ESG SHOWCASE

The Future of Application Security is Access Orchestration by Pathlock

Date: July 2021 **Author:** Carla Roncato, Senior Industry Analyst

ABSTRACT: Organizations on a path to zero trust are re-examining their default user and shared access control models. Mission-critical applications and systems that run the business operations such as Enterprise Resource Management (ERP), Human Capital Management (HCM), and Customer Relationship Management (CRM) have undergone tremendous change just as with cloud-native, SaaS applications. When it comes to access orchestration, the future is unifying—access governance, data protection, and application security across all business-critical applications.

Overview

Compliance is an increasingly complex, critical business function. Even the best organizations in the world struggle to balance adherence and changes in regulations, while trying to retain business agility and enable digital transformation. People-related tasks and access-related risk tools are often siloed and abundant and yet provide very little comprehensive visibility and much less automation to be audit-ready. Cross departmental collaboration is required to manually stitch together their GRC programs. You only need one failed audit to realize this approach is unsustainable.

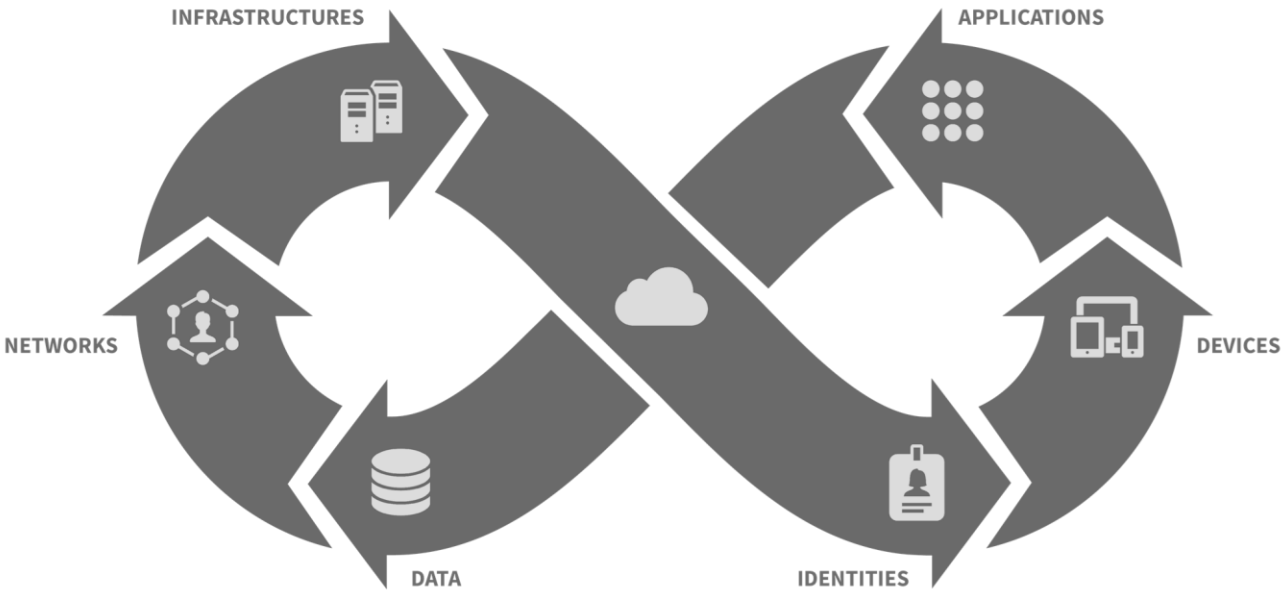
Compliance and Zero Trust (ZT)

Zero trust is not a product, but rather a strategy or model that assumes there are no perimeters or safe zones, no safe users or trusted devices or applications, and therefore there needs to be zero trust. One of the primary tenets of a zero trust strategy is the principle of least-privilege access, which is fundamental to reducing both internal and external threats to organizations. The principle of zero trust is that *"only the minimum necessary rights should be assigned to a user that requests access to a resource and should be in effect for the shortest duration necessary and then relinquished*."

Regardless of what stage of technology and security maturity organizations are in today, interpreting this principle one user at a time, one resource at a time, one policy or regulation at a time, and based on a vague notion of risk and duration is extremely difficult to do. Interpreting Sarbanes-Oxley (SOX) and applying segregation of duties (SOD) into business processes and user access workflows requires a solution that integrates with all financially relevant applications (custom and commercial) to be effective at surfacing policy violations that can result in financial loss and preventing the risky behaviors that can lead to data loss.

Recent ESG research uncovered that organizations with more mature zero trust programs claim that zero trust has simplified compliance efforts (55%) and has reduced the number of data breaches they have experienced (59%), compared to organizations with less mature programs, which reported 41% respectively.[1]

Figure 1. Elements of a Zero Trust Strategy



Source: Enterprise Strategy Group

Access Orchestration for Identities, Applications, and Data

For IT and security professionals, access management broadly refers to a set of processes and tools used to define, verify, provision, enforce, audit, and monitor users' access to applications, data, and systems wherever they reside.

Access orchestration, on the other hand, is a platform approach by which organizational departments can obtain visibility into:

- User permissions and role conflicts.
- Insider risk prevention and potential fraud identification.
- Data classification and protection.
- Privilege activity management and session monitoring.

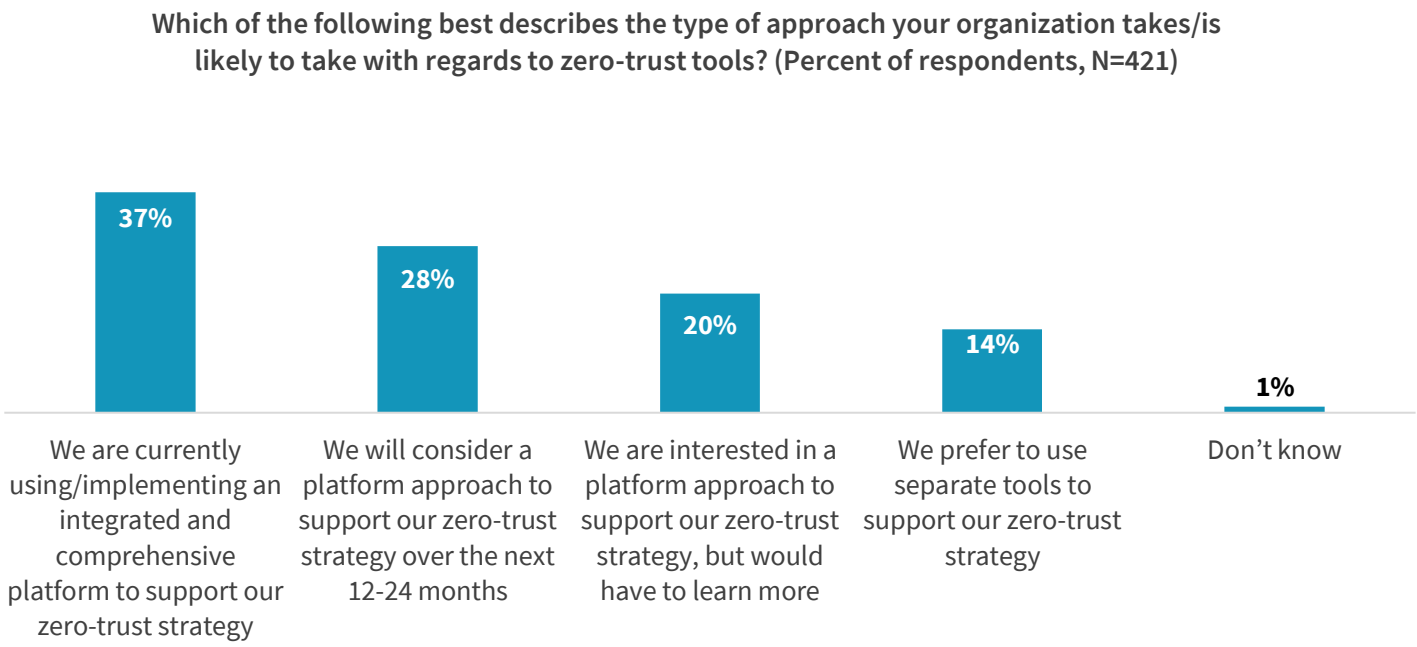
It provides the ability for business stakeholders and data owners to perform ongoing user access reviews armed with this context.

[1] Source: ESG Master Survey Results, *The State of Zero Trust Security Strategies*, May 2021. All ESG research references and charts in this showcase have been taken from these master survey results, unless otherwise noted.

Better yet, automating various manual controls and siloed workflows and unifying separate dashboards for decision-making support on top of existing technology investments can save organizations time and money and cut down on the number of mistakes.

In the same ESG research survey, we found that 37% of organizations are currently using or implementing an integrated and comprehensive platform to support their zero trust strategy, as opposed to using separate and disconnected tools. 28% indicate they will consider a platform approach to support zero trust over the next 12-14 months.

Figure 2. Type of Approach for Zero Trust



Source: Enterprise Strategy Group

Introducing Pathlock

Pathlock is a unified Access Orchestration platform that combines user access governance, data loss prevention, continuous behavioral and transaction monitoring, and least-privilege automation to achieve a path to zero trust.

User Access Governance

Pathlock's user access reviews provide people across the organization with all the details necessary to approve, delegate, revoke, and submit requests including descriptions on the role, reasons, risks, transaction type, and value.

User Access Reviews can take a lot of peoples' time and are often not dynamic, which can lead to too many requests piling up as a bottleneck and result in too many permissions in place well beyond the intended need for access. Additionally, in very large organizations, the volume of roles and amount of role change can make access governance both tedious and error-prone.

With Pathlock's User Access Review, organizations have the flexibility of automating a variety of event-driven scheduled reviews, such as those triggered by a position change noted in the HCM, as well as scheduled daily, weekly, monthly, or quarterly workflows enforcing accountability by owners and approvers. Pathlock's user access reviews provide people across the organization with all the details and workflow necessary to approve, delegate, revoke, and submit requests, including descriptions on the role, reasons, risks, transaction type, and value.

Segregation of duties is a core internal control for organizations, based on shared responsibilities of key processes, that disperses the critical functions to more than one person or department. Without this separation in key processes, organizations are more susceptible to error, fraud, and operational risks. Key examples of these processes are for financial transactions and systems as well as vendor procurement processes and systems.

Pathlock's segregation of duties provides people across the organization with an analysis view into business processes in violation by severity, risk type and user. Additionally, access requests can also simulate the risk impact in real time as roles are added and changed, including a customer-specific risk score, which highlights the riskiest changes before they occur.

The intuitive interface takes the guesswork out of which policy violations are occurring, or likely to occur, due to introduction of change requests and where the responsibility for remediation lies within the organization. Policy owners can see a report of their specific controls and probe deeper into the issues and risks to prevent insider fraud.

Segregation of Duties

Pathlock's segregation of duties provides people across the organization with an analysis view into business processes in violation by severity, risk type, and user. Additionally, access requests can also simulate the risk impact in real time as roles are added and changed, including a customer-specific risk score, which highlights the riskiest changes before they occur.

Continuous controls monitoring is another critical element to an effective compliance program and should extend beyond auditing of entitlement assignments alone to monitor activity within applications:

1. Surface actual violations of SOD risks.
2. Enforce business processes and free up cash.
3. Monitor IT general controls and streamline IT audit.
4. Confirm application configuration is up to date.

Pathlock's continuous controls monitoring makes it possible for organizations to automate testing and reporting on all transactions to achieve audit and compliance goals. With their library of pre-built privacy and regulatory controls such as SOX, HIPAA, GDPR, and CCPA, organizations can be assured that the intent of the regulation is established correctly as a control and monitored. Transaction blocking and automatic deprovisioning of account and user access can support organizations that need to ensure process adherence and compliance year-round, not just at the time of audit.

The Bigger Truth

Organizations on a path to zero trust are re-assessing the mission-critical applications and systems that run the business operations such as Enterprise Resource Management (ERP), Human Capital Management (HCM), and Financial Planning & Accounting (FP&A). When it comes to access management, the future is unifying access governance, data protection, and application security across all business-critical applications.

Pathlock's unified access orchestration platform brings a breadth of integrations, depth of monitoring across all controls related to user access, sensitive data, and application security.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188