IMPERVA®

YOUR GREATEST RISK IS ALREADY ON THE PAYROLL

7 STEPS TO PROTECT YOUR DATA AGAINST INSIDER THREATS

When internal users with trusted access to data are careless, become compromised or have malicious intent, enterprise data is exposed. Security teams can use this checklist to evaluate their current data security program and identify gaps pertaining to insider threats.

Steps to Data Protection	How to Detect and Contain Insider Threats
1. Discover and classify sensitive data	Automatically and repeatedly identify business critical information that is exposed to insider risk.
2. Monitor all user access to data	Monitor all users that access databases, file shares and cloud-based apps – not just your privileged users.
3. Define and enforce organizational policies	Immediately prevent unwanted data access behavior and enforce separation of duties.
4. Leverage machine learning to detect unknown threats against enterprise data	Filter through the noise and proactively identify the most worrisome data access incidents.
5. Use interactive analytics tools to investigate security incidents	Enable the SOC team to quickly investigate incidents and understand all data access activities of individual users.
6. Quarantine risky users	Contain risky behavior by granularly quarantining users or blocking access to specific data.
7. Generate reports to document security events	Accurately document all insider-related security incidents.

Learn more at www.imperva.com