innerActiv Insider Risk Intelligence Platform

Fast, actionable insider risk intelligence platform that analyzes employee, endpoint and data activity to expose risk and protect your organization from within

Digital and Remote Workforce Monitoring

Gain operational and employee observability to spotlight accidental or malicious threats.

- Configure custom monitoring policies with varying privileges to secure the organization and ensure employee privacy
- Understand activity including resource consumption, application, data and web usage, active hours, and other concerns
- Analyze and trend changes in behavior and workflows to instantly identify high-risk employees
- Enforce policies regardless of whether the user is on or off-network
- Correlate data points across multiple time zones and regions
- Customizable options to notify and interact with end users or operate fully silent "stealth" mode

Data Loss Prevention

Keep the most sensitive data safe across all channels, on and off the network.

- Monitor access and handling of sensitive data, proprietary data, PII, account information and more
- Identify unapproved or atypical usage of data on the network or in email, social, and employee collaboration tools
- Understand when data is being changed or removed from secure repositories
- Block data from crossing critical exfiltration points such as outgoing email, uploads to third party locations, and printing
- Alert on potential data dump activity such as bulk moves or large file transfers
- Automated management of sensitive data in motion on printers, removable drives, or webmail uploads

System, Application, and Endpoint Inspection

Prevent threats on user endpoints by detecting and blocking abnormal or suspicious activity.

- Security oversight and continuous inspection of all systems and endpoint devices including cloud services, offsite computers, and peripherals such as Lexmark printers
- Real-time alerts for concerns like file tampering, unauthorized server access, remote access, or data removal
- Trend and risk telemetry to uncover unknown or hidden threats from everyday usage and privileged users
- Alerting or termination of unknown and unapproved processes at the endpoint, and applications new to the environment

Real-time Actionable Insights

Ensure proactive defense and investigation readiness for compliance or security anomalies.

- Realtime and continuous detailed activity metrics
- Instantly receive emails or SIEM level alerting on critical events
- Dashboard views and investigation tools to review incidents and gain instant knowledge of "who, what, when, why and where" happened
- Optional end-user interactions for education, warnings, and blocking for critical events
- Root cause anlaysis of incidents and potential risks allowing issues to be tackled before becoming a critical event

Compliance Without Compromising Productivity

Mitigate security and compliance risk without compromising workforce experience.

- Centralized control to quickly detect, analyze, and contain suspicious activity
- At-a-glance status of regulatory compliance by individual user, group, department, or the entire organization
- Built-in case management with deep event forensic details, history and screen captures of all incidents