innerActiv

SOLUTION BRIEF

Prepare your organization against insider threat

44% increase insider threat incidents since last year

What is insider threat?

An insider threat is a security risk that comes from within your company. Employees, partners, vendors, interns, suppliers or contractors can potentially become an insider threat. These people have legitimate access to your internal network and may accidentally leak or purposely steal sensitive information.

60% of breaches caused by insiders – either maliciously or inadvertently

What types of insiders exist?

Insider threat can be categorized as:

- Unintentional threats, both accidental or due to negligence, occur through carelessness and exposes an organization to a threat
- Intentional threats are actions taken to harm an organization for personal benefit or to act on a personal grievance

85 days incident containment

What are the potential impacts?

- Theft or loss of mission critical data or intellectual property
- Impact of downtime on productivity
- Cost to detect and remediate systems and core business processes
- Loss of competitive edge
- Legal and regulatory impact, including litigation defense cost
- Trust & confidence with stakeholders
- Diminished brand and reputation

2022 Ponemon Cost of Insider Threats Global Report

Warning signs to identify insider threat

Insider threats can affect companies of all sizes in all industries. Whether accidental or intentional insiders can wreak havoc on organizations because they are authorized to access proprietary information including information about security practices, data, and systems.

Accidental

- Opening a phishing email
- Using weak password
- Access attempts to devices or servers containing sensitive data
- Large quantities of data either saved or accessed by a specific user
- Attempted access to external USB ports and printers

Negligent

- Leaving a highly sensitive laptop unattended
- Forgetting to log out before leaving work
- Emails containing sensitive data sent to a third party or unsecured location in the cloud
- Not keeping devices and services patched/upgraded to latest versions

Malicious

- Remote network and data access at irregular hours
- Frequent data access requests unrelated to job
- Installing unauthorized software
- Multiple attempts to access blocked websites
- Disabling of antivirus tools and firewall settings
- Malware installation

How prepared is your organization in mitigating insider threat?

innerActiv insider Risk Intelligence Platform

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

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

Protect from within

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

---

Analyze risky behavior

The vast majority of security threats follow a pattern or sequence of activity leading up to an attack, and insider threats are no exception. Insider threat intelligence is needed to measure, detect and contain undesirable behavior of trusted accounts within an organization. Through continuous monitoring of user and system access, activity and data movement, a baseline of trusted behavior can be established to bring risks that you may not even notice to light.

Detect and investigate threats in real time

Insider threats can be harder to identify or prevent than outside attacks and are invisible to traditional security solutions like firewalls and intrusion detection systems. Real-time threat detection monitors all user, data, infrastructure and network activity to identify trends and anomalies based on modeled behavior and custom configured security policies. Alerts and dashboard views provide real-time investigation and knowledge of "who, what, when, why, where" to determine how to respond to any vulnerability.

Contain incidents and minimize impact

When anomalies appear, determining whether the irregularities are, in fact, potential insider threats can be costly to an organization. In fact, according to a recent report from Ponemon, 2022 Cost of Insider Threats Global Report, impacted organizations spent $15.4 million annually on overall remediation and took 85 days to contain each incident. By anticipating versus reacting to workplace shifts or suspicious activity, lower the cost of investigations and overall operational impact to your organization.

Meet 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. Built-in case management with deep forensic details and history of all incidences ensure compliance.

Prevent future attacks with increased security resiliency

When considering cybersecurity planning and readiness, insider threat management can no longer be ignored. Today the most highly regulated industries, such as the public sector and financial services, are leading the way spending on average about twenty-five percent of their security budget to combat insider risk. Proactive defense intelligence and risk telemetry can combat compliance or security anomalies and safeguard your organization.