semperis

Ransomware, Risk, and Recovery: Addressing the Risk Today's Threats Pose to Your Active Directory

Sean Deuby

Director of Services, Semperis

An Unprecedented Cyber Threat

Denial-of-Availability (DoA) Malware

- **City of Torrance** (4/2020)
  - 150,000 citizens
  - **In progress – 200 GB of data stolen**
  - 150 servers / 500 workstations encrypted
  - Local backups erased
  - $680,000 ransom denied – data revealed
- **Maersk** (6/2017)
  - World’s largest shipping company
  - **55,000 devices destroyed in 7 minutes**
  - **All 1200 critical applications offline**
  - CIO slept at the office for 70 days
  - $350M

A BALANCED CITY • INDUSTRIAL • RESIDENTIAL • COMMERCIAL • TORRANCE

Mondelēz International

MAERSK LINE

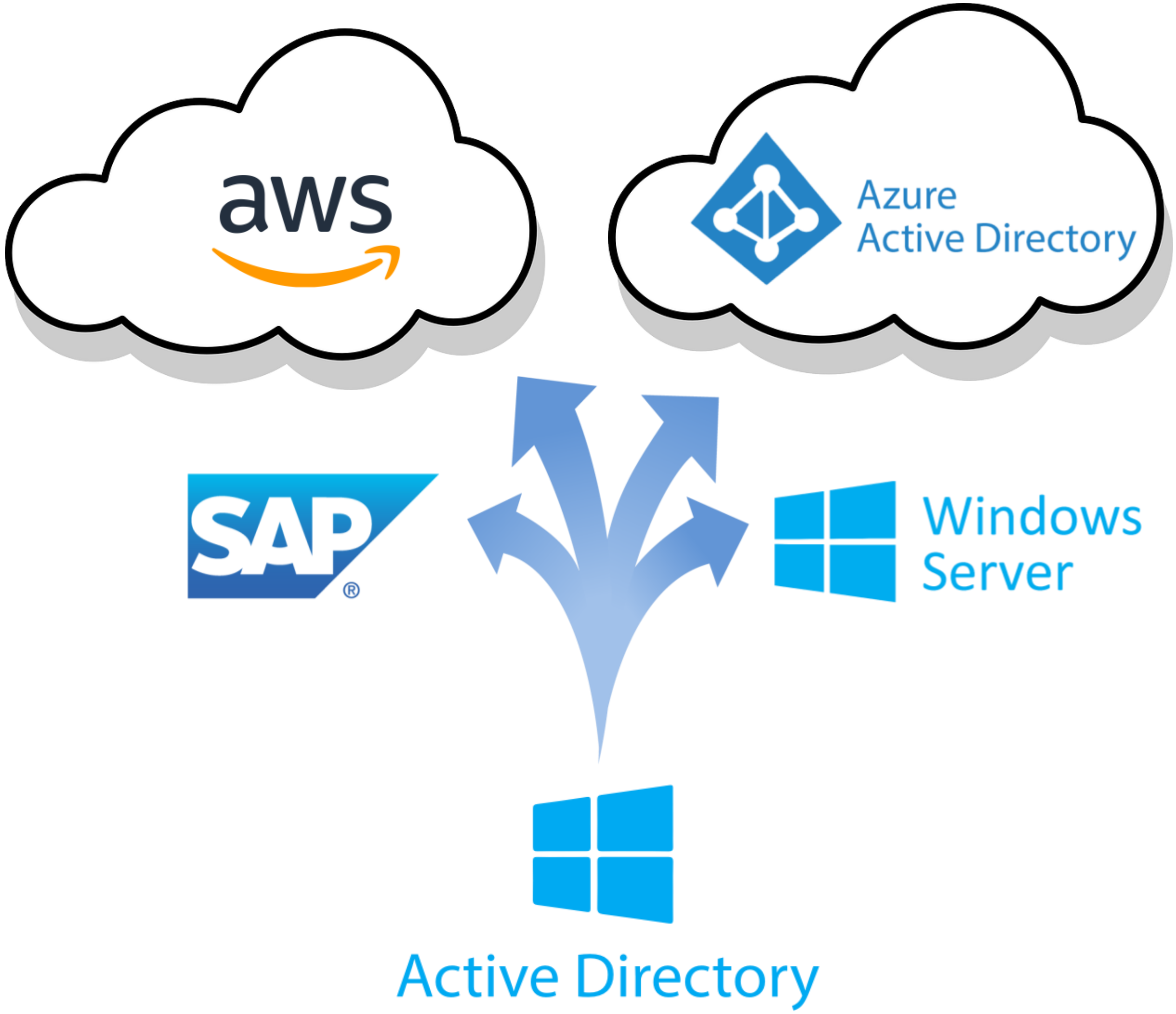
PyeongChang 2018

MERCK

Hydro

At Risk: Active Directory

- **Active Directory** remains the basis for most hybrid identity
- Highly vulnerable to DoA malware
  - Maersk: 146 of 147 domain controllers
  - Olympics: All domain controllers
- Extremely difficult to recover in disaster scenarios
  - Maersk: 9 days
- Prerequisite to restoring everything else
- **Most organizations do not have a regularly-tested AD DR plan**



Questions You'd Better Have Answers to Before the Crisis Strikes

- What are your critical applications? What DCs to they rely on?
- Have you read the Microsoft forest recovery doc? Do you have a local copy? (Remember AD is down!)
- Do you understand the procedure?
- Have you customized the procedure for your environment?
- Have you tried your procedure? Regularly?
- Have you ever tried the procedure at 2 AM with the CIO asking you questions in one ear and the crisis bridge in the other?
- Can you perform the 16 steps (many on each DC) without error because one mistake = time-consuming redo?
- Do you have a complete set of backups?
- How do you know the backups are enough foe a forest recovry?
- How do you know the backups are malware free so won't re-infect AD?
- Which DCs host DNS?
- Which DCs do you generate IFM packages on?
- Which DCs do you re-promote?
- How do you quickly send IFM packages to these target servers?
- Can you rebuild all your DCs in parallel?

What Does it Take to Perform a Forest Recovery?

1. Pull the network cables from all the DCs

For each domain,

   2. Nonauthoritative restore of first writeable DC
   3. Auth restore of SYSVOL on that DC
   4. Look for malware, etc. Forensic analysis: is it safe to continue?
   5. Reset admin account passwords
   6. Seize FSMOs
   7. Metadata cleanup of all writeable DCs except for targeted seed forest
   8. Configure DNS on the forest root DC and point child DCs to it

9. Delete DNS NS records of DCs that no longer exist
10. Delete DNS SRV records of DCs that no longer exist
11. Raise the RID pool by 100K
12. Invalidate the current RID pool
13. Reset the computer account of the root DC twice
14. Reset krbtgt twice
15. Remove the global catalog from the root DC.

    <Wait for GC to unhost>

16. Configure Windows Time

    <seed forest at this point>

17. Connect seed forest to a private network (oh yes - establish a global private VLAN)
18. Verify replication health
19. Add GC to a dc in the root domain.

    <Wait for GC to host>

20. Take a backup of all DCs in the seed forest
21. Create an IFM package for each OS version your DCs are running

For each DC to be repromoted into the seed forest,

   22. Clean up the (former) DC, either /FORCEREMOVAL or rebuild OS
   23. Send IFM package to it. <Wait>
   24. Take the DC off the public network and put it on the private network.
   25. Run a DCPROMO IFM

26. Verify health of the full forest
27. Move restored forest to the corporate network

Semperis and our Solutions

- Enterprise **identity protection** and **cyber resilience**
- **Threat mitigation** and **rapid recovery**
- Semper Paratus: Always Ready
- Combined 50 years of Microsoft identity MVP experience

Semperis AD Forest Recovery™

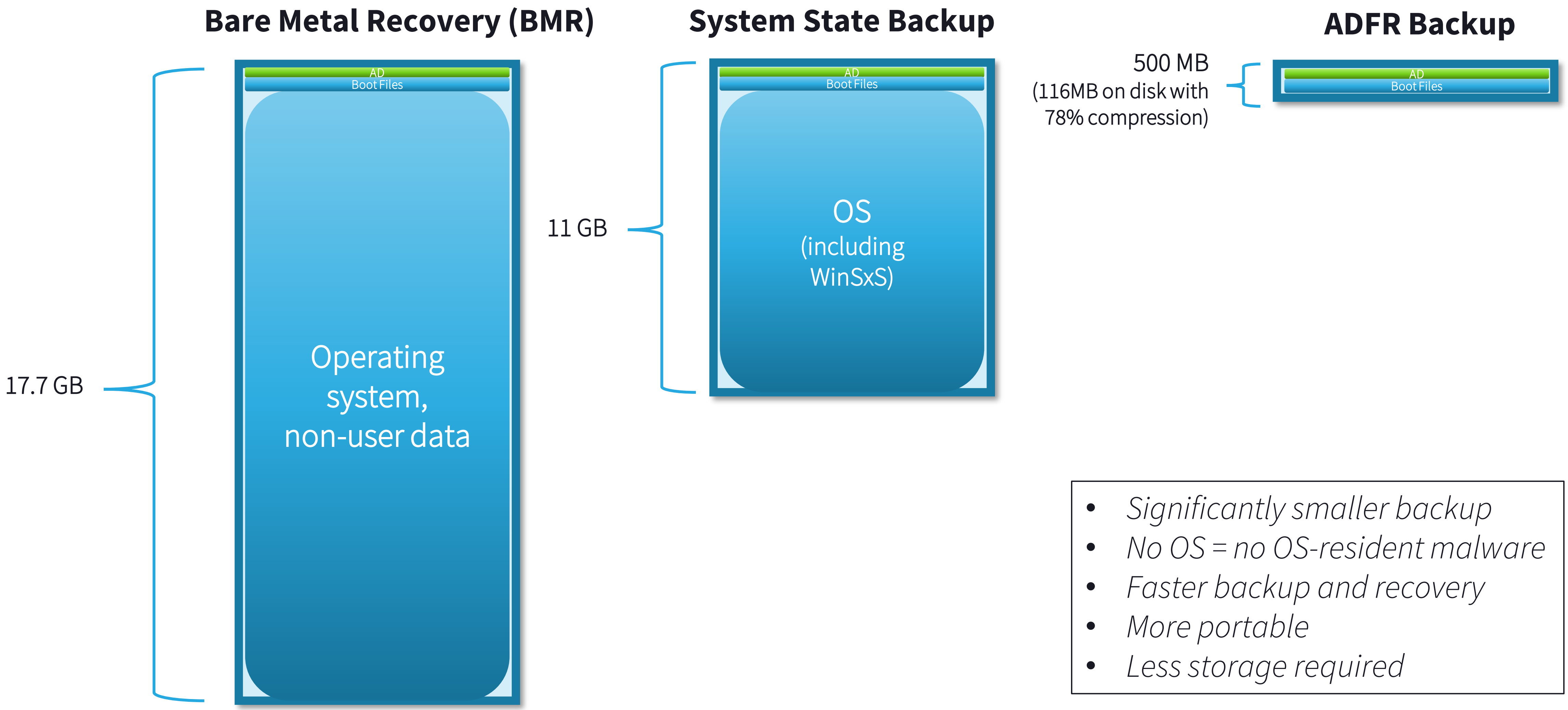
Fully automated disaster recovery orchestration for Active Directory

Semperis DS Protector™

Real-time AD object and attribute

- Tracking
- Auditing
- Roll back
- Security analyzer

Relative Backup Size



Bare Metal Recovery (BMR)

17.7 GB

AD

Boot Files

Operating system, non-user data

System State Backup

11 GB

AD

Boot Files

OS (including WinSxS)

ADFR Backup

500 MB (116MB on disk with 78% compression)

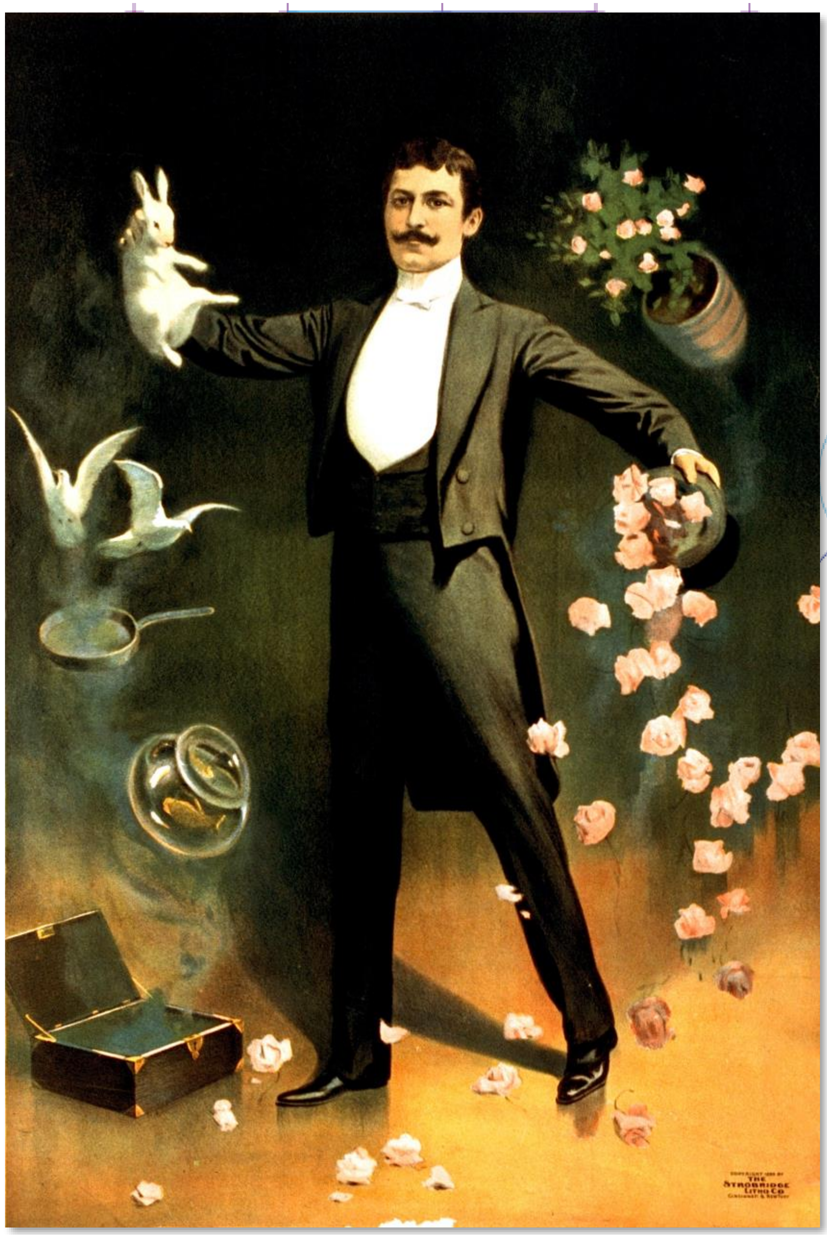
AD

Boot Files

- *Significantly smaller backup*
- *No OS = no OS-resident malware*
- *Faster backup and recovery*
- *More portable*
- *Less storage required*

SEMPERIS

Demo



semperis

2020 Honors

INFOSEC
AWARDS
WINNER
CYBER DEFENSE MAGAZINE
2020

SC 2020 awards
Winner

CYBER
SECURITY
EXCELLENCE
AWARDS
★ WINNER ★
2020

Info Security
Products Guide
2020
GLOBAL
EXCELLENCE
GOLD
★★★★★

EDISON AWARDS
E
GOLD
2020 WINNER

Cutting Edge Ransomware Recovery Solution

Publishers Choice: Cybersecurity Conference Series

Best Business Continuity and Disaster Recovery Solution

Best Business Continuity and Disaster Recovery Solution

Best Cybersecurity Conference

Business Continuity and Disaster Recovery Solution

Data Center Backup and Recovery Solution

Gold Winner: Information Technology— Data Management Category

semperis

Next Steps

1. **Review your BC/DR plans from a cyber resiliency viewpoint**

2. **Evaluate your worst-case Active Directory cyber disaster preparedness**
   - Full forest recovery
   - Risk of malware reinfection
   - Flexibility of recovery scenarios (i.e. recovery to cloud IaaS)

semperis

"…the most important lesson learned was that **organizations must direct more IT resources into system recovery, especially offline backup capabilities.** 'Trust me, it is the best thing to invest in,' Powell said, 'because high-level nation-state cyberweapons will take out everything you have online.'"

"Every company should aspire to **have Active Directory up and running within 24 hours**. 9 days is too long."

Andy Powell, Maersk CISO

semperis

Thank you

Contact info:

☎ +1 703-918-4884

✉ info@semperis.com
SeanD@Semperis.com
SteveM@Semperis.com
JessicaS@Semperis.com

semperis.com/contact