SafeSuite™

NO LEVERAGE, NO RANSOM.

SafeSuite's policy-driven data protection eliminates exposure as a ransom threat.

The evolution of ransomware

Ransomware is no longer about locking you out, but rather, letting everyone in. Modern ransomware attacks have evolved to include not just encryption of files, but also exfiltration of sensitive data. Attackers then threaten to leak that data publicly unless a ransom is paid. And in many cases, it's the threat of exposure – not disruption – that delivers the bigger payday.

$2M
average ransom payment[1]

24 days
average downtime[2]

94%
ransomware with data leak threats[3]

$5.21M
avg. cost of data extortion attacks[4]

Don't repeat history

Change Healthcare (2024)
- Health data of 100M patients
- $22M ransom paid

Minneapolis Public Schools (2023)
- $4.5M ransom demand not paid
- Student & staff records leaked

Caesars Entertainment (2023)
- Personal data of 65M+ customers
- $30M demanded, $15M paid

Mitigate threats with SafeSuite™

Prevents leverage: files remain encrypted and inaccessible to unauthorized users.

Revocable access: admin can revoke and modify access even after exfiltration.

Traceability: forensics and audit trails of access attempts are logged, aiding investigations.

1 Sophos 2024; 2 Palo Alto Networks 2024; 3 BlackFog 2024; 4 IBM 2024

Colorado keyavi.com info@keyavi.com