Digital
Asset
Redemption

Your Ransomware Event Is Over.

(SO WHAT DO YOU DO NOW?)

The dust is settling after your ransomware event. Things are getting back to normal (hopefully). But what comes next?

✗ DON'T:

ASSUME THE THREAT IS FULLY NEUTRALIZED

Paying the ransom and restoring data doesn't guarantee the attackers haven't left other vulnerabilities as parting gifts. Don't skip a full forensic audit to ensure no hidden threats remain in your network.

NEGLECT EMPLOYEE SECURITY TRAINING

68% of all ransomware events involve social engineering. Reinforce employee awareness with phishing training and protocol refreshers to avoid further compromises.

BLINDLY TRUST THE THREAT ACTOR

Leaked data is leaked forever, even if the attackers claimed they deleted it. . Often, it later appears somewhere on the dark web. Continue to monitor for leaks as criminals might attempt to resell or reuse sensitive data or access into your system.

IGNORE SOFTWARE UPDATES

Unpatched software can act as a treasure map to your data. Prioritize patches and updates for both systems and end users.

OVERLOOK THIRD-PARTY ACCESS AND RISKS

Ensure you have a full view of your third-party environment and evaluate access, usage, and privileges to reduce your risk of an attack through those vendors

✓ DO:

MONITOR SYSTEMS AND NETWORK FOR RESIDUAL THREATS

Conduct a thorough sweep to identify any backdoors or lingering malware. Advanced Persistent Threats (APTs) may remain; monitoring can help catch further malicious activity or prevent another extortion event.

REVISE AND IMPROVE YOUR INCIDENT RESPONSE PLANS

Take this time to shore up your incident response plan while the process and experience are fresh so that you can feel confident on what to do and who to call should you experience another extortion event.

IMPLEMENT DATA LEAK MONITORING

Threat actors aren't trustworthy and may still leak sensitive data. Use dark web monitoring tools and specialized services to track and neutralize any potential data exposure or unauthorized dissemination of your company's information.

STRENGTHEN ACCESS CONTROLS

Implement stronger authentication methods and identity and regularly review and update user access privileges.

SECURE AND VERIFY BACKUPS AND PROCEDURES

Ensure that backups are clean, up-to-date, immutable, and securely stored offline. Restoring from backups is critical, but you must verify they haven't been compromised or encrypted during the attack.