A Guide to Insider Threats and How to Prevent Them

A Single Data Breach Costs $3.62 Million

There are 12 types of costs associated with a data breach.

Entry Point Insider Threat Data Breach

-$20K–$10M
-$11.3M–$115M
-$200K–$2000
21%
20%–50%

Entry Points + Insider Threats = Data Breach

Entry points for attackers—such as phishing attacks, unauthorized users, and malware—allow inside threats—such as compromised accounts, infected hosts, and low and slow attacks—to open the door for data breaches to occur.

Not all insider threats are internal employees or disgruntled personnel. Insider threats also include systems compromised by external attackers, infiltrating systems for data staging and data exfiltration, or impersonating legitimate users for unauthorized access.

Not all insider threats are internal employees or disgruntled personnel. Insider threats also include systems compromised by external attackers, infiltrating systems for data staging and data exfiltration, or impersonating legitimate users for unauthorized access.

Most Wanted Insider Threats

Not all insider threats are internal employees or disgruntled personnel. Insider threats also include systems compromised by external attackers, infiltrating systems for data staging and data exfiltration, or impersonating legitimate users for unauthorized access.

Most Wanted Insider Threats

Not all insider threats are internal employees or disgruntled personnel. Insider threats also include systems compromised by external attackers, infiltrating systems for data staging and data exfiltration, or impersonating legitimate users for unauthorized access.

Behavioral Analytics

Micro Focus ArcSight Intelligence behavioral analytics reveals hidden threats by augmenting existing security tools. Its anomaly detection for insider threats complements the pattern matching of rules and thresholds for policy enforcement and the supervised machine learning of malware detection.

Behavioral Analytics

Micro Focus ArcSight Intelligence behavioral analytics reveals hidden threats by augmenting existing security tools. Its anomaly detection for insider threats complements the pattern matching of rules and thresholds for policy enforcement and the supervised machine learning of malware detection.

Behavioral Analytics

Micro Focus ArcSight Intelligence behavioral analytics reveals hidden threats by augmenting existing security tools. Its anomaly detection for insider threats complements the pattern matching of rules and thresholds for policy enforcement and the supervised machine learning of malware detection.

Learn More

Print and required to贯彻落实 recommendation of CISOs.

Learn More

Print and required to贯彻落实 recommendation of CISOs.

Learn More

Print and required to贯彻落实 recommendation of CISOs.