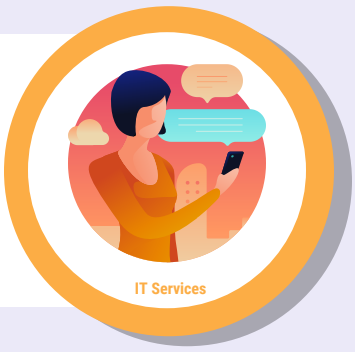
5 Insider Threat Use Cases

#1 Protect sensitive customer and financial data

Financial institution uncovers that its web monitoring software was not restrictive of a particular email client, which was being used to create unauthorized email addresses to open accounts, lines of credit and credit cards. The employee was also privy to customer PII, account numbers and financial data that was shown through usage tracking.

#2 Securely manage a distributed workforce

Technology company needs to securely manage a highly distributed consultant and contractor workforce. Deep analysis of user behavior, data activity and access determined that a consultant was utilizing confidential data, documents and contacts for a similar outside project with a competitor. The detailed forensic data collected was later utilized as evidence in a pending court case.



#3 Investigate security anomalies and incidents

Retailer needed to determine with certainty that select part time employees were fraudulently claiming hours on their timesheets that they did not work. Custom user activity monitoring policies provided the retailer with evidence and supporting documentation that employees were reporting hours they did not work by having other employees clock in for them.

#4 Meet compliance initiatives

Bank wanted to understand how security infractions impacted compliance initiatives before a scheduled audit. The organization was able to identify weaknesses and understand who, what, when, why, where actually happened to make necessary adjustments to security policies and deliver compliance reports that satisfied numerous auditor “checkboxes.”

#3 Prepare for company layoff

As the layoff deadline approached, a pharmaceutical company monitored at-risk users and groups along with broader data exfiltration policies to protect proprietary data. Policies continued to be refined throughout the layoff period to also include web usage and keyword monitoring to ensure any confidential information they own was not mishandled or stolen by departing employees.

Steps to protect from within

innerActiv is a leading insider risk intelligence platform enabling global companies of all sizes to proactively mitigate critical risk and protect their most sensitive data. 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, companies can safeguard their digital workforce from anywhere and build resiliency to meet the evolving cybersecurity threat landscape. Learn more at www.innerActiv.com