Zero Trust….Assume Compromise

> The main reason to look at backup now is ransomware.
> **Thick walls are not enough.”**

Leading Security Software Vendor | **CIO**

RANSOMWARE, BY THE NUMBERS

Increase in ransomware attacks, fueled by the pandemic: **148%**

Anticipated global ransomware recovery costs by the end of 2021: **$20 billion**

Average ransom demand in Q4 2020: **$154,108** (-34% from Q3 2020)

Average days of downtime in Q4 2020: **21 days** (+11% from Q3 2020)

Percentage of ransomware in Q4 that included the threat to leak exfiltrated data: **70%** (+43% from Q3 2020)

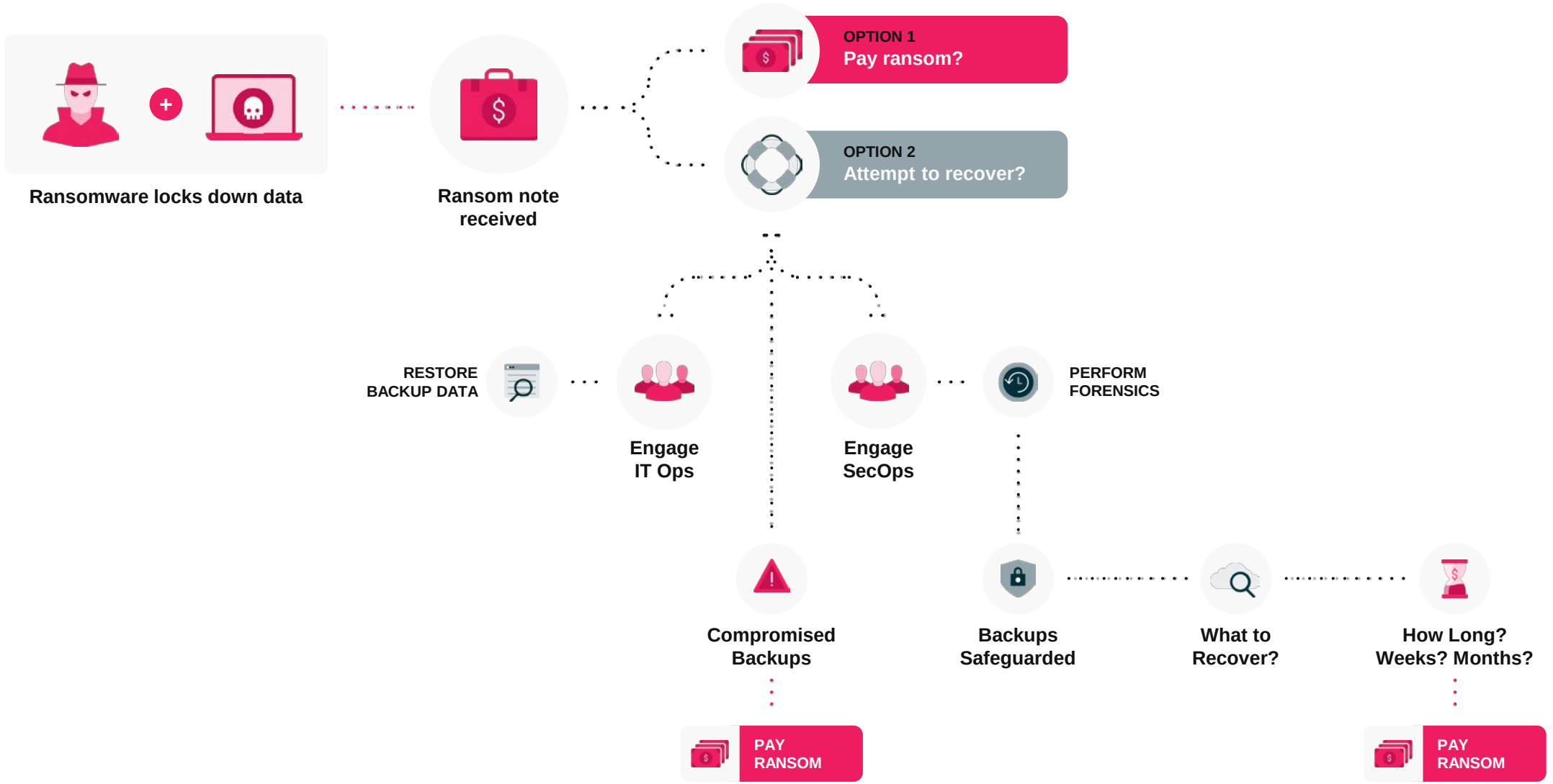
How quickly a new Remote Desktop Protocol (RDP) port — one of the top three ransomware attack vectors — is discovered after first connecting to the Internet: **90 seconds**

How many misconfigured RDP ports are open to the Internet: **4.7 million**

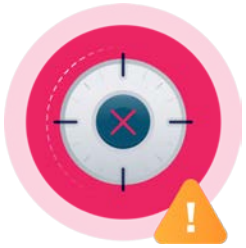
Average number of ransomware attacks that have occurred daily since January 1, 2016: **4,000**

Email messages that contain malware (email phishing is also included in the top three ransomware attack vectors): **1 in 3,000**

The anatomy of a Ransomware attack



The Problem With Ransomware Recovery Today

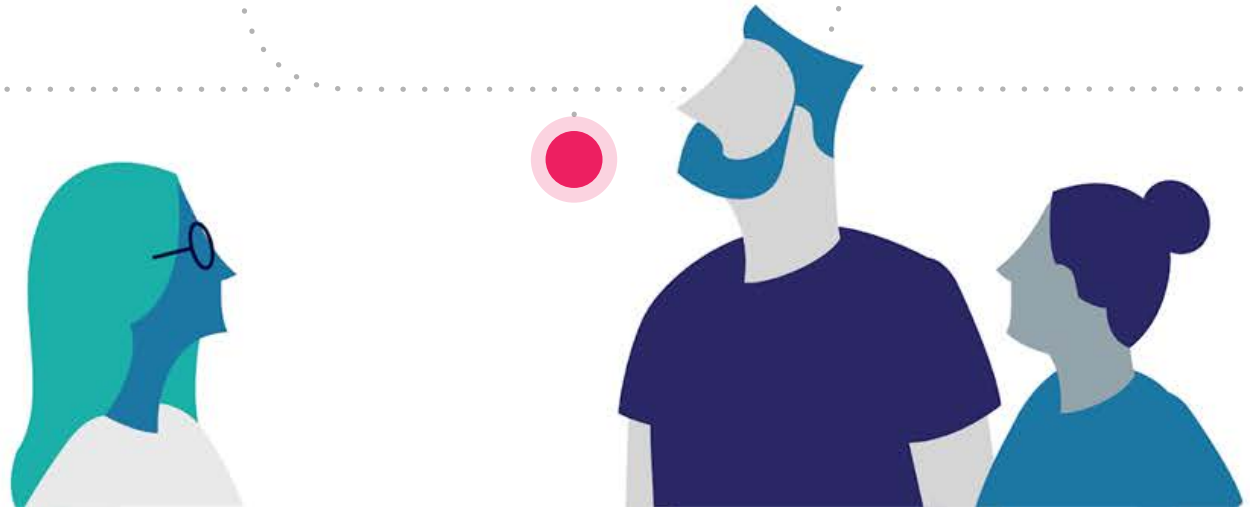


Target back-up systems via open protocols

Extremely difficult to assess 'blast radius'

Is high-value, sensitive data affected?

Recovery is too slow – SecOps and ITOps disconnected



The Rubrik Approach: Zero Trust Data Management

Native Immutability

Data is air-gapped and cannot be accessed or encrypted by ransomware

Scoped Anomaly Detection

Assess what data has been impacted and determine blast radius of attack

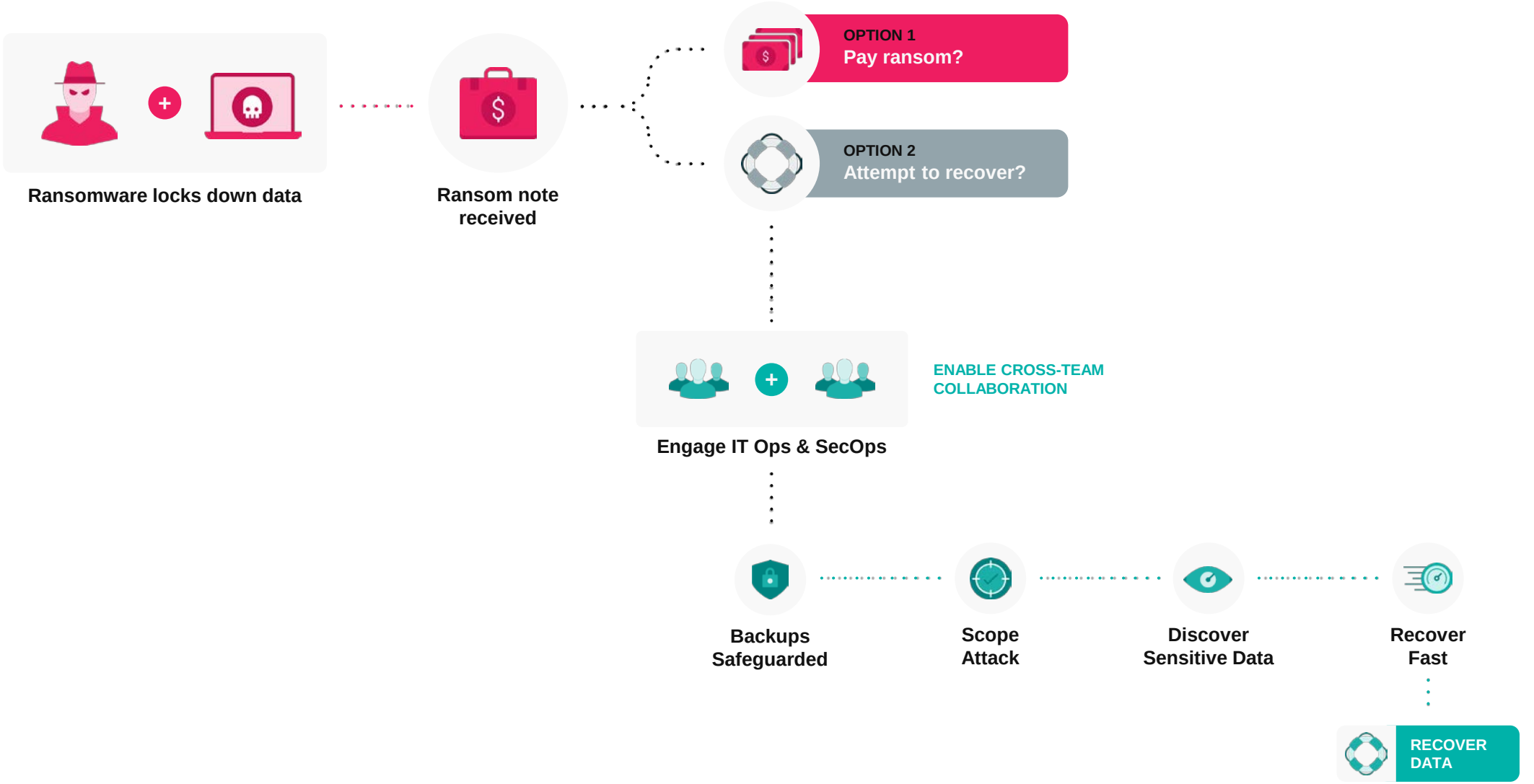
Sensitive Data Assessment

Discover if sensitive data is at risk

Expert Guided Recovery

Automated recovery playbook to get your application the nearest clean data, with sequencing order and recovery type

Rubrik’ Security at the Point of Data



Ransomware Recovery Warranty

Rubrik offers $5M ransomware recovery warranty for Rubrik Enterprise Edition, delivering the ultimate peace of mind.

Learn more

Secure backup checklist

1. Are our backups air-gapped and natively immutable?
2. Are Logins secured with Multi-Factor Authentication and Time-Based One-Time Pin?
3. Retention Lock – Is their any way to expire backups prematurely?
4. Detect & Recover – Can we detect simulated ransomware attacks and automate recovery?
5. Analyze Impact – Can we Automatically detect sensitive data in backups?

rubrik