innerActiv

SOLUTION BRIEF

innerActiv Insider Risk Intelligence Platform

Protect from within

In today's relentless cyber threat landscape, it's common for companies to spend time, money and effort to protect themselves from external attacks. However, the worst threats might be sitting right in front of you, operating from the inside, risking the exposure of trade secrets, customer data and more. With so many employees, contractors, partners and vendors with legitimate access to company systems, it's easy for malicious or even unintentional leaks to occur.

Now with innerActiv, approach your defense from the inside out versus the outside in. Powerful analytics look across user behavior and data movement on endpoints, networks, in the cloud, and on-premises, to provide complete visibility, detection, prevention, and response to potential insider threat situations.

By protecting from within, organizations can safeguard their digital workforce from anywhere and build resiliency to meet the evolving cybersecurity threat landscape.

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

Safeguard with full coverage at the endpoint, on the network, and in the cloud

- Security oversight and continuous inspection of all systems and endpoint devices including cloud services, offsite computers, and peripherals
- Real-time alerts for file tampering, unauthorized server access, remote access, or data removal

Secure data in use, at rest and in motion across all channels, on and off the network

- Monitor access and handling of data, proprietary files, PII, account information
- Advanced threat detection in email, mobile, social, and employee collaboration tools
- Automated management of sensitive data in motion on printers, removable drives, or uploads

Protect your digital hybrid workforce with operational observability to spotlight threats

- Trend and risk analysis of employee access and activity including resource consumption, data, application and web usage, active hours and other accountability concerns
- Customizable options to notify and interact with end users or operate in silent "stealth" mode

Respond in real time with actionable insights to irregular or suspicious behavior

- Centralized control to quickly detect, analyze, and contain suspicious activity
- Dashboard views and reports to review risky incidents and gain instant knowledge of "who, what, when, why and where" happened

Mitigate security and compliance risk while ensuring workforce productivity

- Built-in case management with detailed event forensics, history and screen captures
- Timeline and trending information for event categories, to quickly investigate and address ongoing issues or newly developing trends

Build a proactive security defense and increased resiliency to identify gaps

- Configured to specific compliance regulations, whether federal, local, international, or even your corporate policies
- Assign risk scores and compile various factors and signals to trend violation of those policies

Staggering 44% increase insider threat incidents

2022 Ponemon Cost of Insider Threats Global Report

- **Analyze risky behavior**
- **Detect and investigate threats**
- **Contain incidents and minimize impact**
- **Meet compliance and ensure productivity**
- **Prevent future attacks with security resiliency**

Protect from within

Track signs of suspicious and compromised behavior and flag potential insider risk before they become actual threats

Complete 360 view of insider threat

Insider risk is difficult to detect, and if you don't have all the information, you cannot truly understand the problem or the solution. Real-time analytics understand what insider behaviors or actions represent risks and by correlating data across security tools, your organization can trend user behavior and activity for a full 360 view of potential threat.

Realtime insights to triage and contain risk

Often organizations are reactive, addressing data breaches and other threats only after they occur. Real-time alerts to changes in behavioral patterns and/or potential non-compliance concerns such as file tampering, unauthorized server access, remote access, or data removal, allow security teams to triage and contain incidents before damage occurs.

Configured for unique corporate policies

Every rule and feature has been built with highly customizable options that allow for any exclusions that may be necessary to protect the privacy of an organization and its employees. Once configured to your requirements, whether federal, local, international, or even your own corporate policies, various risk factors and signals are compiled into a risk score. Only that data that you request will display to only approved personnel, so there's no concerns about exposure of personal data or sensitive information ending up as public knowledge.

Compliance without compromising workforce productivity

With today's cloud connected, distributed and highly collaborative workforce, employees are your biggest asset and potentially your biggest risk. Secure work practices coupled with intelligence can identify and differentiate between well-meaning employees, and malicious insiders trying to steal sensitive business data. Ensure compliance with built-in case management that stores deep forensic details and history of all incidences.

Turnkey to quickly move from insights to action

When anomalies appear, determining whether the irregularities are, in fact, potential insider threats can be costly to an organization. By anticipating versus reacting to shifts or suspicious activity, lower the cost of investigations and overall operational impact to your organization. innerActiv's flexible framework, deployment, and pricing ensures the right solution to fit your needs. Whether you have 50 users or 500,000, gain risk insights for your organization to take immediate action.

Prepare your organization against insider threat. Learn more at www.innerActiv.com.