pathlock

Insider Threat Monitoring and Incident Response for Critical Business Applications

Get 360-degree visibility into your critical business applications, with turnkey integration, correlation, and rule sets for 140+ applications.

Insider threats are on the rise

Economic uncertainty has stressed the supply chain and personal finances, spurring an explosion of fraud and magnifying the need for control and enforcement. Negligent or malicious insider behavior, often the most damaging threat to the enterprise, is also hardest to uncover because it can't be detected with simple controls around device, login location, or time of day.

Business applications are concentrated risk stores

Applications are often a security blind spot for security operations teams. Most enterprises rely on 10+ applications to support day-to-day processes, which often operate in silos, off the radar of the SOC. Even though 77% of the world's revenue touches an SAP system, It's a struggle to protect critical data in apps such as SAP, Oracle, Workday, Salesforce, and NetSuite.

A mix of cloud and on-premises tooling and diverse security models further complicates the issue. Legacy solutions can tackle the traditional on-premise applications such as SAP and Oracle, but struggle to integrate to modern, cloud based solutions like Salesforce or Workday. Newer, cloud based solutions can tackle the more modern applications but can't provide coverage for the on-premise environment. Without a comprehensive solution to tackle both environments, you aren't able to monitor application usage, identify risks, and stop threats in their tracks.

SIEM solutions leave applications as an afterthought

SOCs often use SIEM tools as a hub for monitoring and alerts. SIEM tools are broad and focused mostly on detecting anomalies at the network and device level. When you try to build integrations between SIEMs and business applications, you're often saddled with hundreds of false positives indicating access conflicts and violations. Security teams often suffer from "alert fatigue" because it's so difficult to find the needle in the haystack that really matters.

Enterprises also struggle with retaining application monitoring data. Data is often kept in multiple systems, disconnected from central auditing platforms, and isn't easily searchable for post-incident forensics. Plus, billions of event logs can lead to massive bills for processing and storage.

Despite the volume of data, there isn't enough detail on relevant access policies for teams to take action and they require additional manual forensics. For these reasons, many organizations stop using anomaly detection solutions altogether.

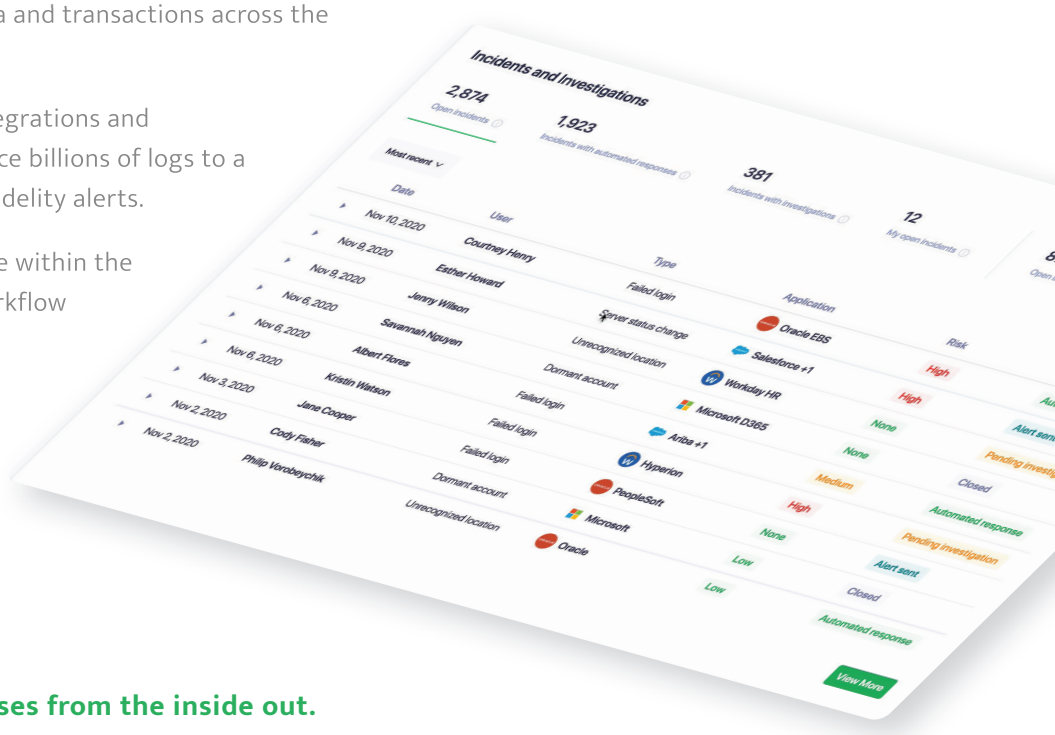
How well do you understand the applications your business users access and what transactions they execute? Would you be able to respond to unusual activity in time to prevent fraud?

Add Business Application Protection to the SOC with Pathlock

Discover and classify data	Identity risky user behavior	Stop threats in their tracks
Determine where personal and sensitive data reside within all of your business-critical applications so you can mask data, measure risk, and set priorities for monitoring and access controls.	A rich catalog of 500+ rules can detect suspicious activity. Deep transactional monitoring correlates events into consumable, accurate alerts for investigation and response.	Integration across the all business-critical applications in your IT environment allows you to automatically terminate sessions and block transactions in real-time.

Seamless SIEM and SOAR integration

- **Visibility.** By integrating applications and SIEM tools, you gain visibility and control over data and transactions across the entire enterprise.
- **Accuracy.** Out-of-the-box integrations and comprehensive rule sets reduce billions of logs to a manageable volume of high-fidelity alerts.
- **Adoption.** SOC teams operate within the security technologies and workflow they use every day, ensuring high rates of adoption.



Pathlock protects digital enterprises from the inside out.

Pathlock supports companies on their journey to Zero Trust by surfacing violations and taking action to prevent loss. Our 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.

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