Ransomware Cheat Sheet

ProLion

RANSOMWARE FACTS & FIGURES

85% *of all companies are being attacked**

21 days *average down-time ****

40 Mio. Dollar *was the highest ransom paid***

300,000 USD *is the average ransom paid*

*https://venturebeat.com/2022/03/01/report-85-of-companies-experience-at-least-one-ransomware-attack-per-year/
**https://www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack
*** https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020

What is Ransomware?

Ransomware actors are mainly focusing on organizations' data to gain financial advantages. They are increasingly deploying a so-called double extortion strategy to increase the pressure to pay the ransom.

By utilizing this tactic, data is stolen first and then encrypted as a Denial-of-Service attack. If the ransom is not paid in order to retrieve the decryption key, cybercriminals increase the pressure by threatening to leak the data to the public or sell it on to other parties.

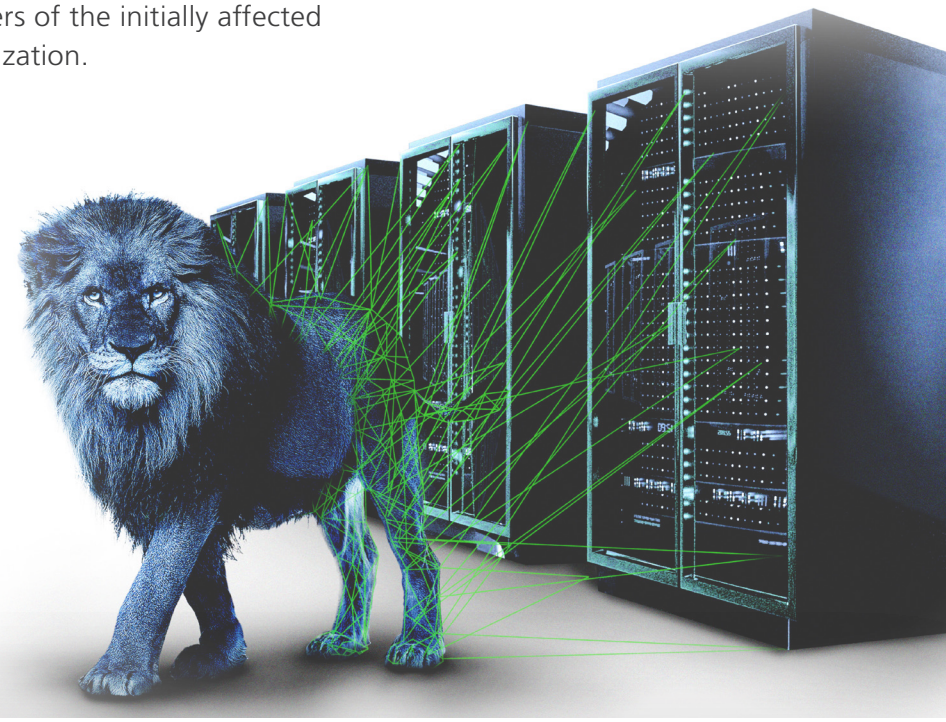
Often hackers also retrieve sensitive data about third parties during an attack. They often use to also blackmail customers, suppliers or partners of the initially affected organization.

Ransomware and data / the storage

Ransomware actors are mainly focusing on organizations' data to gain financial advantages. They are increasingly deploying a so-called double extortion strategy to increase the pressure to pay the ransom.

By utilizing this tactic, data is stolen first and then encrypted as a Denial-of-Service attack. If the ransom is not paid in order to retrieve the decryption key, cybercriminals increase the pressure by threatening to leak the data to the public or sell it on to other parties.

Often hackers also retrieve sensitive data about third parties during an attack. They often use to also blackmail customers, suppliers or partners of the initially affected organization.

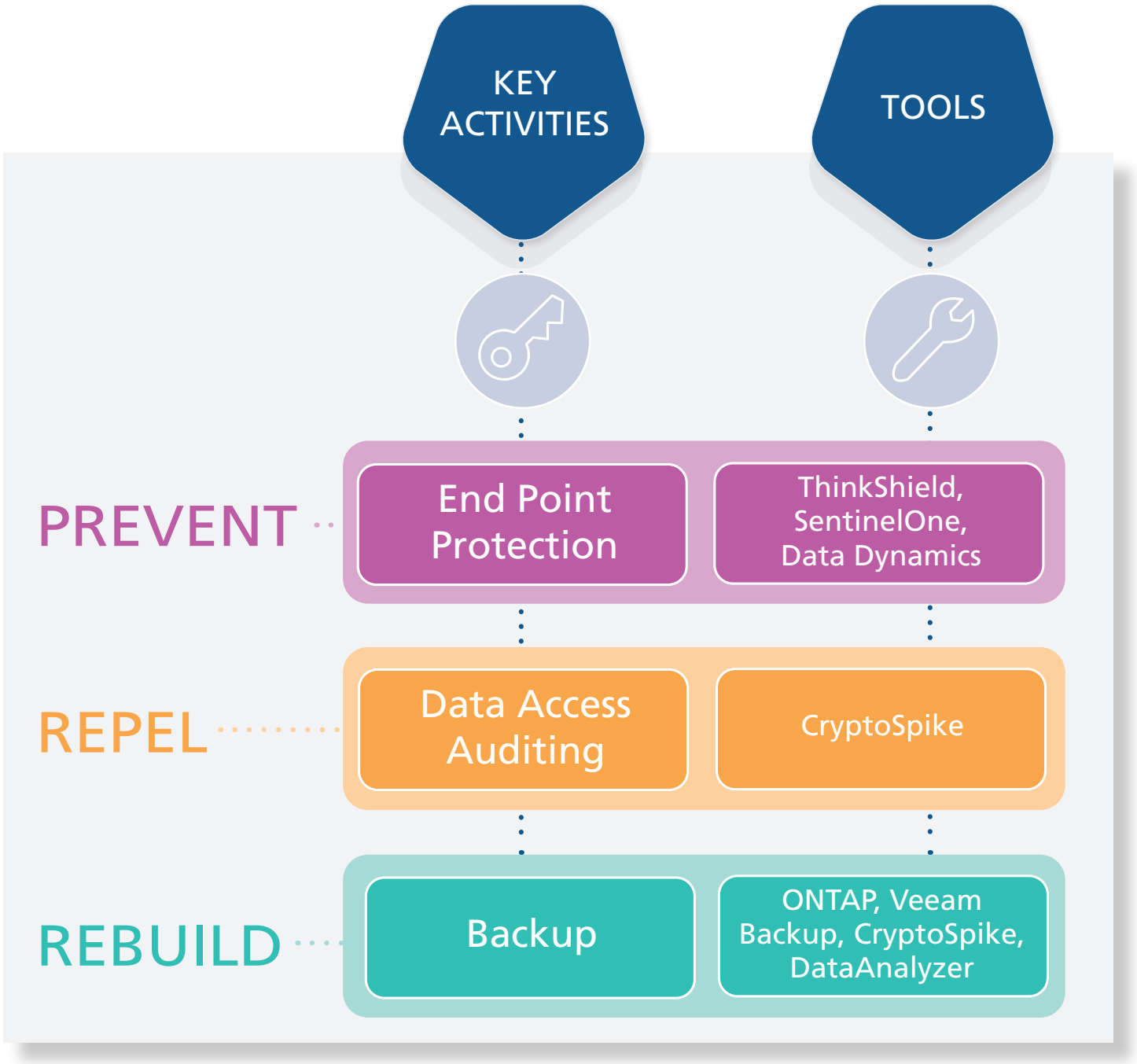


How to defend

Companies have reacted to the growing threat of ransomware by improving backup and restore processes so cyber criminals are adapting their techniques putting more emphasis on compromising backups as well as data exfiltration.

In this scenario backups and recovery plans become largely redundant, meaning that you need to have a far more comprehensive strategy than just data backups and improved recovery plans.

In order to tackle the threat of ransomware, a multi-layer defense approach is recommended:



For further information visit our website at www.prolion.com or get in touch with contact@prolion.com