pathlock

EBOOK

Access Orchestration for the Digital Enterprise

Just-in-Time/Just-Enough Access to Support a Zero Trust Future

270 S. Main St., Flemington, NJ 08822
T +1-908-782-5700
info@pathlock.com

Executive summary

Controls that govern application access prevent financial and reputational damage. Yet, the old ways of designing and managing those controls aren't sufficient for fast-growing digital enterprises for several reasons.

- Access controls originally designed for a small set of IT-managed, on-premise applications aren't sufficient for today's distributed IT environments.
- Enterprises are spending too much time on manual work which increases costs, time, stress, and risk at every part of the access management lifecycle.
- Access governance processes managed in silos provide an incomplete view of enterprise risk, making informed decisions impossible.

As enterprises become more complex, staying with the status quo increases your application-level risk. Management costs escalate and business productivity stalls.

This eBook shows you how you can replace outdated, manual processes with automation designed for the modern digital enterprise. It outlines the differences between traditional access governance and access orchestration, an always-on solution that ties multiple processes together in a central hub.

In this eBook, you'll learn:

- How just-in-time and just-enough access support the journey to a Zero Trust future.
- How to change risk management from point-in-time analysis to a continuous part of every transaction and digital operation.
- How to measure the ways you can save time and lower costs at each stage in the access governance lifecycle.
- How you can determine a meaningful measure of risk to help you make application access decisions and collaborate effectively across your entire organization.

Access orchestration is more than automation.

You can think of access orchestration as the air-traffic controller of identity, access, and application use.

Many IT and security solutions offer functionality that automates some access-related activities. IAM, IGA, GRC, and UEBA, have become specialized segments of the cyber security space, focused on solving only a sliver of the overall access challenge. Access orchestration is the connective tissue that talks to all of them.

Access orchestration is unique because it ties multiple automated processes together in a central, connected hub that is integrated in real time. If an access change happens in one system, it's immediately reflected in all other systems, without any manual intervention. No downloads. No uploads.

Access orchestration allows you to use any security and IT workflow solutions you choose, including legacy technology you already have in place, and connect them together. You don't need to build or maintain APIs to connect them yourself.

Challenge 1:
Traditional access controls were designed for a small set of centrally managed applications.

Historically, enterprises only worried about creating access controls for a handful of critical systems with a small set of privileged users and activities. To ensure adequate Segregation of Duties (SOD) to comply with SOX requirements and other security frameworks, organizations focused primarily on managing access to a central ERP.

Today, the average enterprise has approximately 300 business apps, 98 unique billing owners, and over 20,000 app-to-person connections.[1] Sensitive data and activities span multiple systems, operations, transactions, lines of business, and processes.

The complexity of modern IT infrastructure and diversity of applications require more granular, real-time risk analysis than legacy solutions can provide.

The move to the cloud has made security analysis more difficult.

The acceleration of cloud apps makes access control and SOD challenging to manage. For SAP enterprises transitioning to S/4HANA, functionality that resided on a homogenous technology stack is now concentrated in cloud apps like SAP SuccessFactors, SAP Concur, SAP Ariba, and SAP Fieldglass. Plus, the rise of SaaS means many critical business apps are off the radar of IT as business units have more control over licensing and user management.

Because cloud applications aren't within your firewall, you can't necessarily complete vulnerability scans, or effectively assess their security.

> ***Today, the average enterprise has approximately 300 business apps, 98 unique billing owners, and over 20,000 app-to-person connections. Sensitive data and activities span multiple systems, operations, transactions, lines of business, and processes.***

Each application in your IT environment has a different security and authorization model.

More applications means more diverse, complex controls to create and manage. User roles that are built into third-party applications are typically broader than your internal security model calls for. Some are too rigid. You must reconcile them all to manage access permissions consistently and avoid conflicts between applications.

Legacy IAM and IGA solutions check access conflicts at a high level, but they don't check conflicts at the action level. Most enterprises must therefore maintain their rulesets manually to achieve the level of access control granularity they require.

Manual control management causes duplication and delay.

Each control requires design, documentation, internal Q/A and external testing and auditing. Non-routine transactions require you to assess risk at the same time you design and operate controls.[2] It's no surprise that half of all fraud cases involve internal control weaknesses.[3]

Enterprises are working toward control best practices, but struggle with manual design and management

20% don't have a centralized internal control **repository**

50% have less than 10% of their controls **automated**

70% identify control automation as a top **priority**

50% want to **reduce** their control **deficiencies**[4]

Addressing the challenge

Access orchestration automates controls for every application in your organization.

Access orchestration automatically translates and analyzes business activities that take place in multiple applications, mapping diverse roles and permissions and synthesizing controls in a common platform.

A single set of consistent controls covers multiple use cases and adheres to your central security policies and security framework.

Access orchestration is more granular than role-based access control or attribute-based control.

Access orchestration does more than determine what systems and applications a user can access. It also determines exactly what a user can do with that access once they have it. For example, with granular, action-level controls, access orchestration determines if a user can initiate or approve a particular transaction, share sensitive information, or manage other users.

By replacing manual control creation with access orchestration you can...

- Save control design time and reduce the need for coding resources.
- Reduce the number of controls that must be tested, documented, and maintained.
- Make sure controls are consistent across systems, business units, and geographies.
- Ensure controls account for cross-application conflicts across your entire IT environment.
- Document controls automatically so they're easy to share with execs and auditors.

Challenge 2: Traditional access controls negatively impact IT and business operations.

Application governance is not a once and done activity. It's a continuous cycle with multiple stages, including user provisioning, trust elevation, deprovisioning, session monitoring, and remediation.

In a typical management model, the policies that control application access are disconnected from the systems that manage day-to-day operations. As a result, manual checks and approvals designed to reduce risk introduce challenges at each stage of the access lifecycle.

According to a February 2021 survey of 300+ enterprises from Dimension Research, 72% of organizations report it takes at least a week for a typical worker to get a privileged identity provisioned with access to required systems. That's time a user can't be productive.

Lengthy provisioning processes cause friction.

Traditionally, when IT teams provision users, they must review each role, find out the user's current access, manually identify possible conflicts, request approval, and put mitigating controls in place.

Legacy identity management and access request mechanisms provide workflow routing for provisioning, but still require manual access management. Application role definitions are often too broad, too strict, confusing, or overlapping, which leads to access mistakes and increases risk.

As a result, provisioning processes are often incomplete and inconsistent across systems, teams, and geographics. They also take too long. According to a February 2021 survey of 300+ enterprises from Dimension Research, 72% of organizations report it takes at least a week for a typical worker to get a privileged identity provisioned with access to required systems.[5] That's time a user can't be productive.

Trust elevation takes too long and isn't closely managed.

There are many reasons for privileged users to have temporary, elevated access to sensitive data and activities. For example, developers may need "break-glass" or "emergency access" for troubleshooting, and they often need it right away.

Projects that involve third-party vendors or contractors typically require access to be allocated for a period of time. Business users

need to be able to work with vendors and get them going quickly. They shouldn't have to wait while IT manually runs scenarios and configures access.

Once elevated or temporary access is set, it's easy to forget. Too often, access is left standing long after it is required.

Deprovisioning delays increase risk.

Half of enterprises report that it usually takes them three days or longer to revoke access for a departing worker. According to the same Dimension Research study, many workers, including 56% of sales managers, admit to taking company data with them with they leave.[6]

Monitoring is time consuming and cumbersome.

Session monitoring ensures that access control policies are functioning as expected. Monitoring is often tedious work that involves combing through logs and watching videos of user behavior.

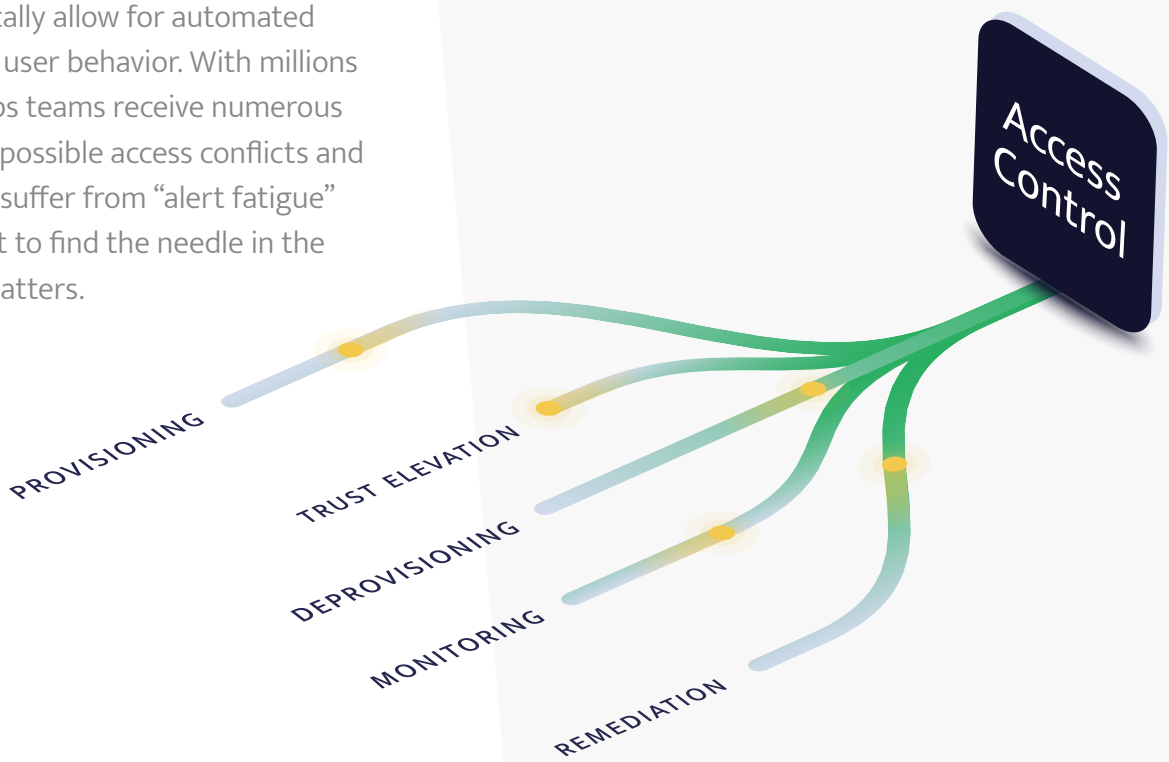
Monitoring tools typically allow for automated alerts for unexpected user behavior. With millions of user activities, IT ops teams receive numerous daily alerts indicating possible access conflicts and violations. They often suffer from "alert fatigue" because it's so difficult to find the needle in the haystack that really matters.

Despite the volume of data, IT teams often don't have enough detail on relevant access policies and require additional manual forensics. They spend time questioning data reliability and chasing false positives. The number of false positives causes many organizations to stop using the anomaly detection solutions available with legacy security solutions.

Finally, enterprises also struggle with retaining session monitoring data. Data is often kept in multiple systems, disconnected from central auditing platforms, and isn't easily searchable for post-incident forensics.

Remediation is too slow to prevent damage.

Negligent or malicious insider behavior, often the most damaging, is also the hardest to uncover because it's easy for insiders to hide. It can take weeks or months to fix incidents, if you even know that they occur. The average incident takes 77 days to contain.[7]



Addressing the challenge

Access orchestration streamlines management throughout the access lifecycle.

Access orchestration supports provisioning, deprovisioning, and every application interaction that happens in between.

Automated, integrated provisioning gets users up and running fast.

You can run "what-if" scenarios and system checks to catch potential conflicts within and between applications such as ERP, procurement, Human Capital Management, CRM, and more.

Provisioning teams can proactively run scenarios to ensure a least privilege, Zero Trust posture. At the point of provisioning user access, IT operations and business approvers can see what's causing access restrictions down to the t-code and authorization object level.

Adaptive controls provide just-in-time, just-enough access.

Access orchestration allows you to quickly elevate access for firefighters or third parties without slowing down productivity for technical and business users.

You can set conditional time-bound access for employees. It automatically shuts off at a time you determine to avoid standing access.

Continuous monitoring allows staff to focus on exceptions, not false positives.

With access orchestration, continuous control monitoring ensures business transactions adhere to SOD requirements and protect sensitive, personal data. You can move from checks that are limited, periodic, and manual to comprehensive, continuous, and automated. Instead of chasing false positive, you can focus only on the exceptions and alerts that matter.

All data is stored in one place so you can analyze according to risk. There's no need to review logs or watch video recordings. You can watch your dashboard update in real time. Or, you can set exception alerts at the line-item level of detail for only those activities you really need to monitor (e.g. configuration changes and payments) so you only receive alerts when actual materialized conflict has occurred.

Deprovisioning is automated and centralized.

When an employee leaves your organization or a contractor's project ends, you can remove their access to all systems and applications at once.

Remediation actions stop threats from becoming catastrophes.

Preventative controls can block fraudulent or non-compliant transactions in real-time. Automated triggers can remove privileged access rights and terminate sessions to stop insider threats in their tracks. You can choose to turn off user access or auto-reprovision access to a least privilege status, based on real usage activity.

Challenge 3: Legacy access governance doesn't provide a consolidated, real-time view of risk.

In a traditional process, access governance activities are disconnected across many technology stacks and teams. With that type of siloed approach, it's difficult to gain a complete understanding of a single user's activity or the full scope of access risk to your organization. As a result, enterprises are less agile than they should be. There's a lot of finger-pointing about who owns access governance and who remediates issues. Gaps in policies and management processes provide windows for fraud and cyber threats to enter.

> ***"An organization may have several different GRC programs scattered across various departments instead of a single enterprise-wide program. So, the insights and risk assessments gleaned from these narrower programs would not necessarily reflect the organization's overall risk."***
>
> Michael Rasmussen,
> principal analyst, GRC 2020

User Access Reviews are too cumbersome to be accurate or effective.

A key detective control in your access governance process, User Access Reviews (UARs), are meant to ensure that business decision-makers know who has access to perform critical tasks. They flag potentially toxic access conflicts and bring them to the attention of reviewers.

UARs are often very manual processes that take place offline. Organizations must review thousands of users, regardless of any role or status change.

In a typical access review process, staff must manually compare access rules with specific transactions and business processes. Typically, this means generating reports on users and access privileges with spreadsheets and macros, toggling between your role conflict matrix and an SOD data dump. You can spend days analyzing the data looking for risks and user conflicts. You must route reports to managers for review and manage their return. Finally, you must compile a final audit-ready report.

Performing reviews this way is costly, slow, and can cause mistakes. Because they are so time-consuming, UARs typically only happen once per year, which means it's easy to miss access violations that occur between checks.

While the responsibility of performing access reviews generally falls to a company's audit or IT administrators, business users are the consumers of reports and ultimate decision makers. Unfortunately, it's not uncommon

for reviewers to simply rubber stamp 'Access Approved' without understanding the business or financial impact of their access decisions.

GRC programs and systems are too disconnected.

Governance, Risk, and Compliance (GRC) systems help with workflow management, but they don't tap into the data that defines risk or controls that help reduce it.

As Michael Rasmussen, principal analyst at GRC 2020, explains, "an organization may have several different GRC programs scattered across various departments instead of a single enterprise-wide program. So, the insights and risk assessments gleaned from these narrower programs would not necessarily reflect the organization's overall risk."[8] Each GRC system or process may have a different method to define and measure risk, instead of a common methodology to measure impact in terms that business leaders all understand.

Addressing the challenge

Bring IT, security, governance, and business teams together.

With access orchestration, automated integration, correlation, and consolidation of all application data provides a single view of risk all teams can share.

UARs are clear and effective.

Access orchestration automates the UAR process so enterprises can save time and cost and increase accuracy. Instead of periodic reviews, UARs can be triggered automatically based on events for just-in-time review and response. Reviewers easily see all toxic access conflicts and the business impact of access decisions.

Enterprises can move toward a risk-based security framework.

Access orchestration is continuously analyzing access and activities to create a real time, comprehensive picture of risk. Armed with accurate information, you can create a systematic method to identify, evaluate, and prioritize the access-related risk facing your organization.

A key aspect of risk-based security is understanding the impact of risk decisions. Access orchestration helps you measure your risk exposure in real-time in terms of tangible, financial impact to your business. Instead of surfacing millions of exceptions and estimating their potential impact, you can see actual access violations and pinpoint users and applications that need attention. You can take immediate action to remediate risk where it matters and see your financial exposure decrease.

Everyone can work together toward a common goal.

Effective risk management demands a collaborative approach.

IIA's recently revamped their widely adopted "Three Lines of Defense Model" in 2020 to reflect the evolving role of risk management. The new model encourages collaboration between business functions in a way the previous model didn't. As IIA President and CEO Richard Chambers explains, "The new model's principles-based approach is designed to provide users greater flexibility. Governing bodies, executive management, and internal audit are not slotted into rigid lines or roles."[9]

> ***"The new model's principles-based approach is designed to provide users greater flexibility. Governing bodies, executive management, and internal audit are not slotted into rigid lines or roles."***
>
> Richard Chambers, president and CEO, IIA

For example, the new approach means that it's not sufficient to put the onus of UARs solely on business decision makers. Rather, it's the responsibility of technical teams to surface the data the business needs to make decisions, and present it in a way that they can clearly understand.

Access orchestration empowers everyone involved in risk management, including IT, security, governance and compliance teams, as well as business users, to share a common understanding of access risk. Because all access-related controls, applications, databases, and other IT systems are linked together, information is kept up to date in all systems. A change in one is immediately reflected in all others.

With access orchestration, risk scores and dashboards are easy to understand so enterprises can make informed, data-driven decisions as a team.

Measure return on investment (ROI) of access orchestration.

Compare the time, cost, and risk your enterprise must bear with and without access orchestration.

Activity	Without Access Orchestration	With Access Orchestration
Control design and monitoring	High-cost coding talent spends time designing, testing, and maintaining controls. Enterprises typically spend $1,000,000+ in manual control management.	A library of hundreds of prebuilt controls for SOX, GDPR, CCPA, and other compliance types accelerates control creation and brings rule maintenance to zero.
User Access Reviews	It's common for enterprises to spend approximately 15 minutes for manual review of each user, per system, per cycle.	Enterprises reduce the number of accounts needing review by 50% or more. Manual review time is slashed by 90%.
Compliance Reporting and Auditing	Enterprises typically spend $500,000+ annually in manual SOD review and reporting costs.	Automated SOD review and report generation reduces costs by over 90%.
Application access provisioning and deprovisioning	New employees and contractors lose 4-5 days of productivity waiting on application access. Terminated employees and contractors leave behind thousands of zombie accounts.	Users—including third parties with emergency access—are provisioned and deprovisioned automatically and instantly across all systems and applications.
Threat response and remediation	Applications send billions of events to your SIEM. They must be logged and stored at high cost. Security analysts must be hired and trained to monitor and react to alerts. Yet they spend 90% or more of their time investigating false positives.	Applications send 99% fewer events to the SIEM, thanks to intelligent correlation and filtering. Cost of ingesting, processing and storing logs decreases, saving $1 million per year or more. High-fidelity alerts reduce false positives by 90% or more, reducing the labor required to investigate threats by the same amount.
Threat remediation	The average insider threat incident takes 77 days to contain, often because it's impossible to tell which alerts require attention and difficult to know which actions will address them.	Automated prevention, including blocking downloads and deprovisioning users, slashes response time to minutes. Even true threats can be traced and remediated quickly, with less skilled/non-technical resources.
Risk of data loss	Data loss is typically discovered months after the incident, once sensitive data has already left your systems.	Data loss is captured in real-time, reducing risk of cyber catastrophe by 30%.
Cost of fraud	Insider fraud typically amounts to 5% of an organization's annual revenue.[10]	With fewer opportunities for fraud and proactive monitoring and response, insiders are enabled to do the right thing.

See what type of ROI is achievable for you.

Pathlock's access orchestration platform has been developed from years of experience supporting the world's most security-conscious enterprises. With Pathlock you can manage all aspects of access governance in a single platform, including user provisioning and temporary elevation, ongoing User Access Reviews, control testing, transaction monitoring, and audit preparation. Based on the most comprehensive control set in the industry, Pathlock synthesizes siloed security models and continuously monitors transactions across all your applications.

Contact us

for a free ROI assessment tailored to your organization and goals.

Pathlock protects digital enterprises from the inside out

Pathlock enables granular, just-in-time access control for sensitive applications and business processes so IT and security teams have stronger oversight of privileged activities.

- **SOD management**. Ensure Segregation of Duties within and across applications.
- **Adaptive access control**. Align access rights for groups, users, roles and access objects across multiple security models. Set context-based permissions and implement preventative, detective, and mitigating controls.
- **Provisioning**. Run what-if scenarios to catch potential conflicts within and between applications such as ERP, procurement, Human Capital Management, CRM, and more.
- **Temporary, emergency access**. Set just-in-time access that expires automatically. Provide auditors granular detail into activities during periods of elevated access.
- **Privacy compliance**. Prevent unauthorized access to sensitive data with PII discovery, data minimization and masking, and transaction-level controls.
- **Future-proof controls.** Manage a single set of controls that cover multiple use cases and map to a consistent security framework.

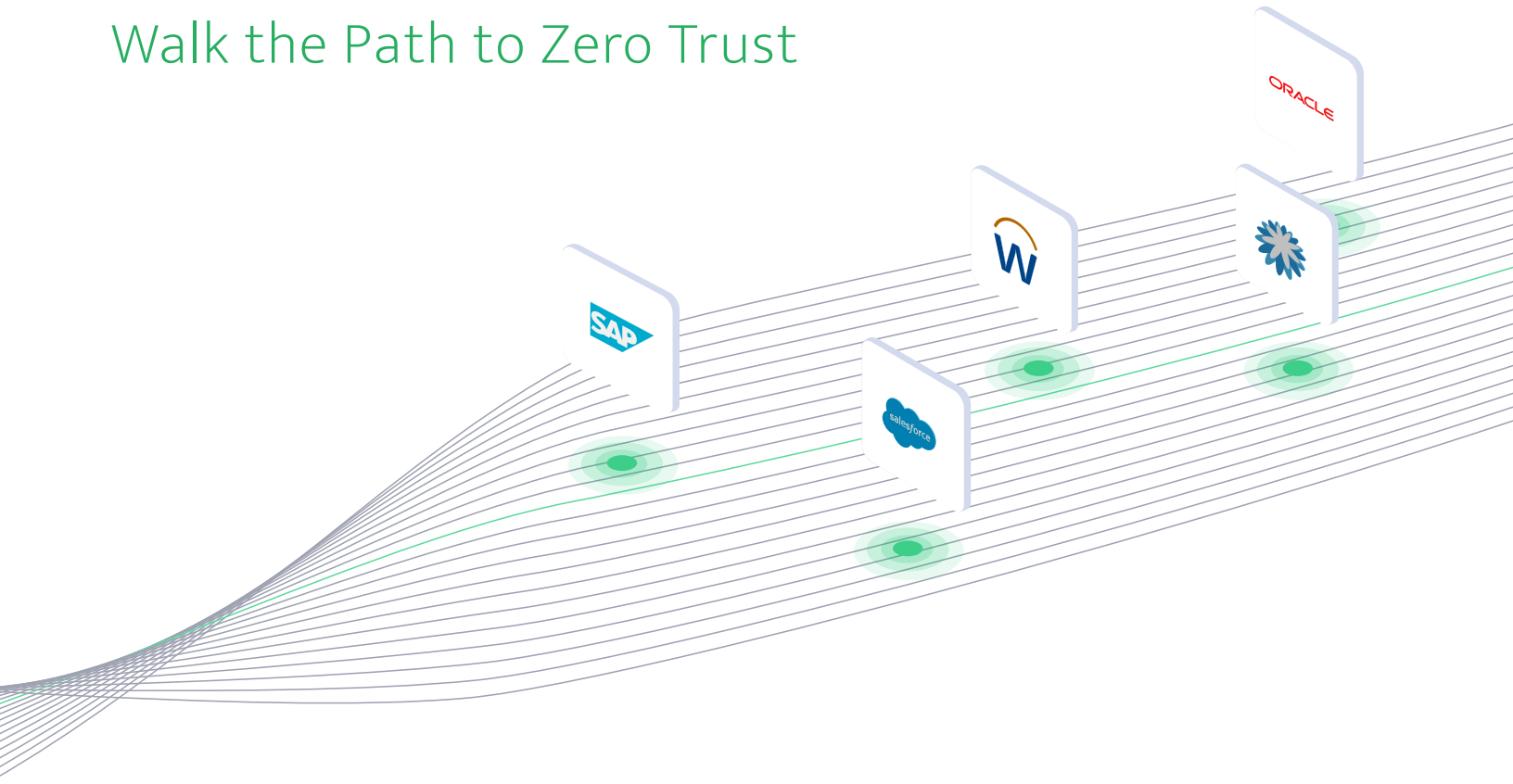
Our connected platform integrates all access-related rules and user activities in real time. In easy-to-understand dashboards, you can see actual access violations, not just theoretical possibilities. Risk scores demonstrate the financial impact of access decisions. You can quickly prioritize actions to shut down threats before they cause damage.

With 144+ built-in connectors to our cloud-based platform, we get you up and running fast, so you see ROI right away.

Pathlock's Access Orchestration Platform

Control	Control Premium	Control 360	Control 360 ZT
Eliminate cross-application conflicts to meet Segregation of Duties and SOX compliance requirements.	Continuously monitor granular user activities within and across applications. Measure financial exposure of risk.	Supercharge data security and privacy using adaptive, just-in-time access and ongoing mitigating and detective controls.	Enforce least privilege provisioning within your workflow. Automate incident response and time-bound deprovisioning.

Walk the Path to Zero Trust



References.

1. https://www.blissfully.com/blog/saas-statistics/
2. https://www.acfe.com/rttn2016/costs.aspx
3. https://www.thecaq.org/guide-internal-control-over-financial-reporting/
4. https://assets.kpmg/content/dam/kpmg/ch/pdf/results-grc-survey-2019.pdf
5. https://www.idsalliance.org/wp-content/uploads/2021/02/IAM-Stakeholder-Perspective.pdf
6. https://www.idsalliance.org/wp-content/uploads/2021/02/IAM-Stakeholder-Perspective.pdf
7. https://www.proofpoint.com/us/resources/threat-reports/2020-cost-of-insider-threats
8. https://www.sapinsideronline.com/articles/conquer-user-access-reviews-in-sap-systems-once-and-for-all/
9. https://www.bankinfosecurity.com/how-to-leverage-grc-for-security-a-6164
10. https://iaonline.theiia.org/blogs/chambers/Pages/New-IIA-Three-Lines-Model-Offers-Timely-Evolution-of-a-Trusted-Tool.aspx

About Pathlock

Pathlock protects digital enterprises from the inside out. Our access orchestration solution supports companies on their journey to Zero Trust by surfacing violations and taking action to prevent loss. Enterprises can manage all aspects of access governance in a single platform, including user provisioning and temporary elevation, ongoing User Access Reviews, control testing, transaction monitoring, and audit preparation.