INSIDER THREATS

YOUR BIGGEST SECURITY RISK IS WITHIN

What is an insider threat?

The security risk posed by an enterprise's employees, associates, partners, contractors, and service providers with access to enterprise resources and data is classified as an insider threat. Insider activity is one of the biggest security concerns to enterprise data because perpetrators already operate past the first line of defense.

34% OF ALL BREACHES INVOLVE INTERNAL ACTORS.[1]

Insider threat profiles

Negligent insiders

compromise enterprise security by neglecting to follow cybersecurity policies. They often fall prey to social engineering attacks.

AN EXTENDED PHISHING SCAM COST FACEBOOK AND GOOGLE **$100 MILLION**.[2]

Inadvertent insiders

are employees whose accounts are compromised by external actors. They are unwitting participants in security incidents.

5.2 MILLION RECORDS OF MARRIOTT GUESTS WERE ACCESSED VIA COMPROMISED EMPLOYEE ACCOUNTS.[3]

Malicious insiders

willfully use their legitimate access to critical data to steal, delete, tamper with, or leak it for revenge or personal gain.

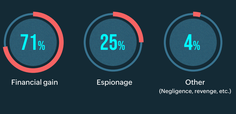
2.9 MILLION RECORDS OF PII WERE EXPOSED BY A VENGEFUL DESJARDINS EMPLOYEE.[4]

Insider threat motivators

According to the

Data Breach Investigations Report,[5]

the primary motivators of data theft are:



The impact of insider attacks

1

Huge monetary losses

The cost per insider attack is between **$100,000 AND $2 MILLION.**[6]

2

Loss of critical data

In 2020, the number of exposed personal data records increased **141%**.[8]

3

Operational disruption

The five-year operational disruption cost for an organization that suffered a data breach was a whopping **$1.2 BILLION.**[7]

4

Loss of credibility

70% of consumers would stop doing business with a company if it experienced a data breach.[9]

Why are insider attacks difficult to combat?

01

Maximized damage potential

59% of insiders had credentialed access to the organization's network and software.[10]

02

Extended detection time

On average, insider threat detection and containment takes **77 DAYS.**[10]

03

Privileged smoke screen

63% of organizations think that privileged users pose the biggest insider risk.[10]

04

Lack of effective detection tools

17% of organizations do not monitor user behavior at all.[10]

How to mitigate insider threats

Consolidate user activity reports

The more visibility you have into your Active Directory environment, the better your chances of detecting insider threats.

Monitor privileged users

A critical component of insider threat detection, monitoring privileged users will help you keep a close eye on users who can cause the most damage.

Track data usage and movement:

Audit all data accesses, including permission changes and data transfers to external storage devices, to detect anomalies quickly.

Deploy user behavior analytics:

Detect, investigate, and mitigate threats like malicious logins, lateral movement, privilege abuse, data breaches, and malware.

Automate security incident responses

Execute responses such as shutting down machines and disconnecting user sessions to mitigate data breaches.

ManageEngine
ADAudit Plus

Combat insider threats with ADAudit Plus

ManageEngine ADAudit Plus is a UBA-driven change auditor that continuously monitors user activity and provides detailed reports to enhance your insider threat detection strategy.

Explore the insider threat detection capabilities of ADAudit Plus using a free, 30-day trial.

Write to us at support@adauditplus.com to schedule a personalized demo.

Download now

Data sourced from:

1. Data breach investigations report 2. CNBC 3. Marriott International 4. Securworld 5. Bitglass - Insider threat report 6. Data Breach Quick View report 7. Beneath the surface of a cyberattack 8. Thales 9. Cybersecurity Insiders - Insider threat report 10. Cost of insider threats