pathlock

EBOOK

Manual Access Control Can’t Keep Up?

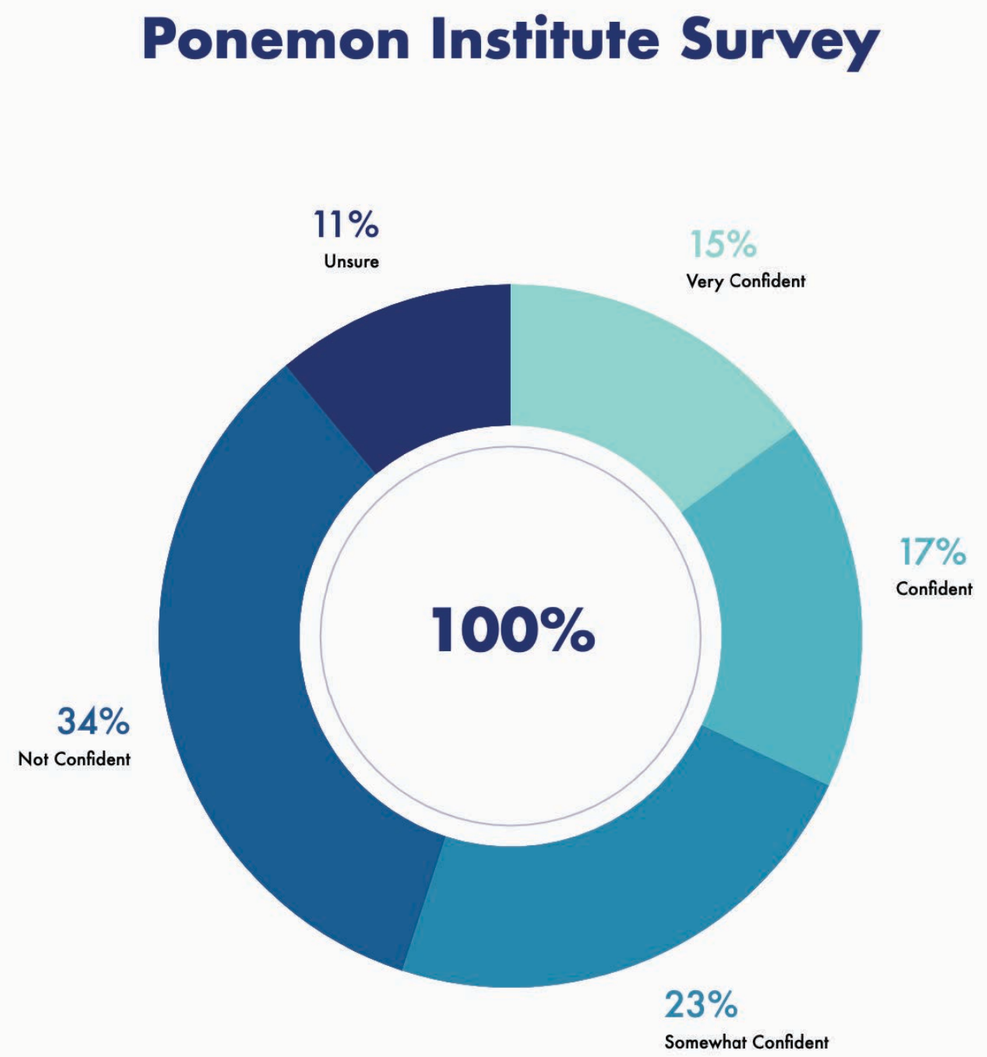
How to Extend Your Compliance Programs to SAP Cloud and Non-SAP Applications.

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

Today's access controls

are usually enforced at the application level which means each access control regimen is effectively "siloed" one can't "see" the other. It's challenging enough to manage access within a single application. Managing that kind of access across all enterprise applications, across thousands of users, and across multiple business processes the scale of complexity skyrockets. And adding to that complexity is that these applications may be on premise or in the cloud.

Factor in the reality that user access requirements changes often. People transfer to other departments and divisions. New responsibilities emerge. Users get promoted. And new applications come online. Tracking and managing that constant change is a significant challenge.



How confident are you that your organization has enterprise-wide visibility for user access and can determine if it is compliant with policies.

Ponemon Institute Survey Drive Responsibility for Governing User Access into the Business

> ***"This project was extremely successful. Working with existing resources, we can now manage critical role-based access in a complex cloud landscape that integrates ERP, identity management, and procurement solutions from SAP.***
>
> Information Systems Manager, Identity Management, Maple Leaf Foods Inc.

What's more, there's no audit trail of these activities. So the spreadsheets get emailed to business owners, they're manually updated, and mailed back to the security/administration team, which must determine what actions to take if the manager wants to revoke access for certain tasks and certain users.

More importantly, what happens when user access spans multiple applications? Who is responsible for gathering the data and manipulating it for easy consumption? (Too often, that data is highly technical and not very actionable.)

How pervasive is the business-controls problem? A recent study by ACFE found that "a lack of internal controls, such as segregation of duties, was cited as the biggest deficiency" in control weaknesses that can lead to fraud. In its "Access Governance Trends Survey," Ponemon Institute LLC found that 57 percent of organizations surveyed lack the confidence to know whether their user access practices are compliant because they don't have enterprise-wide visibility of that user access.

What enterprises need is a way to abstract the system-level complexity and aggregate it across systems so that we can rationalize and reconcile a user's entire set of access privileges. The way to achieve this is through a business-process lens – not an application-specific lens. We need to think like a business user by providing a business-friendly context. It's the business users who know what's required for job functions and whether to accept or manage any given risk. A business oriented lens recognizes that the controls enterprises need are process-specific and can often span multiple applications and systems, each with their own access-control model/protocols.

Achieving Visibility into Access Risk

The only way to achieve proper risk mitigation and remediation is to obtain the committed involvement of the appropriate business managers – but many are reluctant to do so, feeling that systems access is an IT-only issue. That's not the case, of course. While IT may drive the methodology of how systems are secured (often the security model is quite complex), the business manager is responsible for the policy of the security model – such as approving who has access to their business.

Business users need an automated way to see user access data across all applications, and that requires a sophisticated infrastructure to collect that access data, normalize security models across multiple applications, and aggregate for business (not technical) reporting. That aggregation must span on-premise, hosted, or cloud-based applications. That data must also be collected continuously so that business users can work with the access data that exists in the application at any given moment. Outdated batch extraction of user access data with period-based analysis is costly, complex, and error-prone.

A common, centralized mechanism to enforce access policies enables you to implement a single set of controls that span multiple applications. That eliminates the repetitiveness and complexity of managing access controls in "application silos" and ensures that access policies are applied consistently across the entire organization.

> ***"By focusing on actual SoD events rather than possible SoD events, we reduced the amount of data we have to review by 95%. With more than 15,000 users in our monitoring scope, Pathlock has significantly increased our efficiency."***
>
> Senior Director of Finance,
> Jabil Circuit Inc.

Understanding Access Risks

Risk analysis is more than simply understanding who has access to what services. It's also about what they are doing with their access. A proper analysis of access risk enables the organization to understand the risks and prioritize risk-resolution activities, because not all risks are equal. A detailed analysis of segregation of duties (SoD) risks will show business-application owners precisely which users have potentially toxic combinations of access privileges. But more than that, the analysis must go further and identify users who actually conducted transactions that constitute SoD violations. This crucial ability to determine who has the potential to commit an SoD violation vs. who actually committed an SoD violation helps to quickly prioritize the risks that must be addressed first.

For example, if there are SoD concerns about data being updated, you don't want to see records where the user simply changed a customer's fax number –an update that has no bearing whatsoever on the company's risk exposure. Of course, if the employee changed payment terms or credit limits, it has a meaningful impact and could violate company policies. The security administrator needs flexible controls to fetch transactional details to produce mitigation reports and to ensure that only key data correlated with SoD violations is retrieved. A fine-grained understanding of what users are doing with their access privileges enables you to eliminate "false positive" risks.

Powerful analytics and comprehensive reporting are needed to analyze the impact of different scenarios used in managing the "role life-cycle" and satisfy the requirements of line-of-business users, auditors, and IT security professionals. For instance, trend analysis helps us view and understand the enterprise's compliance posture at any given time, such as viewing violations across users and identifying the applications that embody the highest risks. In many cases, simple drill-down dashboards help the business understand why access risks are occurring. For example, the analytics might show risks by user, risk type and location so that business users can better understand how to resolve the risk.

In all instances, proper analysis depends on a clean, clear presentation of user-access data in a business-friendly context through an intuitive user interface. Only through this accessibility and legibility/clarity can line-of-business owners take the responsibility for governing user access.

Risk Mitigation

At its core, risk-resolution revolves around the ability to orchestrate a process (or series of related processes) that involves a cross-functional team of directly accountable stakeholders, such as application owners, security practitioners, IT professionals, and others. These are the people who must make the policies and decisions about when to maintain privileges and when to revoke them. Failure to orchestrate this process to resolve identified risks can lead to unacceptable compliance gaps relating to access risks.

> ***"Leveraging innovative solutions like SAP Access Control and Pathlock allows Sharp to do more and maximize resources. For example, we achieved an 80% reduction in IT personnel time required to manage access governance and SoD controls. This translates to a reduction of 300 hours per month spent on SoD monitoring. In addition, we increased the number of systems managed by SAP Access Control by 33%."***
>
> Associate Director, Information Security
> Sharp Electronics Corporation

So how should we orchestrate this process? Access-risk resolution is predicated on the ability to deliver timely and accurate information on user-access policy violations within their departments. One of the simplest steps to take is to automate the revocation of access entitlements that create policy violations. That can happen through a fully automated approach that leverages a direct entitlement change-management action for the target application. Alternatively, we can use a semi-automated approach, where a help-desk ticket is opened to route the revocation request to the application owner. Semi-automated approaches are somewhat less appealing, however, because they have an inherent level of latency. It's not atypical for an application owner to set aside such revocation requests and handle them in a single batch session every week or two. Such delays introduce compliance issues because valid access credentials remain unprovoked for days or weeks.

Monitoring and Mitigating the Risks

Of course, risks are part and parcel of any enterprise's operations –it wouldn't be unusual for a large organization to have hundreds of access-risk gaps that must be investigated and assessed and whose legitimacy must be confirmed. Inevitably, you will have a subset of individuals who must have access to a broad range of systems, processes, and transactions to perform key tasks that create SoD violations.

Application monitoring of risks –such as SoD transactions –involves correlating transactions to the users who conduct them. Capturing SoD transactions also enables organizations to put compensating controls in place and greatly streamlines and simplifies audit prep and reporting. For instance, it helps organizations focus external audit resources on actual SoD risks that are occurring, as opposed to the mere potential to conduct an SoD transaction.

An automated solution can quickly and consistently interrogate every transaction for a given user that presents a potential SoD issue, ensuring a consistent review using the same criteria across the organization. What's more, through tighter definitions of SoD violations, the automated solution eliminates the false positives –the results show only true SoD violations that merit review.

Since the volume of this activity can be very high, automated controls are necessary to filter thousands or hundreds of thousands of transactional details, correlate the data across the user's activities, and present that data in an easily consumable format. Email notifications can advise process owners about exceptions –and only exceptions –that merit further investigation. Not only can the process owner then conduct the review and documentation online, the audit team can also perform its review online as well. This can reduce or eliminate costs by eliminating the need for audit travel expenses since a manual review of hardcopy documentation is no longer necessary.

Conclusion

With Pathlock you can quickly ensure your enterprise landscape is secure, respond to suspicious activity and analyze business activity for risk or compliance issues.

Pathlock

- Lowers the internal cost of control monitoring, testing and reporting by 80% over manual approaches
- Minimizes the risk of insider threat by alerting and responding to suspicious activity
- Monitors real-time risk across SAP cloud, Workday, Salesforce.com, Oracle, Kronos and other business applications to establish consistent access compliance policies
- Automates manual mitigating/compensating SoD controls with 100% transaction monitoring
- Facilitates timely reviews via automation

Organizations who perform manual controls once or twice per year (due to resource intensive control requirements) can now monitor weekly or monthly which greatly decreases the amount of time fraudulent or inappropriate activity goes unnoticed.

In addition, Pathlock ensures transparency to the financial impact that risk has on your supply chain processes. It provides real-time visibility to the financial exposure caused by issues as they occur in order to drive change that reduces your overall risk exposure. It enables you to:

- Focus on materialized risks as they occur with 100% transaction monitoring
- Quantify the financial exposure of risk to drive business change and support business transformation.

About Pathlock Technologies

Leading global companies rely on Pathlock Technologies to make managing risk and staying ahead of audit issues easier and more cost-effective. Pathlock has the only solution that monitors everything – all applications, all users, all transactions, all risks – all the time and automatically identifies, analyzes, calculates financial impact, and reports on actual user risks; so the business understands the financial exposure the risks present and can easily act on them. Stop manually monitoring data samples. Pathlock provides an easier, more comprehensive, consistent and cost-effective approach to managing policy compliance enterprise wide. Our customers have saved millions in labor costs, audit fees and loss prevention.