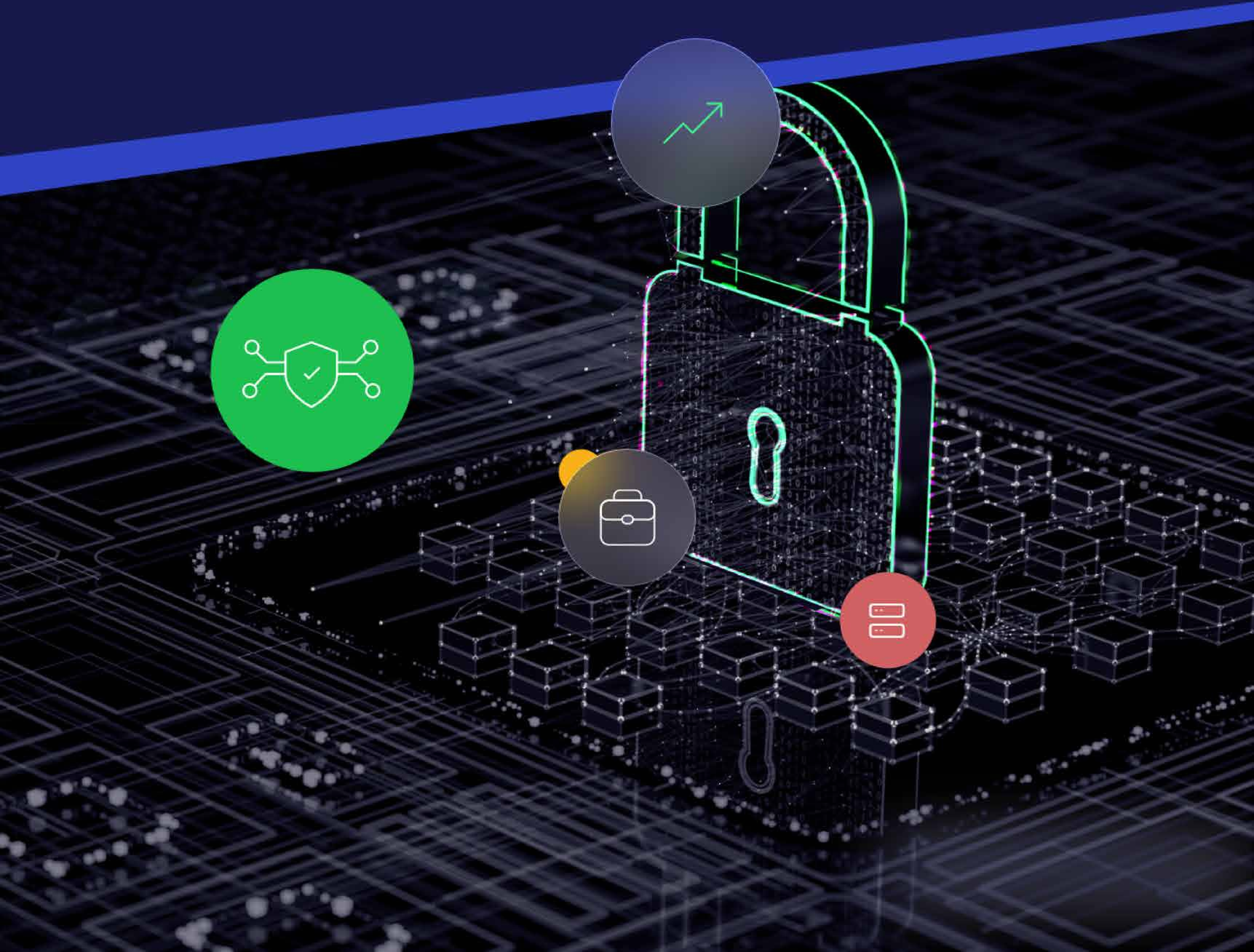
- ZOHO ENTERPRISE PERSPECTIVES -

Enhancing organizational security to meet evolving cyber threats

To remain viable, businesses must develop more comprehensive strategies for org-wide security.



CONTENTS

Clear and comprehensive security strategies are essential for maintaining the flow of business operations, preventing revenue loss, and establishing strong customer relationships. But as emerging technology gives way to more advanced threats, businesses are facing more complex challenges to cyber security. Here, we discuss strategies for protecting business systems and data.

Securing the evolving workspace through zero-trust architecture

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.

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]

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

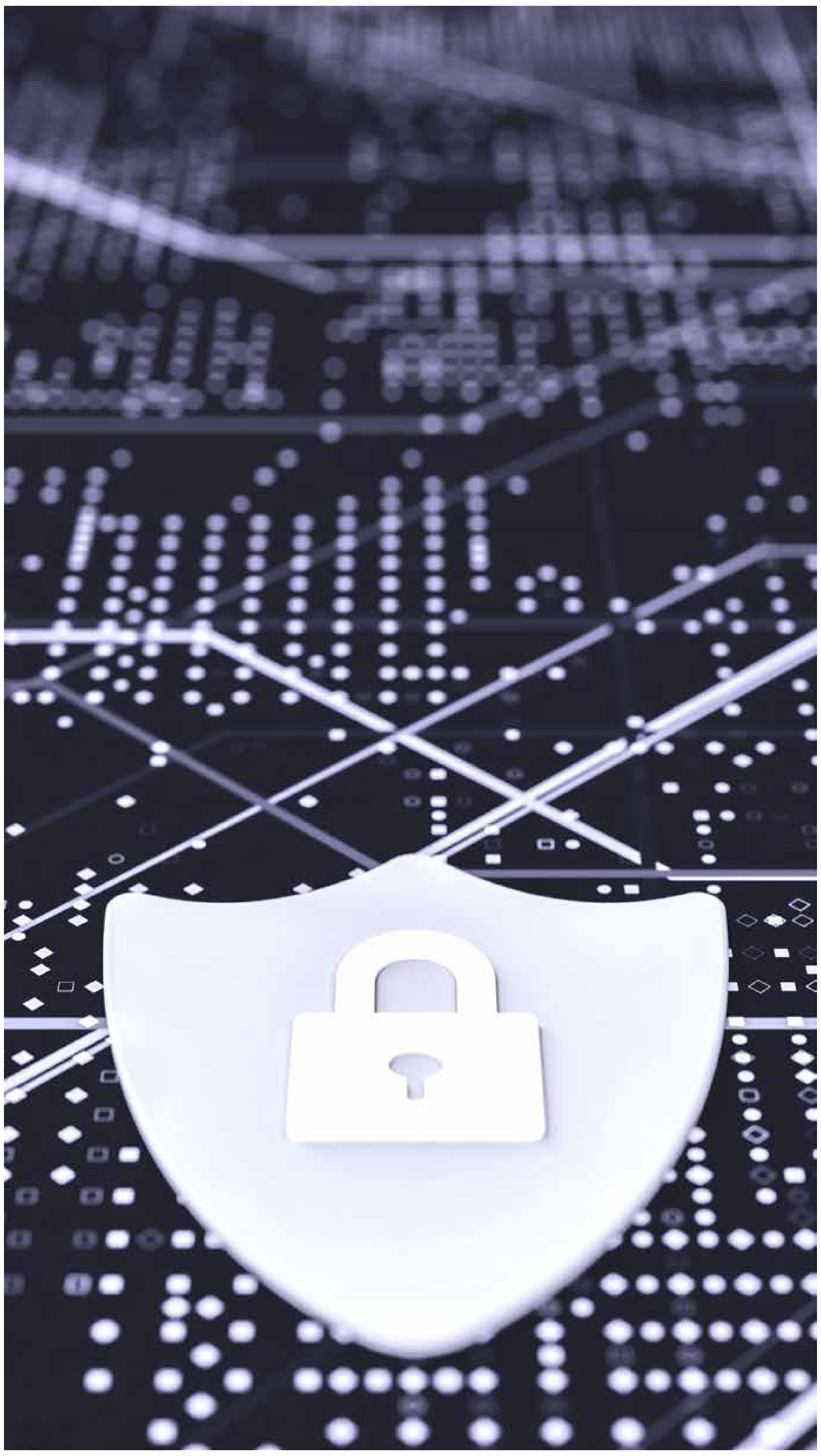
Experts agree that the vulnerability of these decentralized workplaces is only going to become more pronounced as time goes on, but forcing employees back to office premises full time has turned out to be challenging and often counterproductive for productivity and morale. For many companies that have 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.

[1] McKinsey

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.



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.

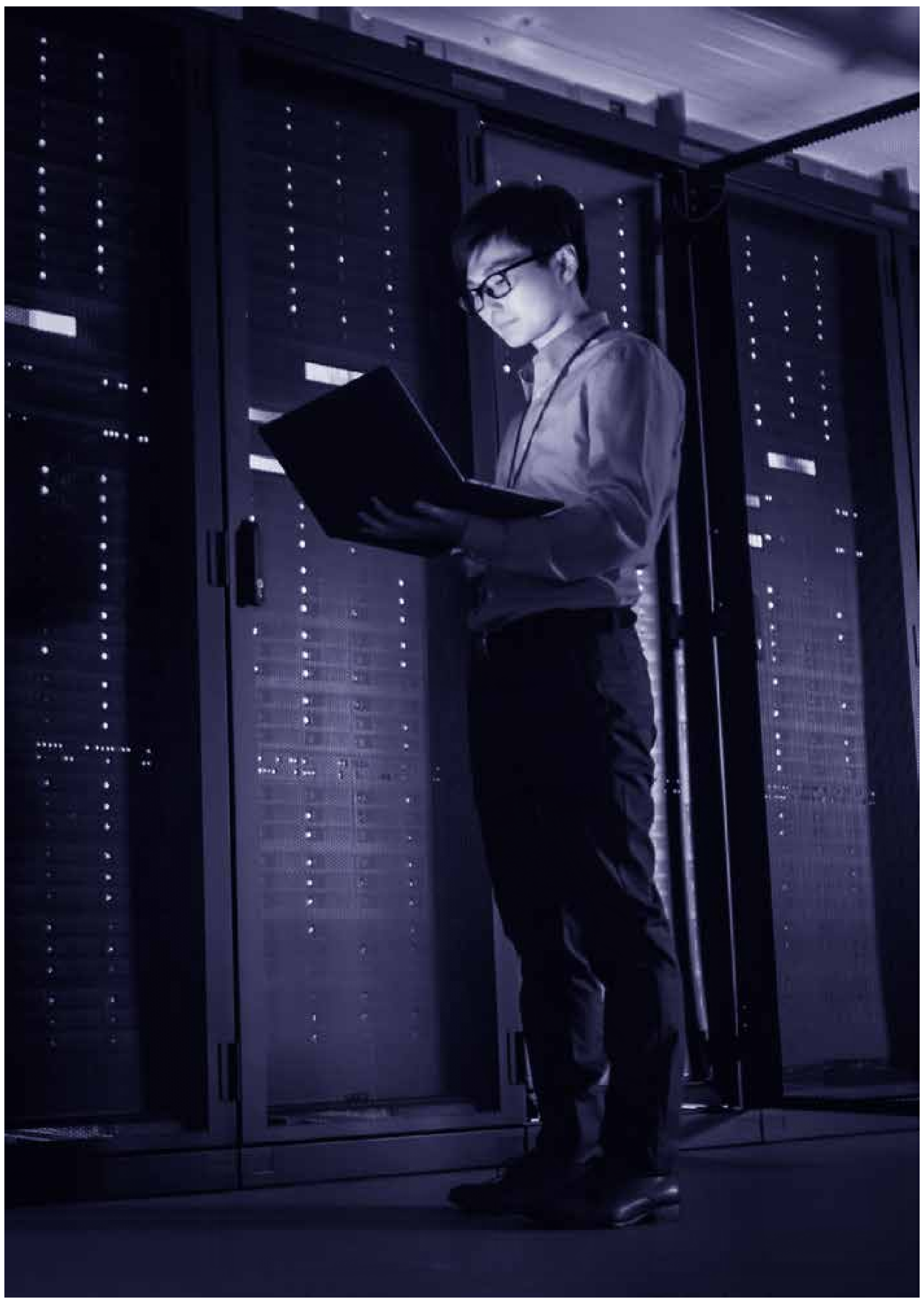
> *Zero-trust is projected to be a* ***$52 billion*** *industry by* ***2026.***
>
> **[CNBC]**

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

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

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.

[4] CNBC | [5] CyberTalk

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

[6] Fortune

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.

Assessing and addressing the risks of Shadow IT

Through a strategic, communication-centric approach, business leaders can mitigate the risks of rampant Shadow IT usage within their organizations.

There are many reasons why only 51% of organizations meet their original project delivery goals[7]—but a lack of transparency exacerbates them all. Without transparency, a manager can never accurately assess bandwidth, resource allocation, or team performance. This is what makes Shadow IT so pernicious. It precludes real insights into what teams need to achieve their goals and milestones.

Broadly, Shadow IT refers to any use of applications, software, or devices hidden from an IT team's view. Software is usually the most common offender, typically in the form of one-off apps. And while those tools might drive short-term collaboration, they can silo valuable conversations and data, threaten data security and compliance, and present an inaccurate panning.

Most employees turn to unsanctioned tech because they need it to work more effectively. In other words, it's a sign of an engaged employee; not a nefarious one. This is good news, because 52% of tech executives report that their employees are purchasing unsanctioned applications[8]. In response, some organizations are equipping teams with unified software solutions. This can help decrease the need for disparate applications, but it won't eliminate them entirely. With this in mind, forward-thinking business leaders are turning their attention to risk mitigation.

Audit

The only way to find Shadow IT in an organization is to look for it. Surveying employees about their own use of Shadow IT is a great way to start. An open and non-punitive approach increases the likelihood that employees will come forward without additional prompting.

[7] Australian Institute of Project Management

[8] Businesswire

Another strategy is using budget audits to uncover surreptitious IT spending. SaaS management tools can spot anomalies in traffic and server load, or track how data and metadata are moving through the organization.

Understand

The easiest way to reduce Shadow IT is to develop robust internal communication channels. Most employees turn to Shadow IT to increase on-the-job efficiency. This is where listening becomes essential; the only way to improve compliance is by understanding why the current tech stack is insufficient, and gather information on what tools might improve employees' software experiences. Employees are your best source of information for this.

Of course, communication is never a "one-and-done" scenario. Understanding the pros and cons of a given software solution requires an ongoing, open conversation. The employees stepping forward about their own use of Shadow IT will likely prove your best collaborators. As attentive and proactive problem solvers, they are already finding solutions for on-the-ground problems often invisible to those at the managerial level.

Assess

After understanding why employees are turning to Shadow IT, it's time to assess the risk it poses. Not all scenarios are created equal; it's important to triage them accurately. However, establishing a rule about Shadow IT usage is not a comprehensive solution. Employees will continue to turn to unsanctioned tools until they have the right tools or capacities to meet their needs.

In some cases, curbing the risks of Shadow IT can be as simple as defining the types of activities for which use is permissible. For example, ChatGPT might be safe for creating marketing copy, but off-limits for analysis and reporting of internal data. By maintaining a list of approved apps (and activities within them), IT teams can offer employees customization options that maintain an organization's broader information security promises.

Establish

Building formal communication processes is an effective way to ensure that everyone engaged with a project stays in the loop.

If lack of timely IT support is causing employees to turn to Shadow IT, workflows can translate support requests into tasks or projects with pre-set SLAs and escalation rules; the same method can be applied to the procurement and approval process for new technologies. Offering employees visibility into progress with regular updates makes compliance far more likely.

Software is only useful when it's used. But because software is constantly being updated, and its capabilities and features are continually expanding, it's understandable why many employees resist org-wide implementations in favor of the familiar apps they've customized to their needs. Ongoing education not only drives awareness of org-approved offerings, but provides an opportunity for org leaders to reaffirm best practices and alert employees to the security risks of Shadow IT.

Lean in to resource management

You can't measure what you can't see. And when Shadow IT is where the work happens, effective project management is a largely futile effort. Instead of working on strategic analysis or resource allocation, managers have to waste time asking for updates, trying to locate documents and collateral, and pinpointing why the budgets have gone so far off the rails.

When everyone works from a single (and shared) UI, it's easy to make quick course corrections and communicate them to all relevant stakeholders. Consolidated data leads to smarter data; when information is no longer cordoned off in unknown systems, it can exponentially grow in its organizational value.

In the absence of a unified system, good communication becomes essential; it is what connects every member of a project team to a common set of strategies, goals, and actions. And that connection is an organization's best chance of mitigating the risks that arise from the use of disparate software.

Data governance as an enabler of self-service BI

Evolving the definition of data governance for modern enterprises offers opportunities for improved data literacy and increased ROI.

Self-service BI has ramped up dramatically in recent years. In 2020, 62% of businesses deemed it essential to their operations,[9] and that importance has only grown. With the vast quantities of data that mid-market and enterprise-level organizations are crunching on a daily basis, development in the BI and analytics space is focused on offering self-service functionality at scale. The goal is to enable higher quality customer experiences through targeted, data-backed strategies that international teams can build, implement, and measure on their own.

> *__82%__ of data-management decision-makers find it difficult to forecast and control data costs.*
>
> [Forrester]

Unfortunately, these efforts are being stunted by ineffective data governance. The rise in shadow IT illustrates that employees are increasingly seeking value outside their organization's BI setup in order to drive value for customers. Self-service data solutions are evolving and scaling, but the same cannot be said for the policies and procedures that manage them. And trying to apply traditional governance techniques to modern, self-service BI tools has led to major challenges, such as an over-reliance on IT teams, a lack of org-wide data literacy, low data visibility, and ROI loss from ad-hoc data solutions.

[9] Forbes

To address these challenges, organizations are beginning to create scalable data governance strategies that are agile enough to complement self-service BI. This new approach redefines data governance as a collaborative system of policies, processes, and teams designed to drive data insights into the hands of the people who need them most. This evolution mitigates the organizational pain points of traditional data governance, and tends to reduce Shadow IT, boost customer experience, and increase connectedness across mid-market and enterprise organizations.

Challenges of IT-centric data governance

For some organizations, modernizing data governance strategies means completely redefining their goals. Governance used to revolve around "command-and-control" protocols, in which centralized IT teams set organizational standards for how employees should engage with and use corporate information.[10] Even though data governance has become more expansive in recent years, there is still an expectation that IT teams will carry the burden of implementing policies and procedures that ensure data is being put to the best and safest use.

As companies collect more data, this over-reliance on IT teams does not scale well. Governance operations such as adhering to regulatory standards, consolidating data to prevent inconsistencies or errors, and enabling self-service reporting and analytics, have become larger tasks—only a fraction of which IT is best suited to oversee. Many organizations with successful self-service BI infrastructures have created localized data teams to decentralize these initiatives. This has the potential to allow teams to access higher quality data, take only the information they find relevant, and create targeted data solutions more quickly than before. Unfortunately, this has run organizations headlong into their next big hurdle: data literacy.

[10] Forbes

Only:

21%

of employees feel confident in their data literacy skills

32%

of executives feel they can create measurable value from data

[Accenture]

Supporting data literacy through agile governance

In 2021, Deloitte advocated for data governance to take after agile methodologies through straightforward policies that act as "guardrails instead of bureaucratic hindrances."[11] Some organizations have done this by creating a centralized data governance team that outlines data collection and preparation standards that apply to domain-level data repositories. Instead of prioritizing compliance and risk mitigation above all else, which resulted in too little data accessibility for employees, this approach recognizes that accessibility is essential to drive effective data-driven decision-making and prioritizes improving the quality and usability of the data itself.

> *The momentum towards self-service cannot be stopped, so accessibility should be prioritized. If a governance team works with IT on assigning appropriate roles and permissions, employees can have faster access to ready-to-use data in a way that doesn't sacrifice security.*

Saravanan Muthian
Chief Information Officer at Zoho

Reducing the barrier to entry for employees to access and produce trustworthy insights from data will naturally increase data literacy.

[11] Deloitte

This approach can also act as a powerful enablement tool for data leaders across an organization. When agile governance is coupled with a robust feedback system, it allows data leaders to quickly recognize domain-specific literacy gaps amongst employees and request the tools and training materials from the governance team that will drive the most value.

Challenges of low data visibility

No-code and low-code tools have made data analytics more accessible to the average employee, but they have also revealed and exacerbated the challenges that traditional data governance started. As organizations attempted to move relevant information closer to the teams that would use it, data became fragmented between the preferred storage systems of individual regions or teams, creating data sets and tools that are either repetitious, single-use, or both.

This has the potential to lead to ROI losses from self-service BI. 82% of decision-makers find it difficult to forecast and control data costs because there is no org-wide visibility into all the data and tools their teams are using, and 80% find it a challenge to govern their data at scale.[12] Not only does this mean that many organizations are unable to create realistic budgets based on data solutions that drive the most value, but the security risks that Shadow IT poses extend to in-house solutions that have little to no oversight.

Improving data findability through centralized data cataloging

Data repositories have become pivotal for organizations looking to consolidate their dispersed data assets, but at a certain scale, even a centralized data repository inhibits data visibility and self-service BI. If repositories act as consolidated data storage, then a data catalog is the

[12] Forrester

directory that helps stakeholders pull specific information from that storage. This enables separate business domains to manage their data assets in a localized repository without those tools becoming siloed from the rest of the organization.

The metadata stored in data catalogs is especially key. It communicates whether certain information is sensitive, private, or protected, and it also categorizes data based on how it was collected and what it may be used for. For governance purposes, these metadata records act as documented proof of all the ways in which an organization's data has been moved, used, or changed, improving the security and trustworthiness of data and making org-wide information easier to manage at higher volumes.

On their own, these benefits boost the ROI of self-service BI by creating more awareness within organizations of where data is located and how it's being used. However, data catalogs also ensure that organizational information follows the FAIR data principles: findable, accessible, interoperable, and reusable.[13] These principles help promote data sharing and reuse as a means of generating more collaborative research opportunities and even greater ROI potential.

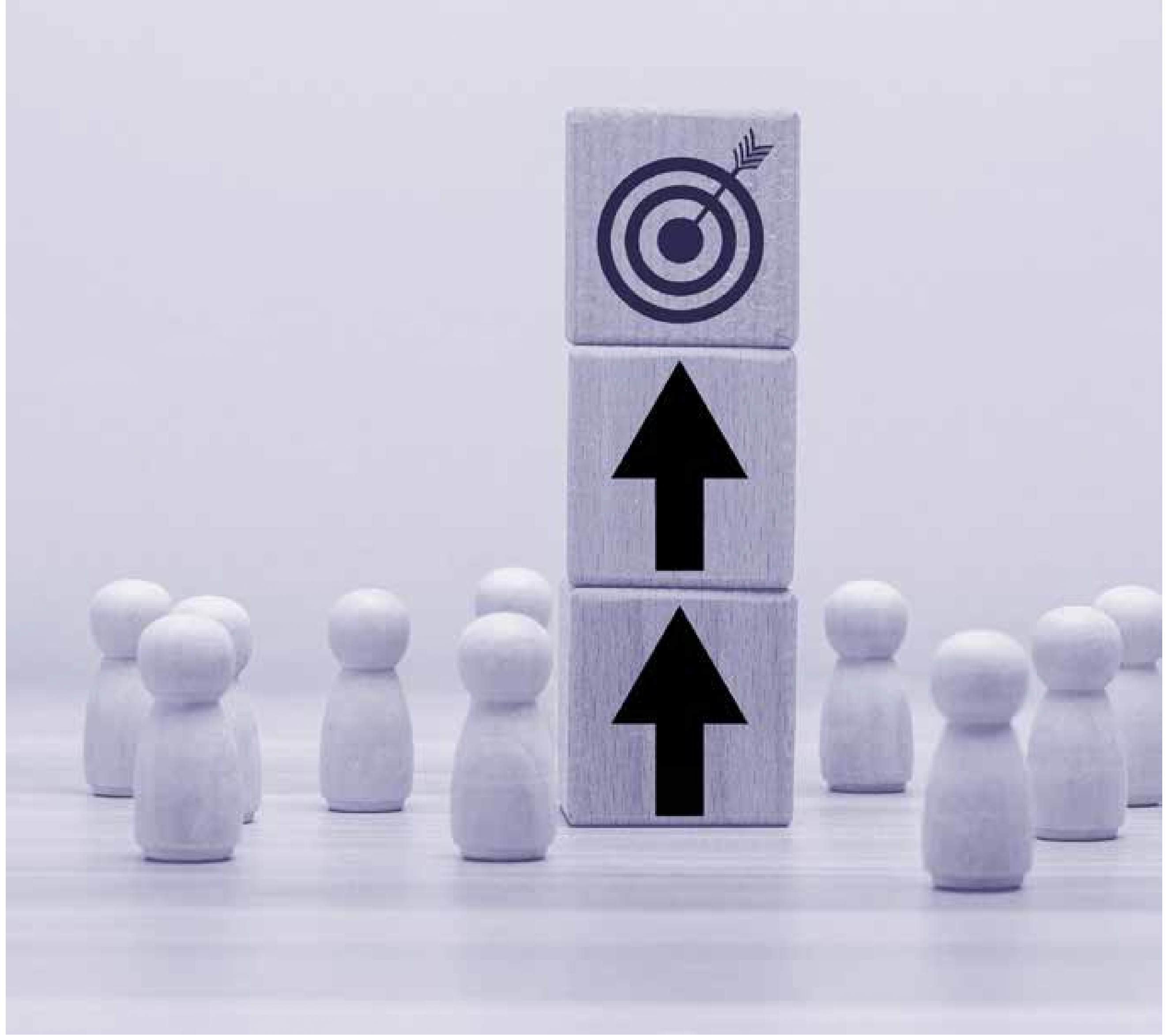
Designed for data visibility

A data catalog is only as strong as its integration with the low-code data tools and repositories that an organization uses. Zoho's custom solutions platform, Zoho Creator, acts as a secure and centralized hub for enterprise-level data solutions, and it's natively integrated with our powerful BI suite for simplified data cataloging, preparation, and analysis.

[13] Vericad

Driving value in self-service BI

Traditional data governance techniques provided obstacles to self-service BI, acting as a bottleneck for real-time insights, blocking visibility into org-wide data, and pushing employees toward Shadow IT as a means of getting around overly stringent and unnecessary policies. Modern data governance has flipped that stereotype on its head, playing an essential role in educating teams about best data practices, providing tools and guidelines to help self-service BI objectives, and ensuring data is as high-quality and trustworthy as possible. Without this governance, self-service analytics projects risk developing inefficiencies that impact not only organizational decision-making, but also the company's entire bottom line.



As self-service BI expands to become the norm of mid-market and enterprise businesses around the world, there is a growing movement toward data empowerment for employees.[14] Organizations have already seen how providing teams with real-time access to data has improved their business operations. Data governance completes this vision by ensuring that, no matter the amount of data a company collects, it remains accessible, high-quality, and ready to be transformed into secure, value-driving solutions.

[14] Forbes

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