
>
> **98%**
>
> *of organizations are concerned about insider threats.*
>
> [World Economic Forum, 2022]

Experts agree that the vulnerability of these decentralized workplaces is only going to become more pronounced as time goes on, but forcing employees back to office premises full time has turned out to be challenging and often counterproductive for productivity and morale. For many companies that have shifted their hiring focus to remote employees, a return to a single secured workplace isn’t even feasible. Other large organizations have branched out into hub-and-spoke office models that simply don’t have the on-premise IT infrastructure to keep up with the rise in cybercrime.

To maintain a defensive stance in the face of these threats, the cybersecurity industry has shifted toward solutions that are:

- **Scalable with enterprises of all sizes**
- **Effective no matter how dispersed a workforce is**
- **Capable of handling increasing volumes of data**

This is where zero-trust architecture (ZTA) comes in. A security framework that enables zero trust means all people and processes are assessed and verified with the same strictness that an on-premise office network would employ. For employees, customers, and external users, as well as devices, networks, applications, and even data sets, zero trust offers protection against external and internal threats equally. This allows companies to have a dispersed workforce and self-service BI infrastructure without putting the organization at greater risk.

Cybercrime's prevalence

1 out of 3 organizations experienced a cyberattack in 2019, up 36% from the previous year.

[McKinsey, 2022]

There were approximately $8 trillion in annual losses from cybercrime in 2023. Costs will hit $10.5 trillion by 2025.

[Cybersecurity Ventures, 2022]

How ZTA mobilization combats insider threats

When looking to implement zero trust, many organizations turn inward toward their applications and data first. The larger the enterprise, the more data is being moved around, the more employees are transitioning in and out of roles, and the more applications are being requested or

built in-house. And for all of this change, the visibility over it is very limited—to the point where 98% of organizations are concerned about insider threats.[2]

The first ask of ZTA is for organizations to understand this risk through a detailed asset inventory, where IT and data teams work together to assess:

- **What in-house and third-party applications are being used**
- **Who has access to those applications, and on what devices**
- **What data is stored within those applications**
- **What networks those apps rely on to interact with company assets**

This inventory gives security teams a clear picture of all the assets that have to be protected, allowing them to segment their various apps, data sets, and solutions into different categories for easier risk assessment and tracking. It also gives leadership a greater degree of data visibility at the org-wide level, offering them the opportunity to cut applications that are no longer serving the company or to consolidate redundant data assets into a single location. While time-consuming to keep updated, these inventories serve as the foundation for ZTA and help keep it robust, flexible, and scalable.

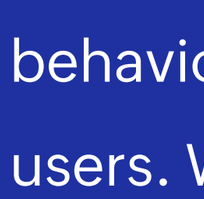
> *Zero-trust is projected to be a **$52 billion** industry by **2026.***
>
> [CNBC, 2022]

How ZTA protects users while increasing data accessibility

Most cybercrime stems from human error. In phishing scams, for example, hackers gain access to stolen credentials via email or text message blasts, taking advantage of users who aren't skeptical enough of the messages they're receiving. Identity Access Management (IAM) is pivotal to blocking these attacks and securing an organization's applications and data to a degree that's compatible with ZTA. IAM includes familiar multi-factor authentication methods like biometrics, access codes, and one-time passwords, which all play important roles in shaping a strong zero-trust

[2] World Economic Forum, 2022

architecture. But machine learning and AI have paved the way for even more nuanced ways of applying IAM for zero trust. By analyzing keystroke patterns, geographical locations, and network connections, security systems can automatically generate dynamic digital identities for users. When a user tries to access protected assets, their credentials are compared to the minimum permissions that an IT or security team has set, and the data they are transmitting is compared to their digital identity on file, triggering additional layers of security as needed.



Quantifying risk

Taking advantage of AI and machine learning in a zero trust ecosystem requires a powerful data analytics platform that can house, interpret, and act on key behavioral patterns among users. With augmented data analysis in Zoho Analytics, these behavioral patterns can be used to generate risk scores whenever a user takes a certain action, such as a login attempt. Additional security measures can then be triggered based on that score, ensuring that corporate assets are protected to as granular a level as your security team desires.

On the back end, this ensures that applications and data are more protected, but for employees, this system actually accelerates their access to the data they need. The asset inventory enables IT or data governance teams to give individual users roles and permissions that outline what they can access, when, and by which means. By automating the creation of these digital identities as part of a larger ZTA ecosystem, access-enhancing features like SSO can be enabled for remote workers or dispersed offices without increasing the risk of internal threats or the exposure to novel cyberattacks.

How microsegmentation encourages clean data protocols

Cloud storage and cloud-based software has made another feature of ZTA all but essential: microsegmentation. Traditional network segmentation secured data flowing in and out of a perimeter-based network, as in a data center or an on-premise intranet platform. But modern enterprises are now dealing with more data than those perimeter-based systems can handle.

The cloud has expanded the capabilities of organizations to manage larger volumes of data, but the borders on cloud-based network environments are much harder to define and control. In the cloud, data can be created, manipulated, shared, and stored without ever leaving a single network, even if that data is being drawn from thousands of data centers across the world. Microsegmentation breaks that massive network up into parts, protecting corporate assets at the workload level instead of relying on a physical perimeter, and because it targets workloads, it can be used to add better security to both single and multi-cloud environments.[3]

Microsegmentation requires specific data classifications in order to isolate individual workloads and allow a cybersecurity team to put firewalls, intrusion and detection tools, and other security measures in place around them. One benefit of this focus on data classifications is that it encourages cleaner data. Not only is there more oversight on data duplications and errors because of the asset inventory, but standardization protocols allow for data to be classified more clearly, which in turn leads to more secure microsegments. The end result is a feedback

[3] TechTarget, 2022

loop that shifts organizational processes closer to zero trust by design, where everything from the way network architecture is built to the way software applications are developed is in line with ZTA right from the start.

Zero-trust adoption

Organizations with fully realized ZTA implementations are seeing significant security and cost improvements, and zero trust is projected to be a $52 billion industry by 2026.[4] Still, full adoption is slow across the board. While 72% of organizations report that they are somewhere in the process of adopting zero-trust models, only 6% report that they have fully implemented ZTA.[5] This reflects both the positive and negative sides of organizational transformation: effective change requires a long view and a deliberate process with all stakeholders at the table, but the security benefits and cost savings of that change won't be realized until the process is complete. For organizations that are planning to implement ZTA or still early in the process, this can mean looking for creative ways to maximize the protection offered by every resource and stage along the way to a full implementation.

Every step toward zero trust is valuable

As cybercrime evolves, the vast quantities of data that enterprises are contending with is becoming a greater risk. Without robust and scalable solutions to address that risk, any value that data brings is diminished by the urgent security needs that come along with it. Zero-trust architecture offers a powerful layer of protection against malicious data access, but implementing it is a resource-intensive challenge, especially when global labor markets are short of nearly 3.4 million cybersecurity professionals.[6] This challenge has led more organizations to conduct regular gap assessments and

[4] CNBC, 2022 | [5] CyberTalk, 2022

[6] Fortune, 2022

improve their overall security documentation process, reducing the burden on their existing cybersecurity teams. Using that extra bandwidth to invest in zero trust can have compounding benefits for organizations in the long run, even if a full implementation is infeasible.

Each step in the process of implementing zero trust offers unique benefits for the challenge of getting more value from data. The first stages of ZTA planning can bring clarity to an organization's data assets by motivating a complete and continuous inventory. From there, identity access management and microsegmentation ensure that the right users are accessing the data they need at the right times, and that the network sessions they're using are siloed from the rest of the organization's assets. As these systems feed into each other, it lays the groundwork for a more secure, more flexible data management process that can empower employees and stakeholders without increasing the organization's exposure to novel security threats.

Why Zoho for Enterprise?

Proven software, customer commitment, tremendous value.

Scalability & Reliability

Zoho for Enterprise reduces the cost of infrastructure, unifies existing apps, and solves complex business problems for increased enterprise fitness, resilience, and scalability.

Customization & Extensibility

Through granular customizations and powerful in-house developer platforms, Zoho lets you orchestrate workflows, streamline data management, and deploy world-class solutions at scale.

Security & Privacy

From owning our own data centers to GDPR compliance features, Zoho enables enterprise organizations to focus on core business priorities, rather than data management.

Enterprise Services

From data migration to consultation and implementation, our team is armed with the in-depth product knowledge and industry expertise to meet your unique technical requirements.

Are you ready to transform your organization?

We're here to help. Have a 15-minute, no-obligation call with one of our **Business Architects** to get all your questions answered.

Find us at **zoho.com/enterprise.** | ZOHO for **Enterprise**