semperis

Ransomware, Risk, and Recovery:
Is Your Disaster Recovery Strategy Ready for Today's Threats?

Sean Deuby

Director of Services, Semperis

Presenters

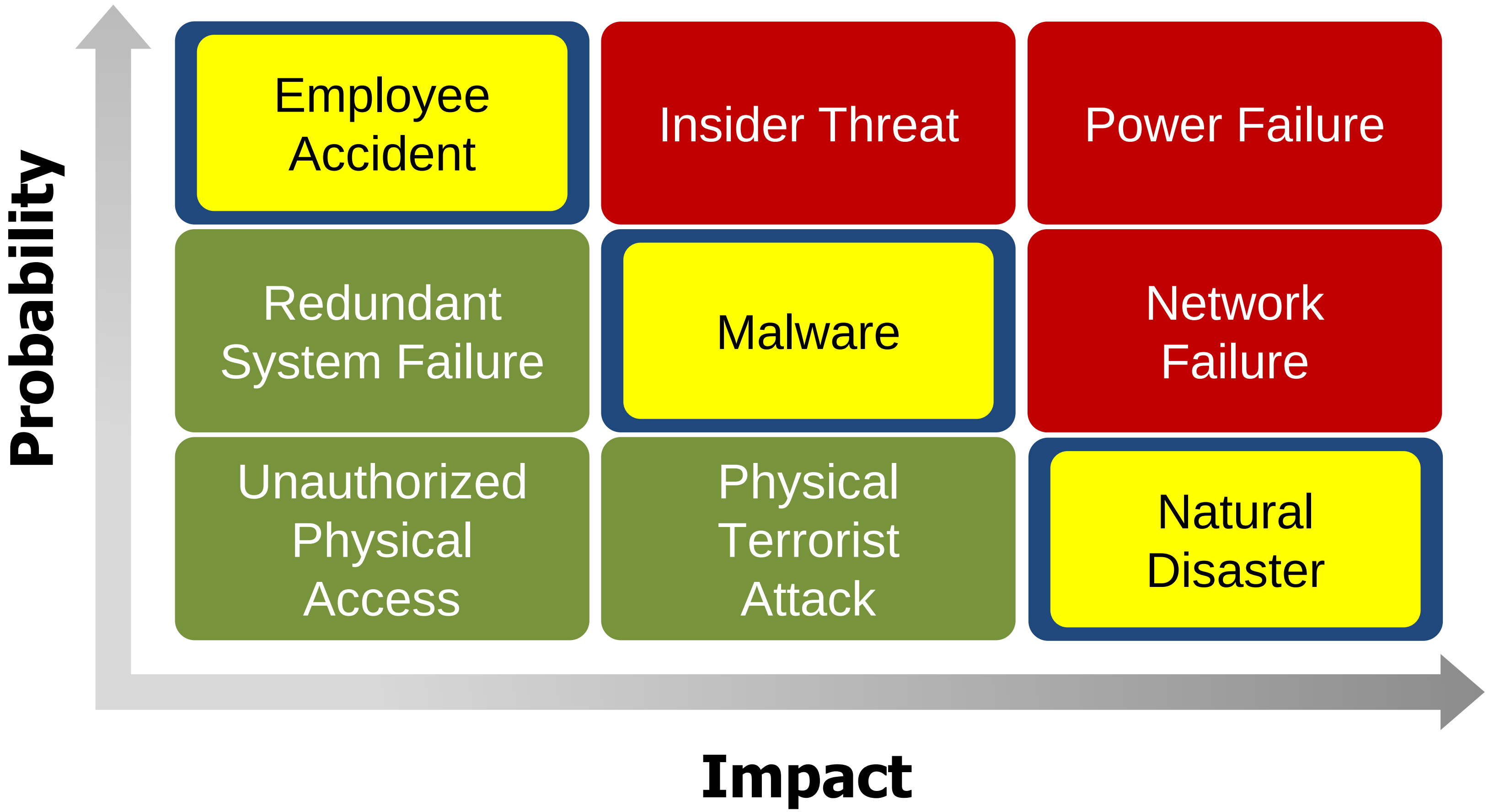
Sean Deuby

Director of Services, Semperis

seand@Semperis.com

Sean Deuby brings 30 years’ experience in enterprise IT and hybrid identity to his role as Director of Services at Semperis. An original architect and technical leader of Intel's Active Directory, Texas Instrument’s NT network, and 15-time MVP alumnus, Sean has been involved with Microsoft identity since its inception. Since then, his experience as an identity strategy consultant for many Fortune 500 companies gives him a broad perspective on the challenges of today's identity-centered security. Sean is an industry journalism veteran; as former technical director for Windows IT Pro, he has over 400 published articles on AD, hybrid identity, and Windows Server.

Classic Disaster Recovery Risk Matrix



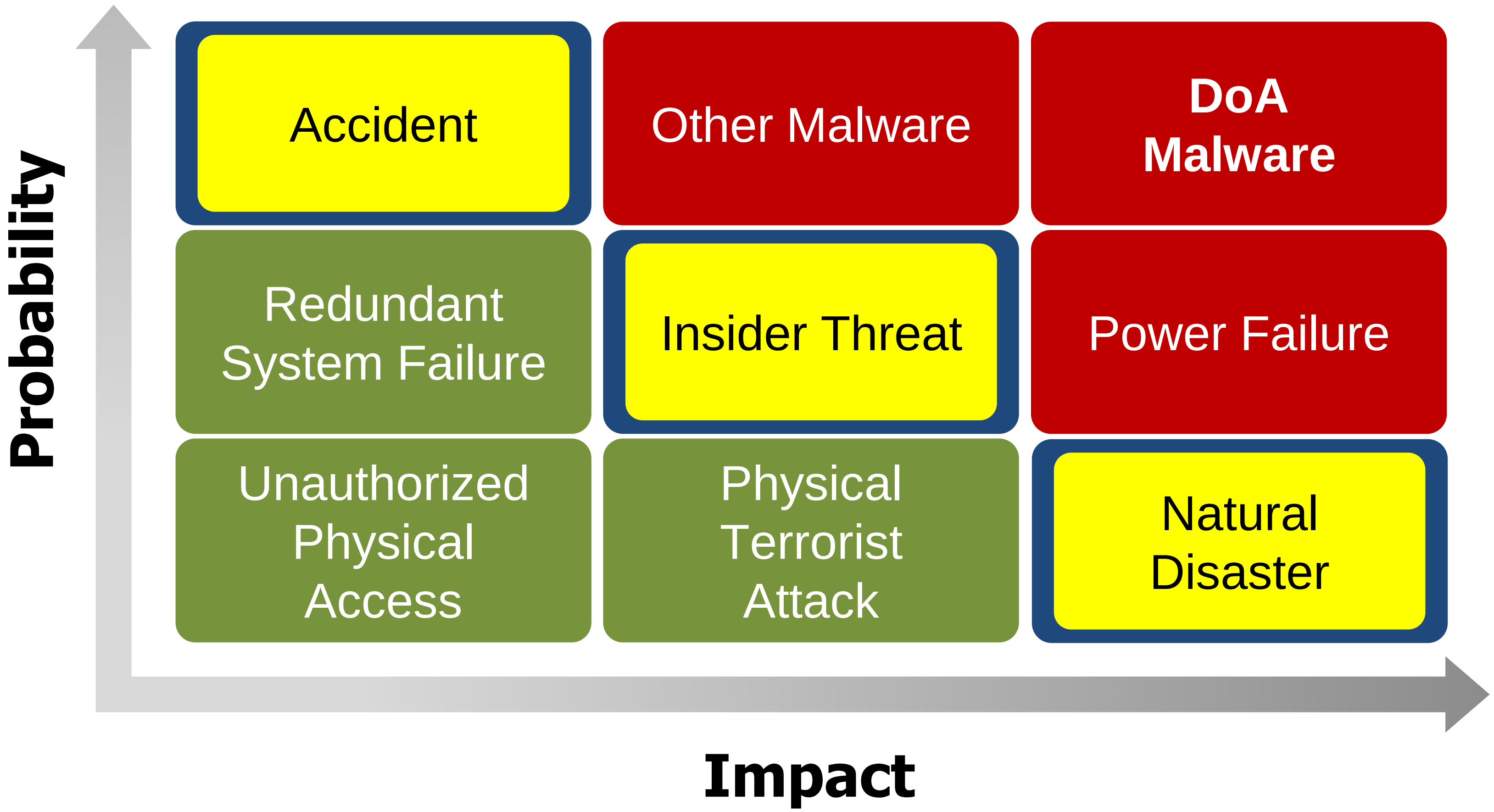
Probability	Employee Accident	Insider Threat	Power Failure
	Redundant System Failure	Malware	Network Failure
	Unauthorized Physical Access	Physical Terrorist Attack	Natural Disaster
		Impact	

An Unprecedented Cyber Threat

Denial-of-Availability (DoA) Malware

- **University of California SF** (June 1)
  - NetWalker ransomware
  - In progress
  - Data stolen, published piecemeal
- **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

Cyber-First Disaster Recovery Risk Matrix



Probability

Accident	Other Malware	**DoA Malware**
Redundant System Failure	Insider Threat	Power Failure
Unauthorized Physical Access	Physical Terrorist Attack	Natural Disaster

Impact

Organizations Are in Denial

- **2020**
  - **Hospital attacks are increasing** (Interpol)[3]
  - **148% in March alone**[4]
- **79% of organizations have experienced an identity-related security breach in the last two years**[1]
- **77% of organizations "confident"** or "very confident" about recovering from an attack[5]
- **But only 21% have contingency plans**
- **And only 11% believe they can recover in 3 days**

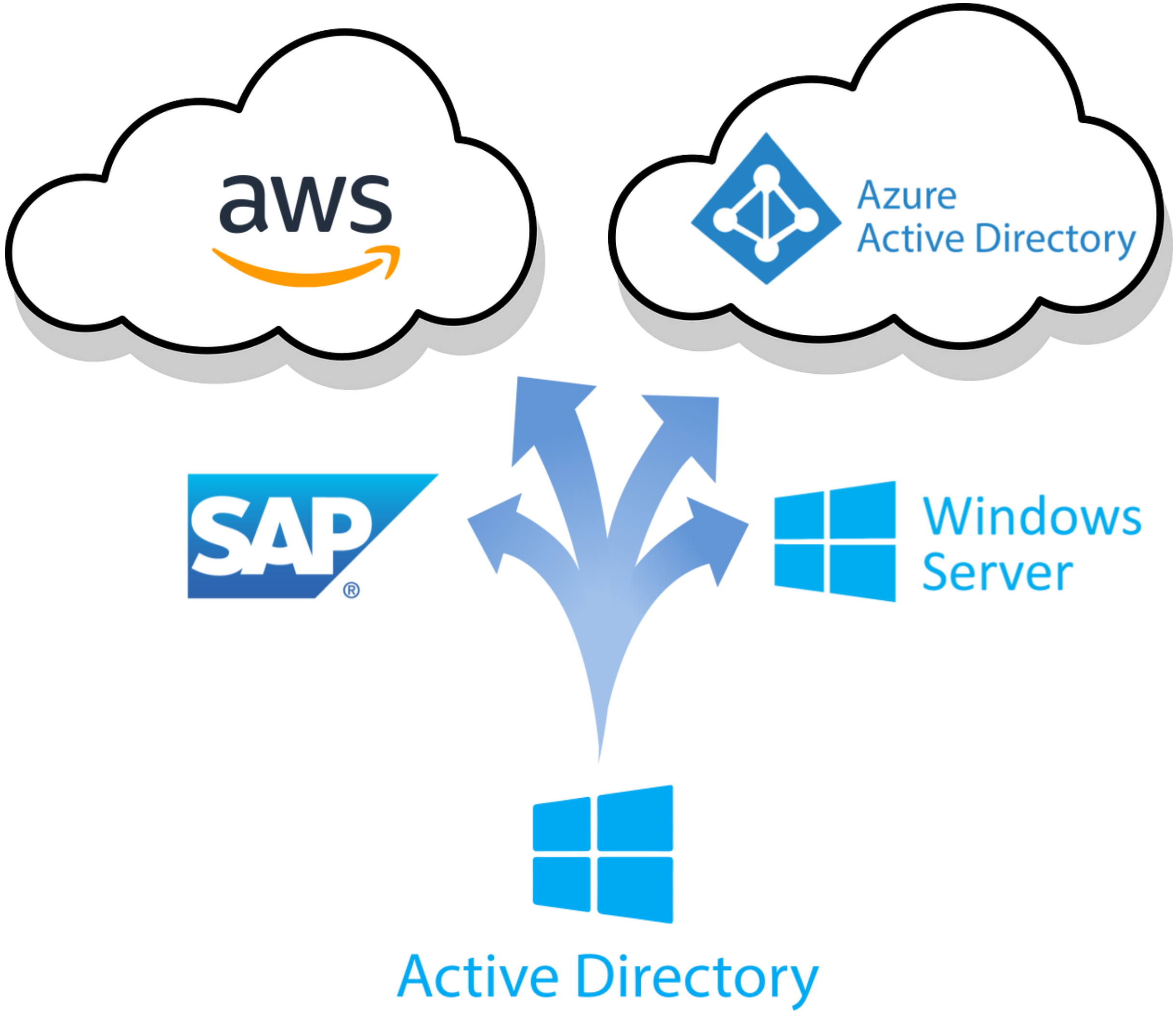
How will you recover from having all your devices encrypted in minutes?

Cyber Insurance Is No Substitute for Preparedness

- Does the attack match your coverage?
  - Acts of war (e.g. NotPetya) aren’t covered
  - What if the attackers release data?
- Does the ransom match your policy limits?
- Recovery on hold
  - Until ransom matches insurance payout
  - Until paperwork processing is complete
- Half of ransomware victims suffer repeat attacks[1]
  - Honda hit three times (spearphished) in last 12 months[2]
- How does it look to your customers (and competitors)?
- Is it right?

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

semperis

- 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?

semperis

1. Pull the network cables from all DCs or otherwise disable

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 all admin account passwords
6. Seize FSMOs
7. Metadata cleanup of all writeable DCs except for targeted seed forest DCs
8. Configure DNS on the forest root DC

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 account 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
22. Build out seed forest with additional DCs to support Tier 0 / Tier 1 operations:

For each DC to be repromoted into the seed forest,

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

<Days pass…>
<Large enough forest to support basic operations>

27. Verify health of the full forest
28. 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

Active Directory Forest Recovery (ADFR)

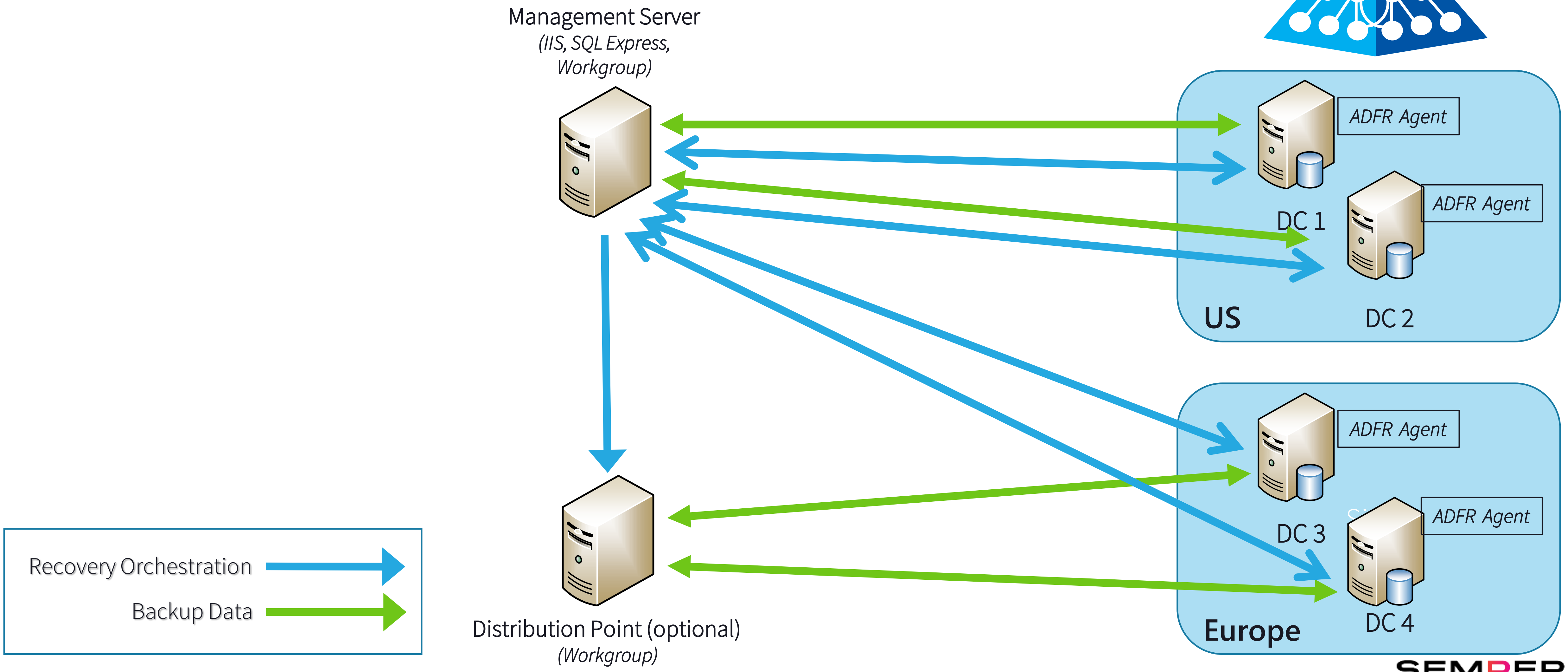
semperis

- **Fully automated Active Directory disaster recovery solution** for:
  - Single DC restore
  - Partition restore (domain, configuration, DNS, application)
  - Full forest recovery

- Restore hundreds of DCs in the time it takes to manually restore a single DC
  - Shortening the recovery time of the entire AD forest **by 90%**

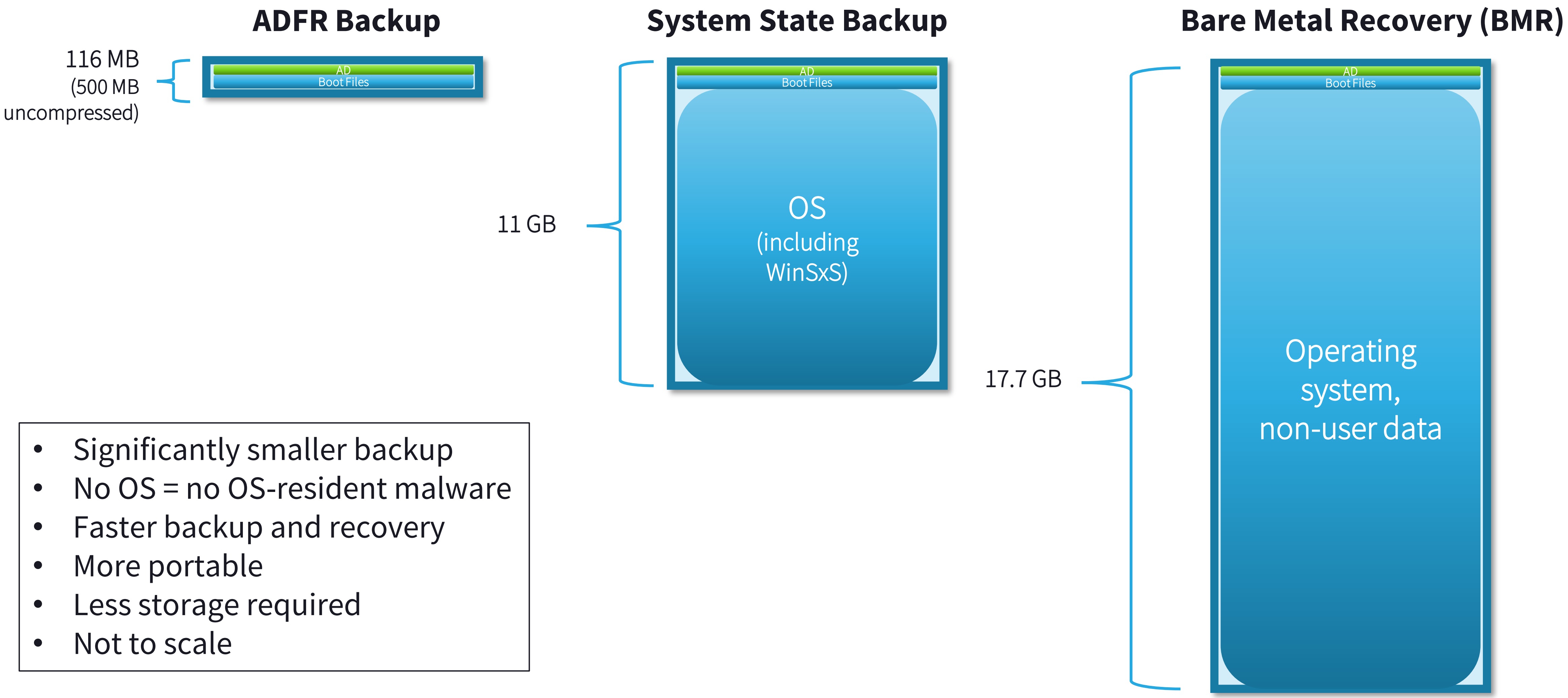
- Specifically architected to support cyber resiliency
  - **"Shared Nothing" architecture:** does not depend on AD to perform a recovery
  - **Anywhere Restore:** recover to any hardware, to any IP, without dependency on source hardware
  - **Clean Restore:** AD backup is de-coupled from OS backup
    - OS isn't backed up (unlike system state or BMR backups)
    - Ensures that malware won't be re-introduced during AD restoration

AD Forest Recovery



SEMPERIS

Relative Backup Size



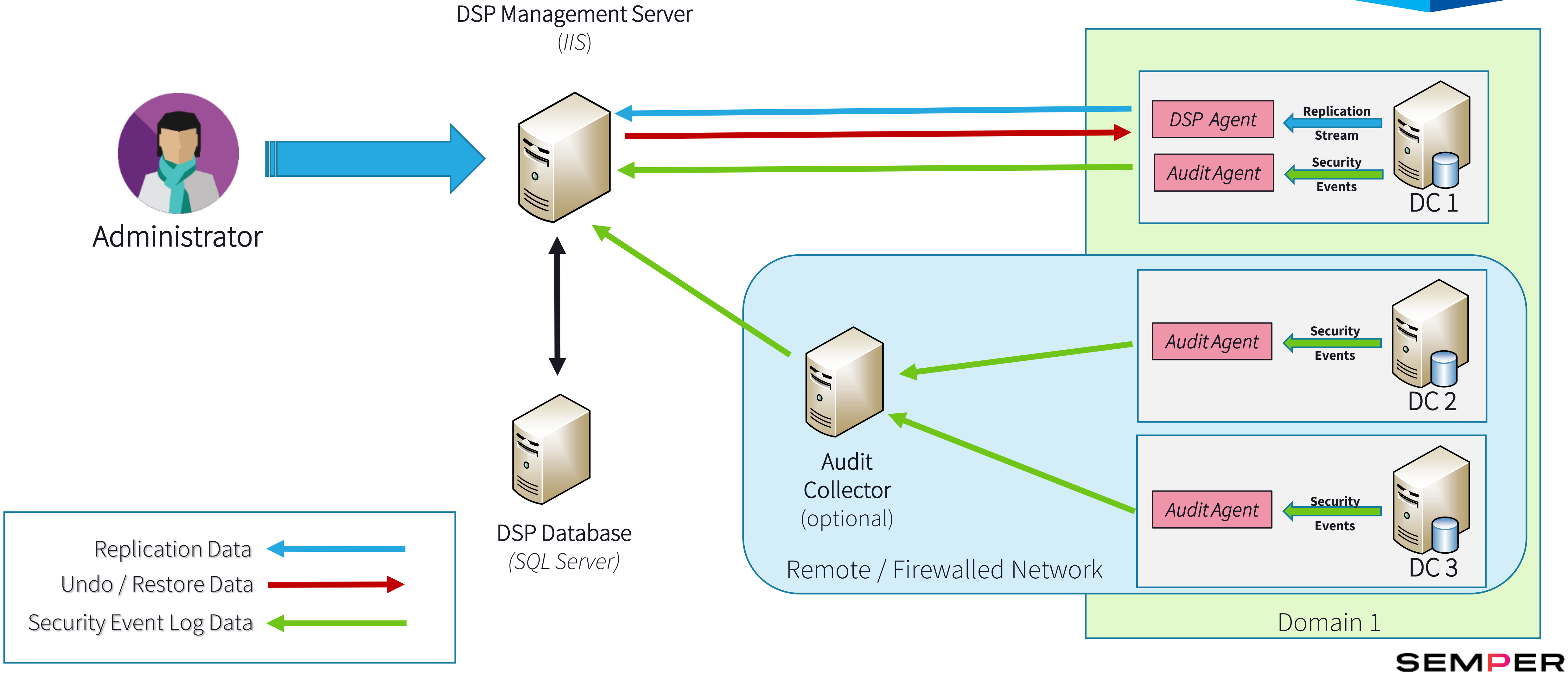
- Significantly smaller backup
- No OS = no OS-resident malware
- Faster backup and recovery
- More portable
- Less storage required
- Not to scale

Semperis DS Protector

semperis

- **What Changes Were Made**
  - **Capture all changes** by monitoring AD replication stream (patented)
- **Who Made the Changes**
  - **See who made each change** – or quickly find all changes made by a particular user
- **Instant Recovery**
  - **Roll back unwanted changes immediately** - without mounting or restoring a backup
- **Tamperproof Tracking**
  - **Capture all changes** - even if agents are disabled or security logs are erased
- **Granular Restore**
  - **Restore individual attributes, objects, and containers** to any point in time - not just to a previous backup
- **Role-Based Access Control (RBAC)**
  - Grant permission to view or undo changes to specific attributes, object types, OUs, etc.
- **PowerShell Module**
  - Easily integrate into existing IT applications

DSP architecture



SEMPERIS

semperis

2020 Honors

INFOSEC AWARDS WINNER
CYBER DEFENSE MAGAZINE
2020

Cutting Edge Ransomware Recovery Solution

Publishers Choice: Cybersecurity Conference Series

SC 2020 awards Winner

Best Business Continuity and Disaster Recovery Solution

CYBER SECURITY EXCELLENCE AWARDS
★ WINNER ★
2020

Best Business Continuity and Disaster Recovery Solution

Best Cybersecurity Conference

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

Business Continuity and Disaster Recovery Solution

Data Center Backup and Recovery Solution

EDISON AWARDS
GOLD
2020 WINNER

Gold Winner: Information Technology— Data Management Category

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

Thank you

Contact info:

☎ +1 703-918-4884

✉ info@semperis.com
SeanD@Semperis.com
GaryL@Semperis.com

semperis.com/contact