



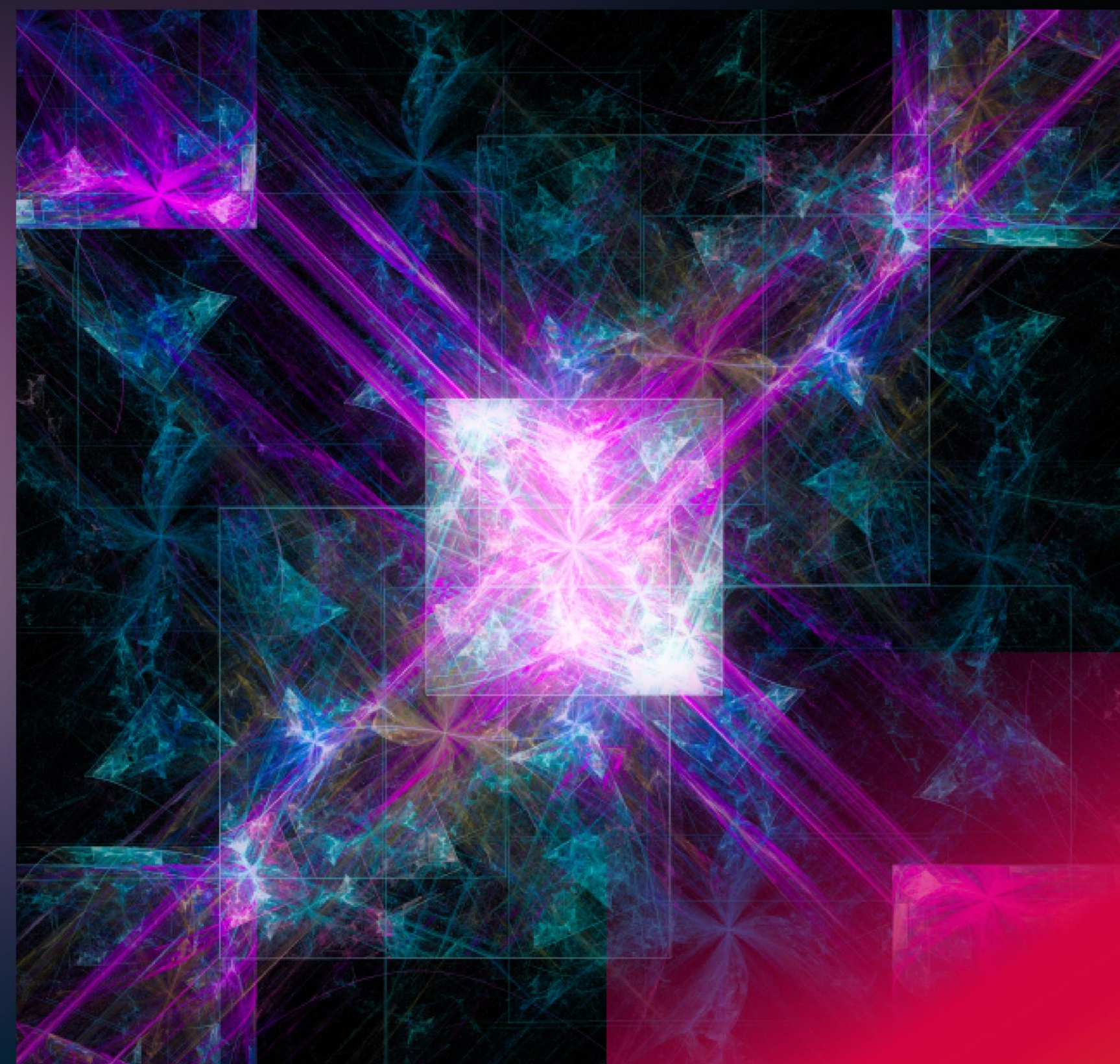
Incident Response and Resilience



Alexandra Weaver


Senior Solutions Architect, *Semperis*

alexandraw@semperis.com



Microsoft Partner

Enterprise Cloud Alliance
Microsoft Accelerator Alumni
Microsoft Co-Sell
Microsoft Intelligence Security Association (MISA)

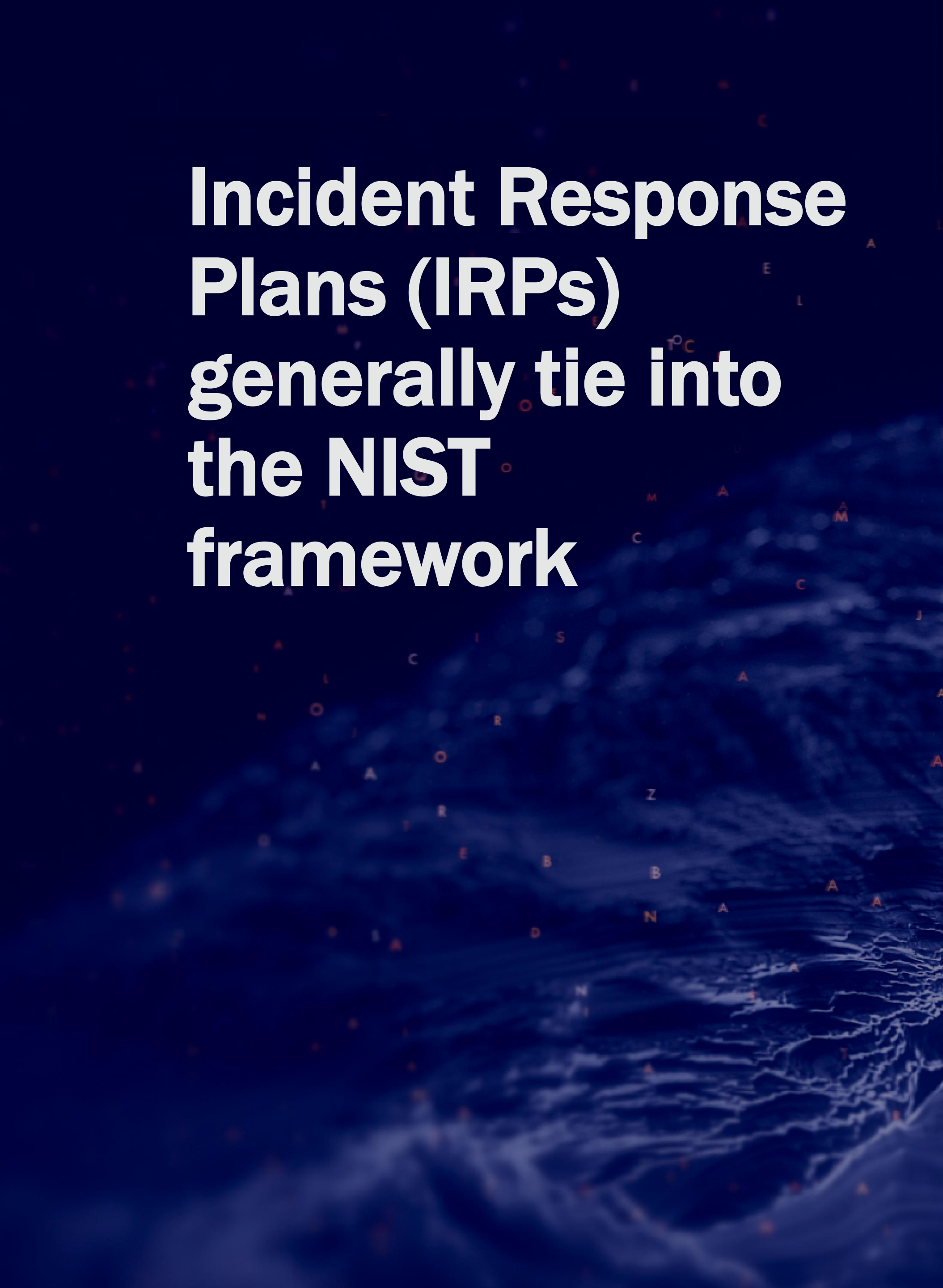


**The best defense
against a
cyberattack is a
well-prepared
incident response
plan**

Incident Response Plans (IRP) are an approach that organizations use to:

- Identify
- Contain
- Eliminate
- Recover from cybersecurity incidents

The **goal** of IR is to minimize damage, reduce recovery time and costs, and prevent future incidents.



Incident Response Plans (IRPs) generally tie into the NIST framework

Six phases of an IRP:

1. Preparation
2. Detection & Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons learned and post incident review

Social Engineering Tactics:



- Phishing
- Vishing
- BEC Business Email Compromise
- Pretexting
- Honeytrap
- Tailgating
- Deep fakes
- Whaling
- Baiting
- Smishing.....

Steps to improve your cyber resilience today

- Map out your most critical assets and understand the business processes that are essential to your **Minimum Viable Company**
- Determine the necessary infrastructure to run those essential processes and services
- IDENTITY is at the center—for 90% of global organizations, **Active Directory is the primary identity system**

Without an AD-specific backup solution, organizations “will have no choice but to pay the ransom.”

Gartner

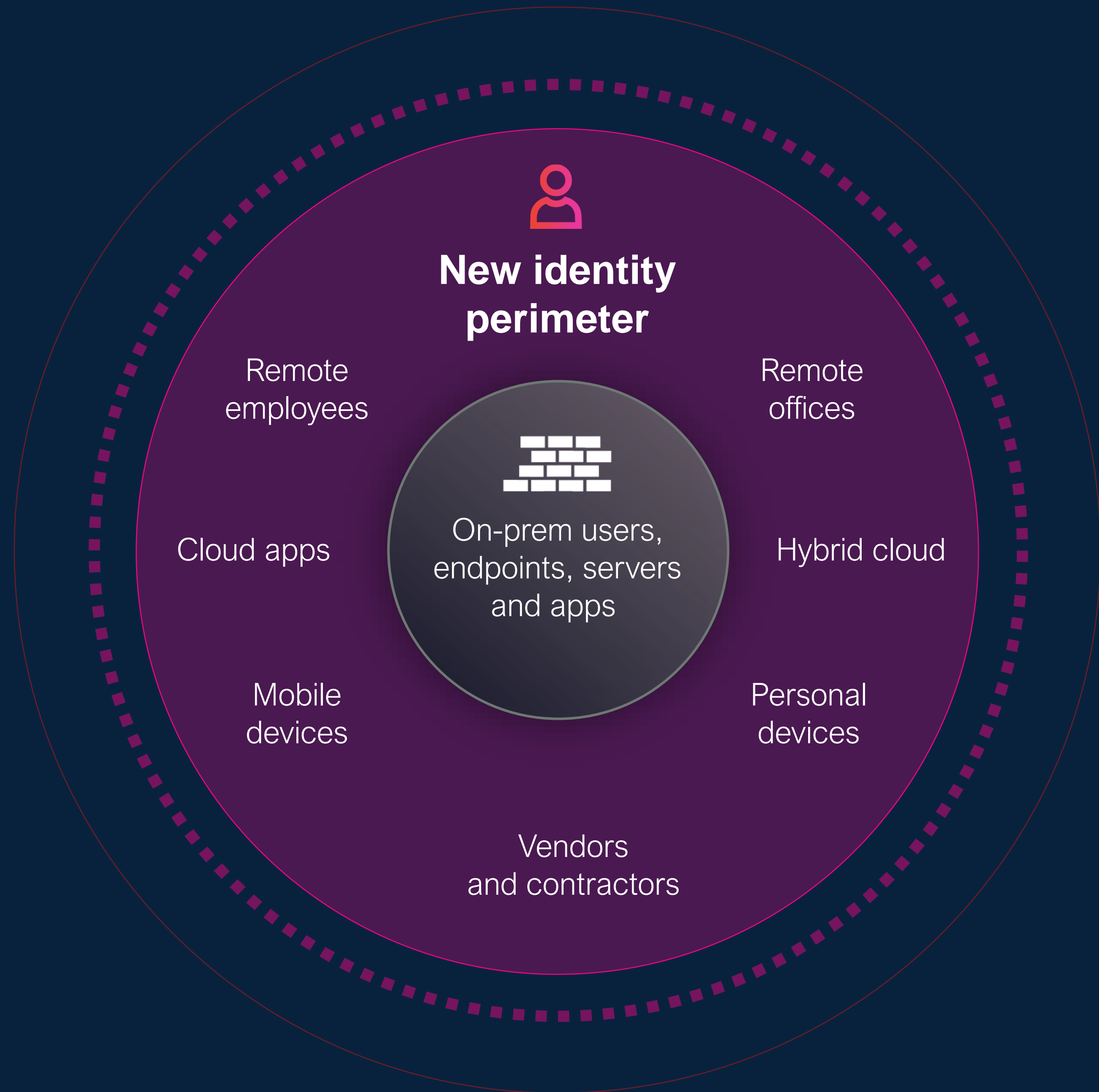
RESILIENCY CHALLENGES

Identity has become fundamental

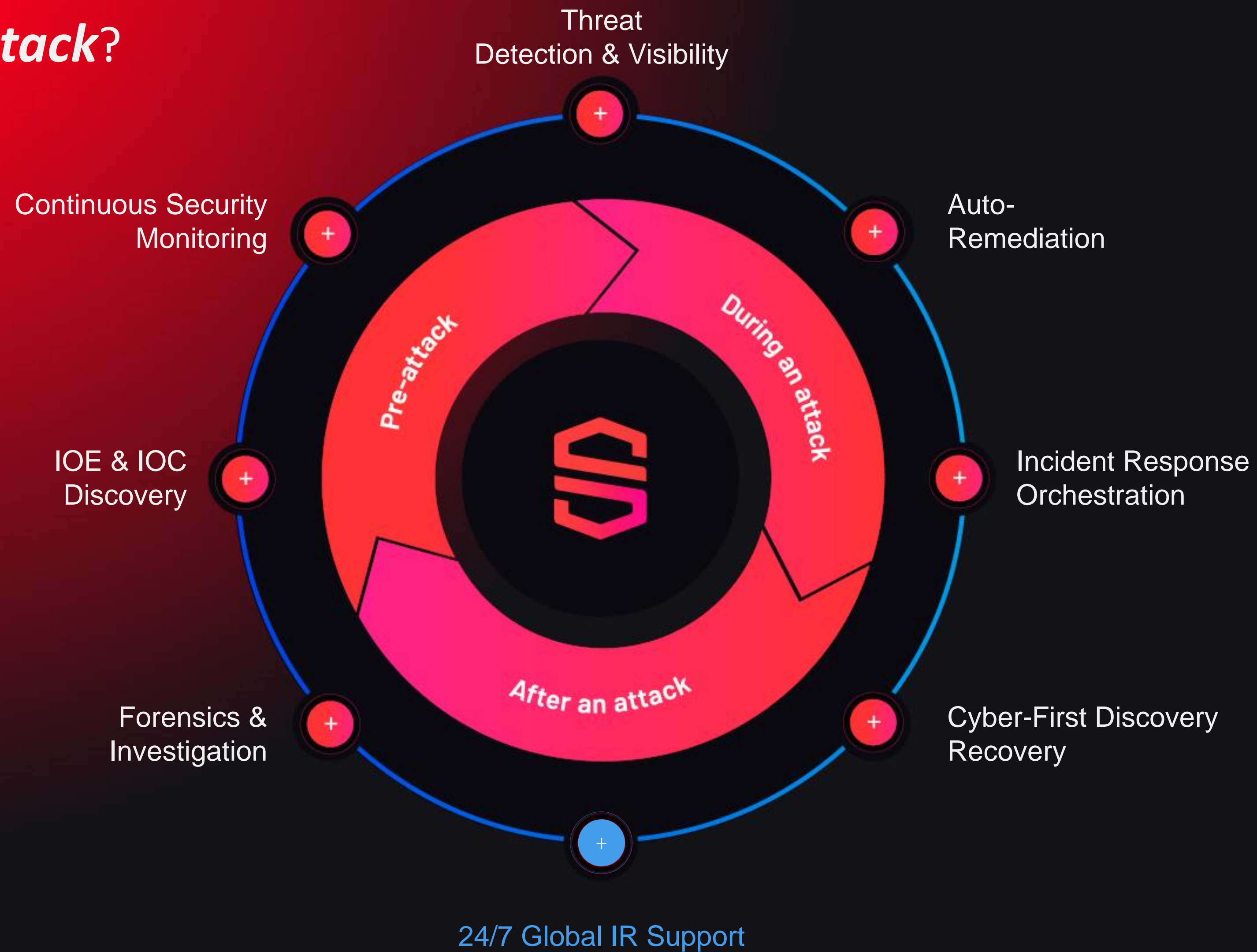
1 Keeps legacy environments secure

2 Enables digital transformation

3 Is a building block of Zero Trust



What is in place to detect ***before***,
recording ***during***, and provide IOC
after a cyber security ***attack***?



Common Cyber Attacks

- Malware
- Phishing
- Zero Day Exploits
- Ransomware
- Password Attacks
- DoS & DDoS
- DNS spoofing

- 
- Trojan Horse Attacks
 - SQL Injection Attacks
 - Cross Site Scripting
 - Insider Threat
 - Root kits

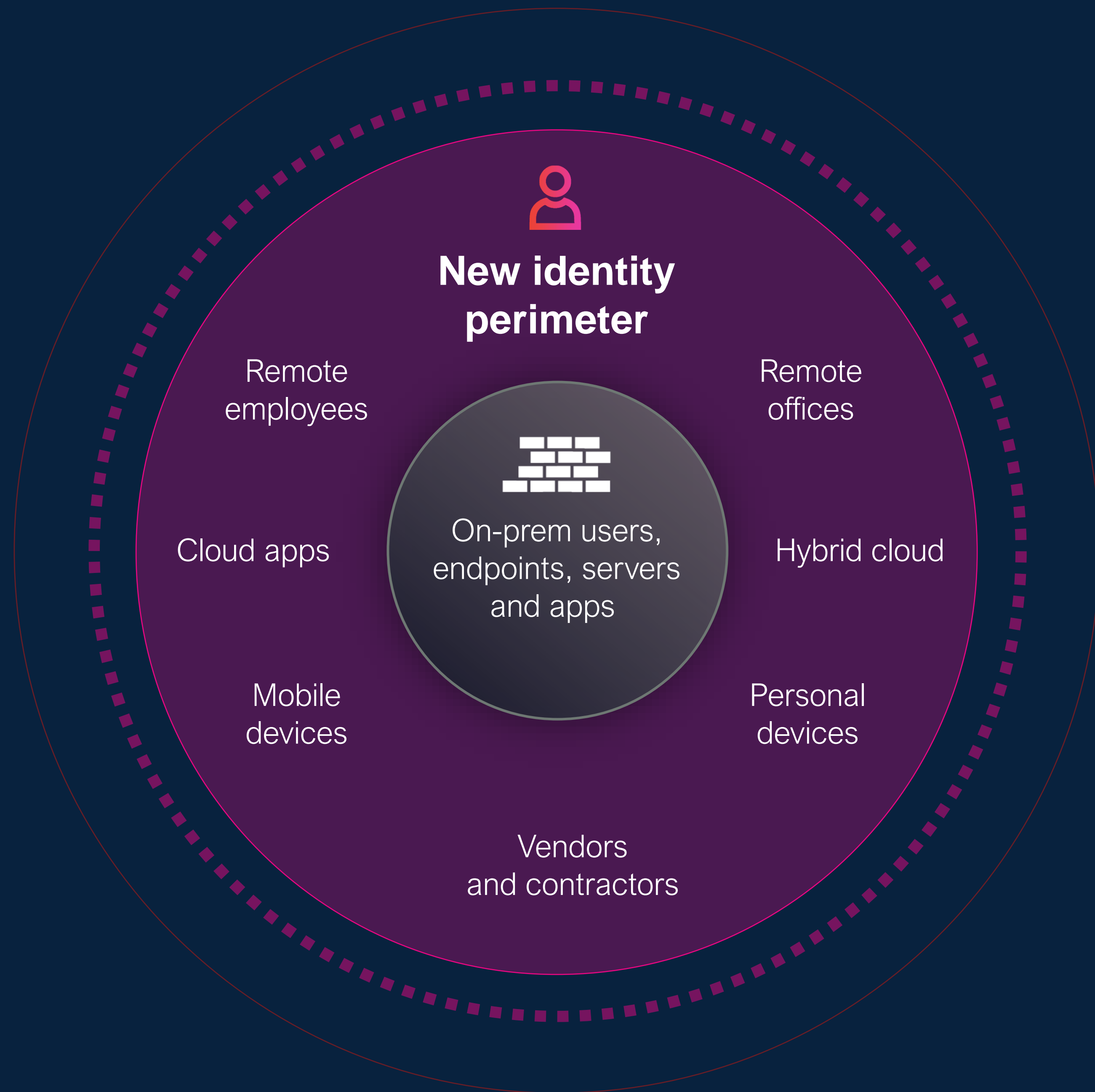
— **AGAIN.... Identity is the key!!!**

Identity has become fundamental

1 Keeps legacy environments secure

2 Enables digital transformation

3 Is a building block of Zero Trust

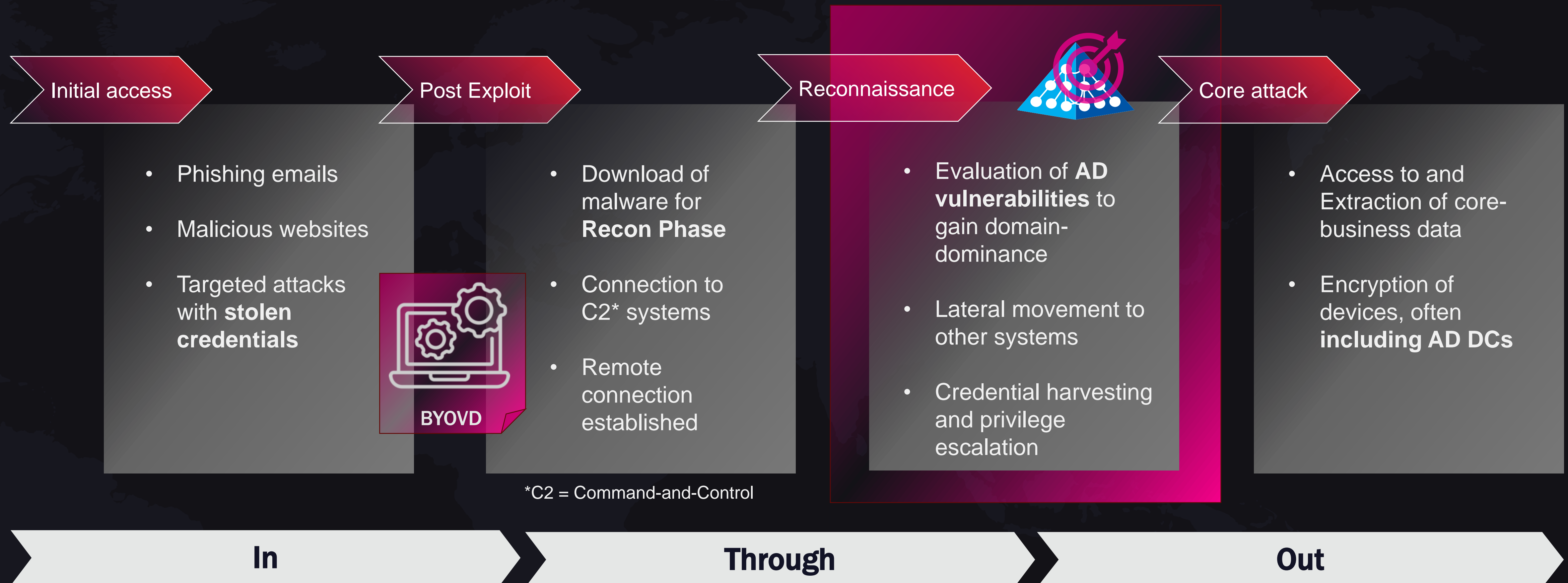


Cyberattacks start with identity compromise

- “Attackers are targeting Active Directory and the identity infrastructure with phenomenal success.” – *Gartner*
- More often than not, attacks like ransomware are the second stage, predicated by an identity compromise. In fact, if you read all the attention-grabbing headlines, you’ll find that most novel techniques rely on compromising identity first.” – *Microsoft*
- “Attackers don’t break in...they log in”



Phases of a ransomware attack

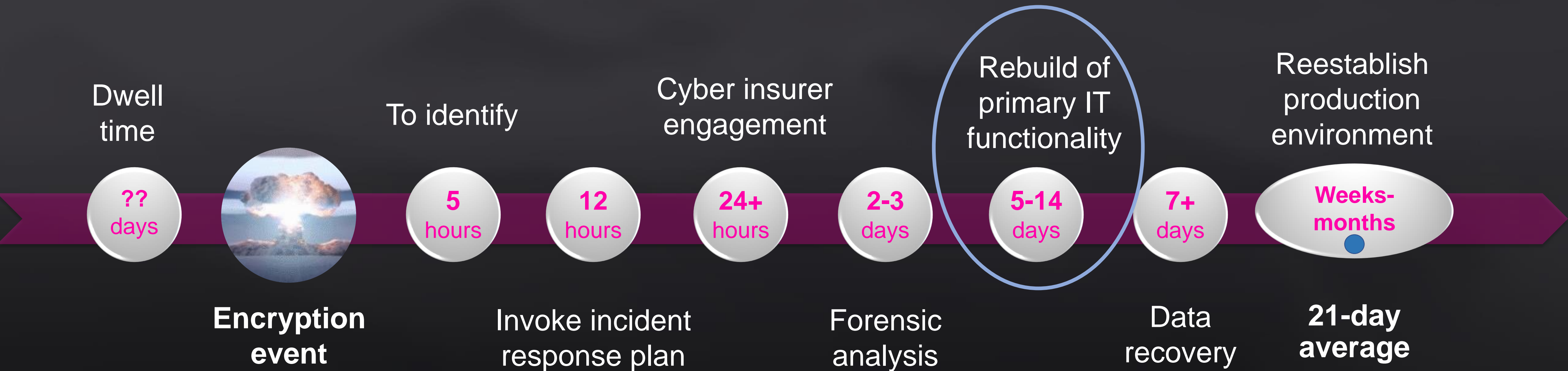




YOUR FILES ARE ENCRYPTED
Your photos, documents and other important
files have been encrypted with unique key,
generated for this computer.

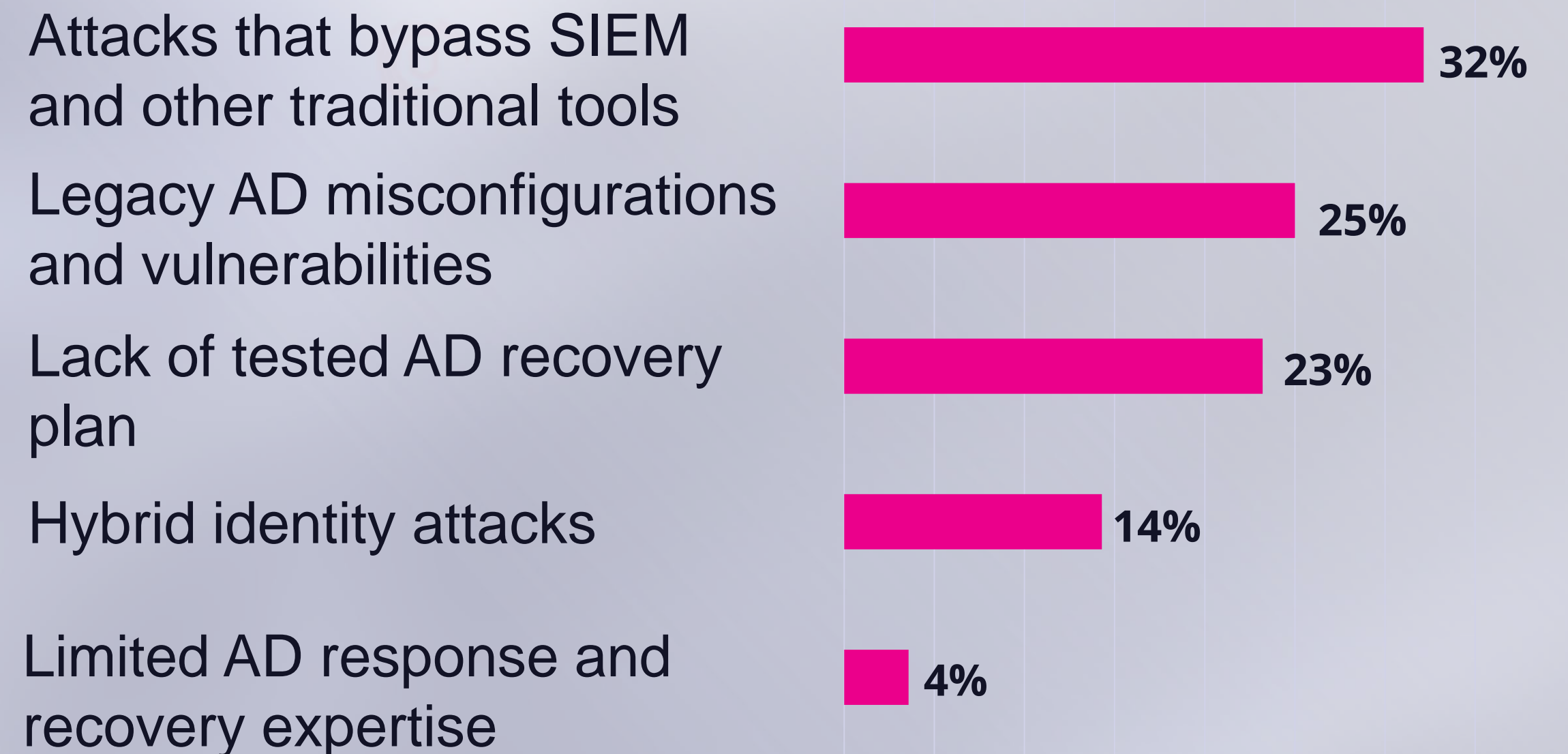
NEXT

Cyberattack recovery timeline



Cyberattacks 101: How to take down Active Directory

Biggest concerns regarding identity threats



SURVEY RESULTS Evaluating Identity Threat Detection & Response (ITDR) Solutions

TODAY'S RISKS

Protecting the digital enterprise

In today's cloud-first, mobile-first world, dependency on identity systems is rapidly growing—**so is the attack surface.**



Cloud applications



Bring your own devices



Scattered hybrid identities



Anywhere, anytime access



Ransomware attacks



Cyber espionage

DO Basics to strengthen your environment:

- ✓ Require strong passwords
- ✓ MFA
- ✓ JIT
- ✓ JEA
- ✓ PAWS
- ✓ VPN when using public Wi-Fi
- ✓ Patch
- ✓ Top-down security initiative

DO Back up Active Directory and prepare for recovery

- ✓ Backup every domain, *especially* the root
- ✓ Backup two+ DCs per domain
- ✓ Test your backups regularly
- ✓ Test downstream applications
- ✓ Use supported backup methods
- ✓ Ensure backups are malware free
- ✓ Don't forget to keep offline copies of backups

Prepare for an Active Directory recovery!

- Know your AD topology and know disaster recovery passwords.
- Know DNS topology and passwords. Name resolutions will fail as long as AD is down.
- Reduce the number of OS versions on your DCs.
- Take a backup of at least two DCs per domain in your forest & **not** backup the OS.
- Know the Microsoft AD Forest Recovery guide. Ideally, you have fully automated all the recovery steps.
- Be prepared for a lot of post restore manual tasks.

Top 10 things to do to improve security

- Implement good identity processes
- Implement trust security
- Secure Kerberos
- Deter lateral movement
- Secure privileged users and groups
- Harden privileged access
- Secure dependencies
- Harden domain controllers
- Monitor for unusual activity
- Back up AD—and be ready to recover

Free AD vulnerability scanning tools

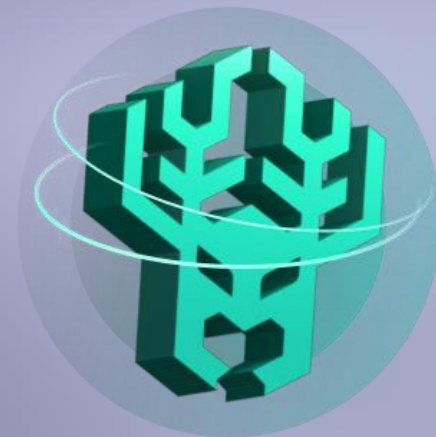
Scan your AD to find out how intruders could use any gaps to their advantage.

FREE → www.semperis.com/purple-knight/
www.semperis.com/forest-druid/



Purple Knight powered by Semperis

- Powerful UI-tool for evaluating security posture of a complete AD forest
- Continuously updated with new indicators of exposure (IOEs) and indicators of compromise (IOCs)



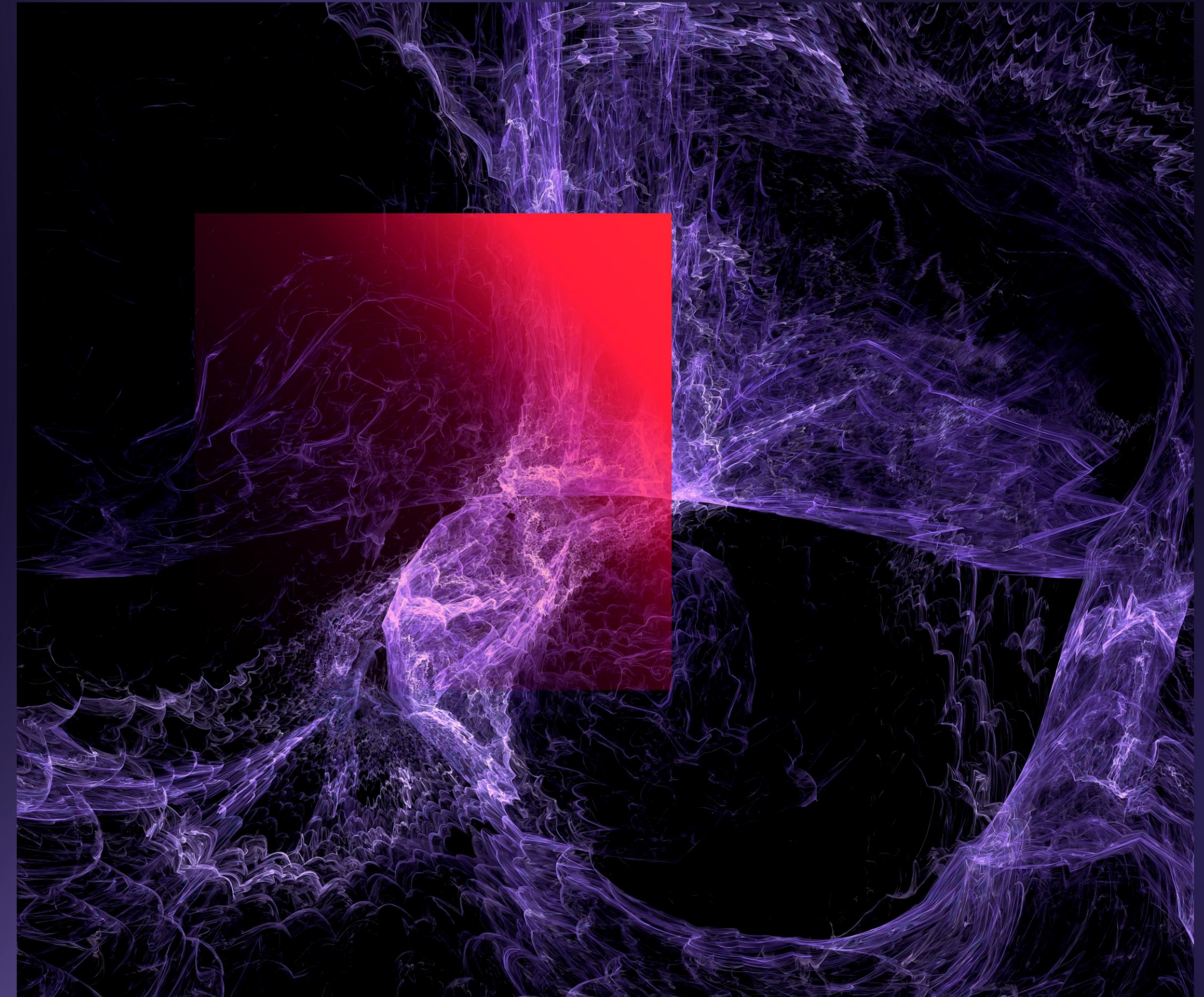
Forest Druid powered by Semperis

- Powerful UI tool for visualization of attack paths
- Easy to use—no setup required
- Built to help AD defenders

Key takeaways

- Active Directory: Your Achilles heel?
- Hybrid attacks: Double the identity, double the attack surface
- Job #1: Lock down AD security
- Scan continuously
- Prepare for malware-free AD recovery!

→ Check out Semperis [Purple Knight](#) and [Forest Druid](#) to get started.





THANK YOU

Questions?

KKR

INSIGHT
PARTNERS



TOP 5 FASTEST-GROWING
CYBERSECURITY COMPANIES

500TM

Technology **Fast 500**
2023 NORTH AMERICA

Deloitte.

3 YEARS IN A ROW OF
DOUBLE-DIGIT GROWTH



NAMED TO FORTUNE'S CYBER 60
2024 LIST

**Inc. Best
Workplaces**

2023

2 CONSECUTIVE YEARS ON
THE LIST

dun's
100

#14 ON DUN'S 100 2022 RANKING OF
BEST STARTUPS



150+ COMBINED YEARS OF
MICROSOFT MVP EXPERIENCE



EY Entrepreneur
Of The Year[®]
2023 Award Winner

EY HONORS SEMPERIS CEO
MICKEY BRESMAN



TOP 10 OF US 100 FASTEST-GROWING
VETERAN-OWNED BUSINESSES