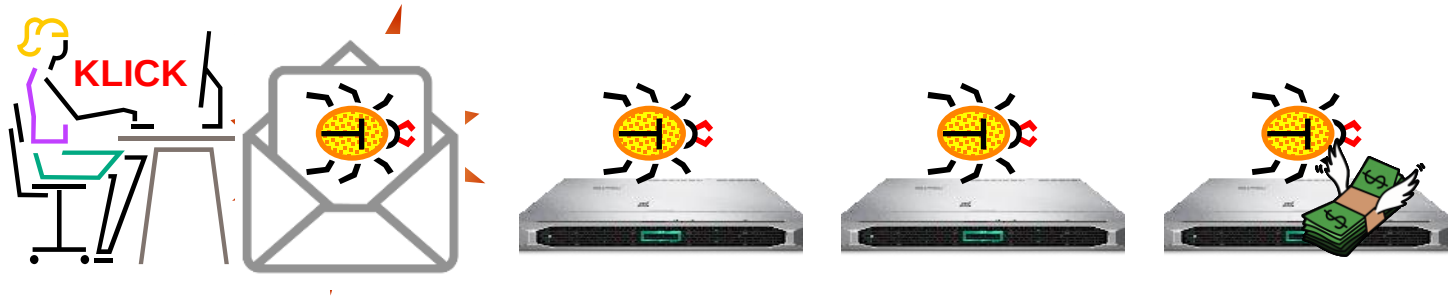
Hewlett Packard Enterprise

Cyber Resilience discussion

James Watson-Hall – Worldwide CTO Hybrid IT
May 2024

Some numbers/ stats….

- **Ransomware is a specific type of malware that holds files hostage and demands payment to release them.**
- **Global ransomware damages are estimated to exceed $60 billion by 2024.**
- **73% of organizations experienced a ransomware attack in 2022/23.**
- **80% of organizations who pay a ransom will be attacked again**
- **Cyber insurance pays out** in almost all ransomware claims (98%), but only **4% recovered all their data**.
- **In 40% of cases**, companies **will lay off employees** because of the damages.
- 69% of ransomware attacks begin with an email.



Source-1: https://tech.co/antivirus-software/ransomware-statistics
Source-2: https://assets.sophos.com/X24WTUEQ/at/4zpw59pnkpxxnhfhgj9bxgj9/sophos-state-of-ransomware-2022-wp.pdf
Source-3: https://www.ibm.com/downloads/cas/3R8N1DZJ
Source-4: https://www.barracuda.com/reports/ransomware-insights-report-2023

Meanwhile in the real world....

REAL LIFE – Customers attacked and the impact

Healthcare

Insurance

Retail

Large UK FSI

© Commvault 2023

Some Facts

Ransomware is a booming business

Every company will be attacked

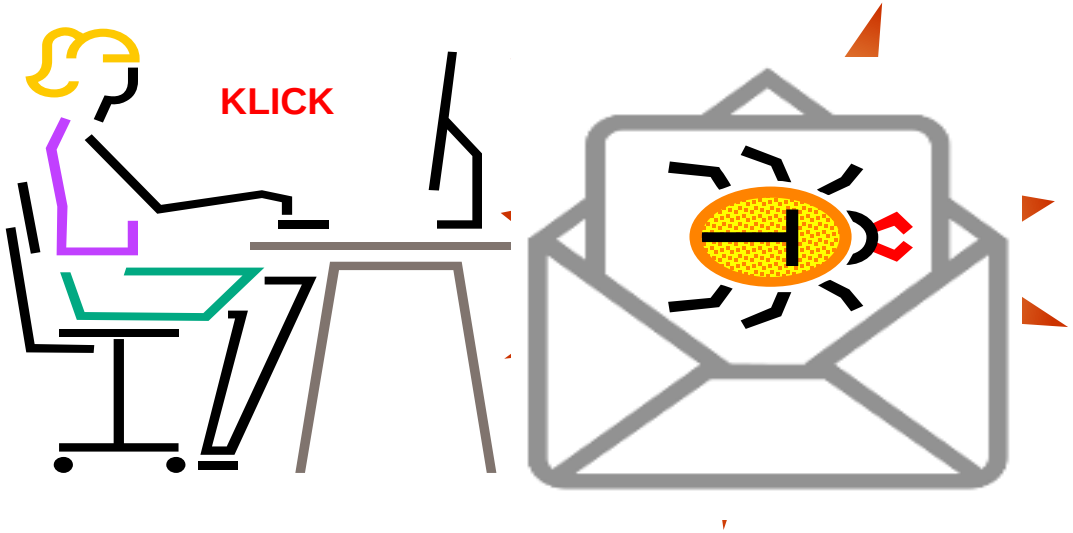
Attacks are planned and well targeted

One vendors technology is not a strategy

© Commvault 2023

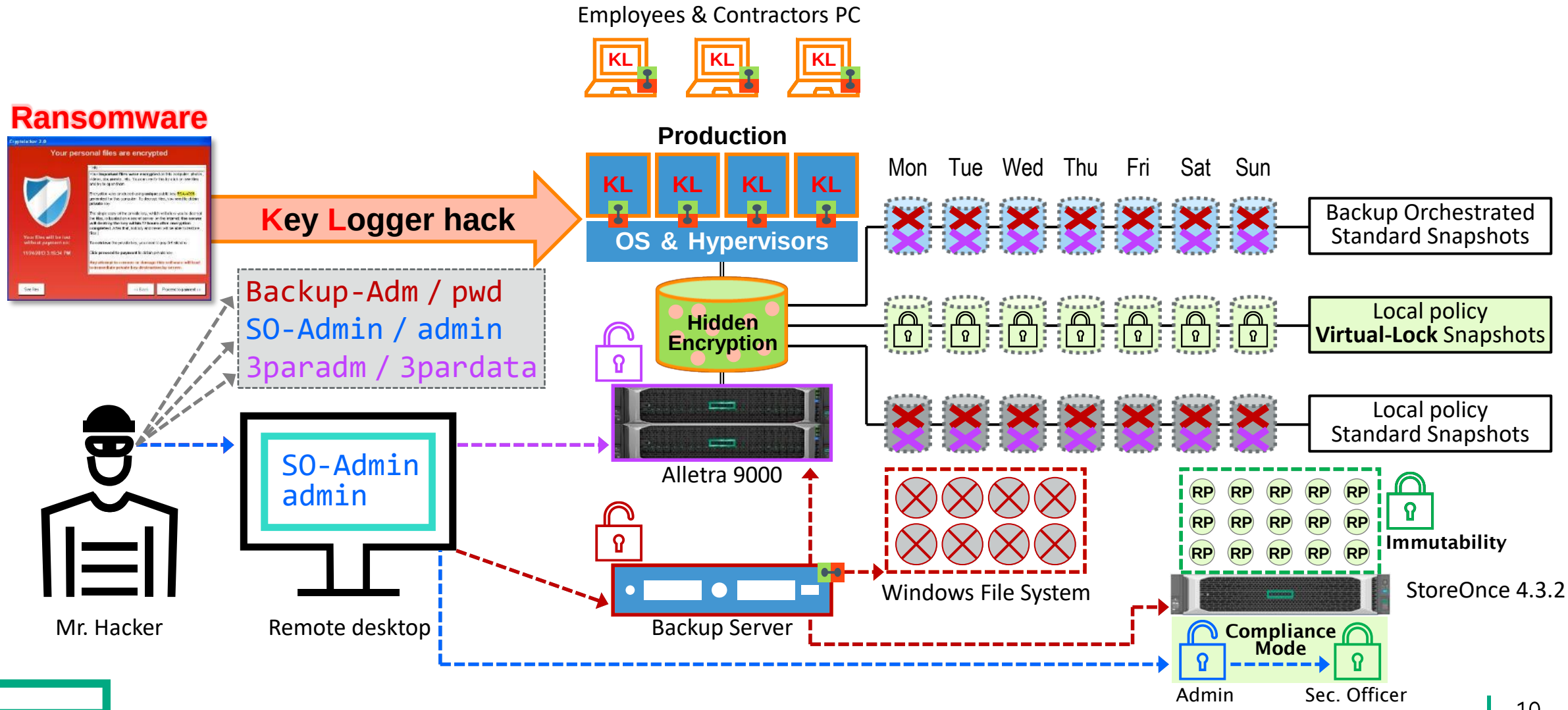
Zero trust blah blah....

People (largely) are the weak link



Think Recovery, that is what counts!

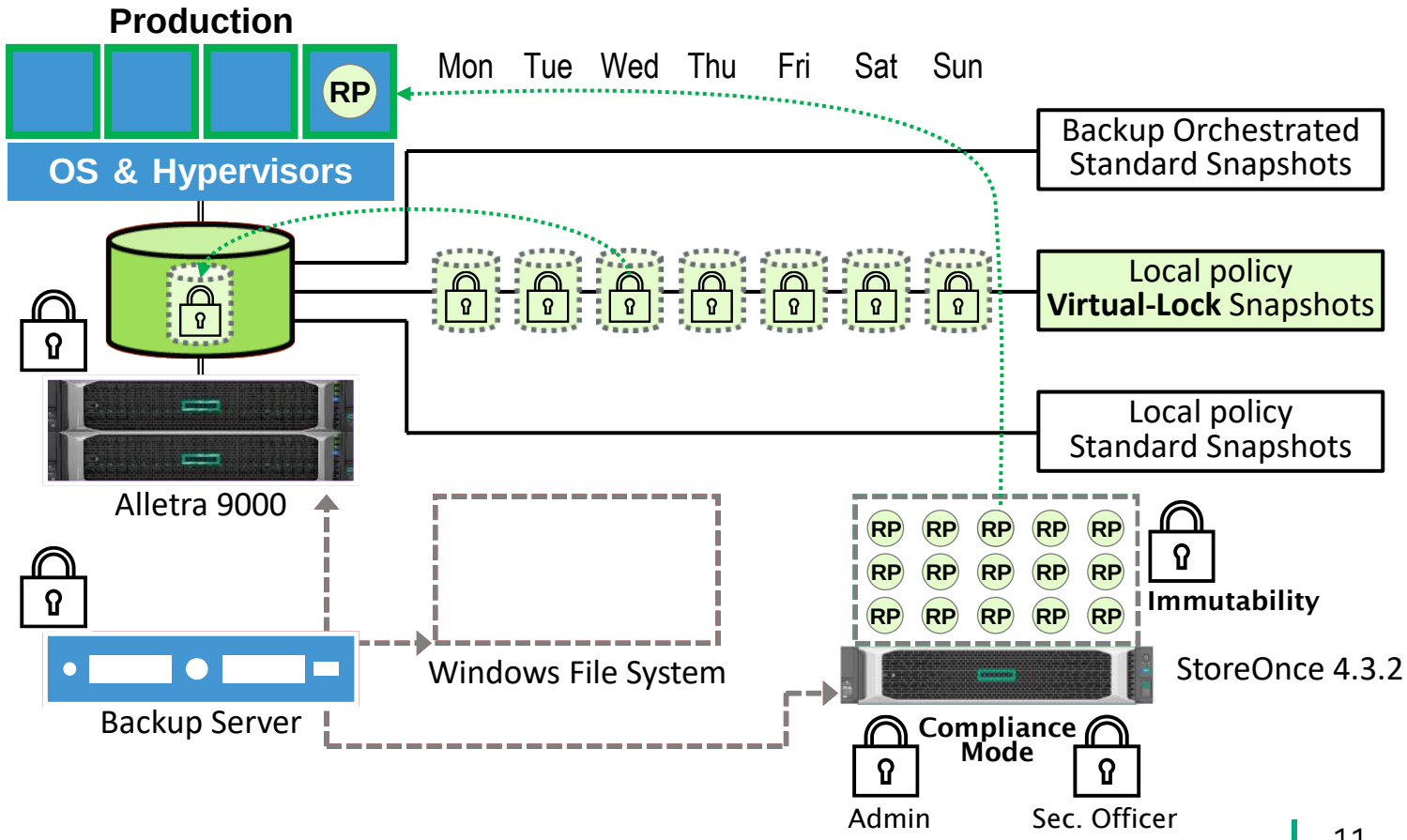
Every environment is different and complex….



Recovery process is what matters……

- Remove the malware,
- Change pwd,
- Clean the environment.

- Find a valid restore point.
- Multiple options: Snapshot and Backup.
- Test it in a clean room, and Recover.



Where to start……

Advisory approach is critical

No one vendor is the solution/ strategy

RECOVERY, PROCESS AND TIME IS WHAT COUNTS

Will AI be the answer?

Maybe.....BUT

People

Inaccurate Logical detail

AI to attack and AI to defend??

Thank you!
Question?

James Watson-Hall – Worldwide CTO Hybrid IT
May 2024