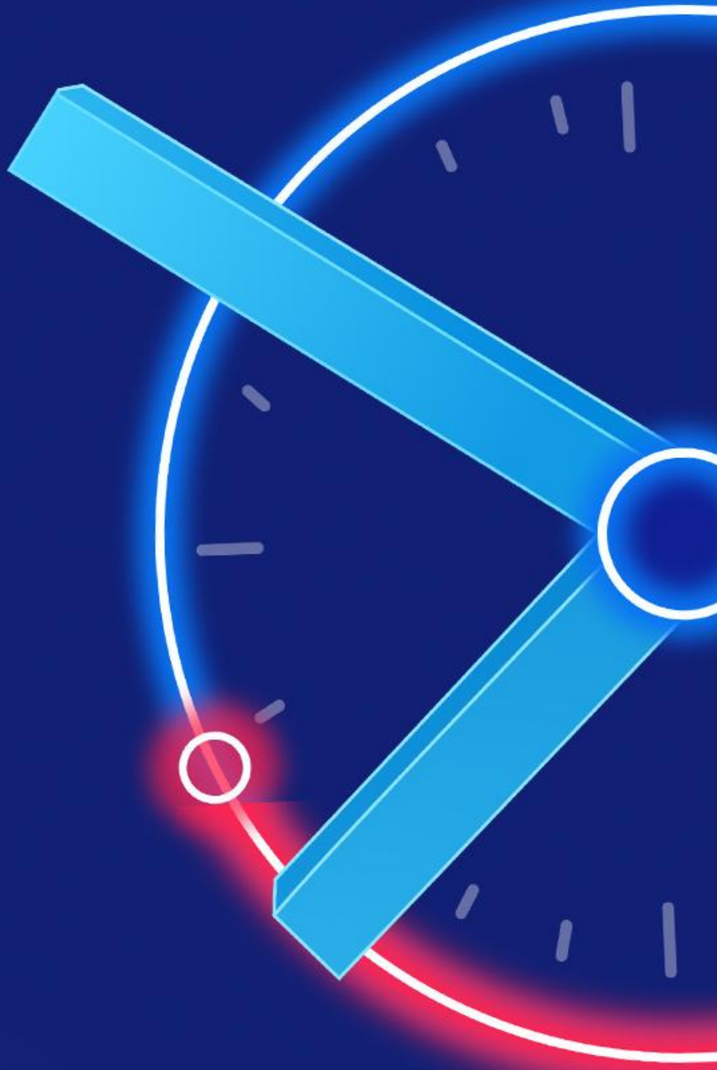
Threat Hunting & Incident Response: Evolving Offense Requires an Evolving Defense

John Anthony Smith
Founder and Chief Security Officer
Fenix24



FENIX 24

John Anthony Smith

Founder and Chief Security Officer, Fenix 24

- Founder & Chief Security Officer of Fenix24 (a Conversant Group company) and five other tech companies.
- Information security fanatic and thought leader through numerous speaking engagements, podcasts, and publications.
- Deep experience with companies in several highly sensitive industries, including healthcare, financial services, and legal.
- Has overseen the design, build, and/or management of infrastructure for more than 400 companies.
- Currently serving as a vCIO and trusted advisor for several companies.
- Extensive experience in legal industry.
- Designed the ILTA first annual cybersecurity benchmarking survey.
- Worked with law firms all over the world, including the U.S, U.K., Australia, New Zealand, Netherlands, & Japan.
- Led his first breach response over 14 years ago and many more since.
- Outspoken advocate for tougher sanctions on nation-states harboring cybercriminals.
- Fervent believer in locating, investigating, and prosecuting cybercriminals

Fenix24 is on the Battlefield Every Day Gathering Real-Time Intelligence Others Cannot

Fenix24 is on the front lines every day, battling cyber terrorists, allowing unique insights into the changing tactics used by threat actors.

Athena7 constantly assesses the infrastructure and technical controls' orchestration organizations are currently using to resist threat actor behaviors and recover from destructive acts.

Grypho5 leverages data from both current threat actor tactics (from Fenix24) and proven cyber tools and processes (from Athena7) to offer the most comprehensive and evolving protection.

Argos99 increases cyber resilience and incident recovery by providing companies with expert insights into their own assets and infrastructure.

1000+ BREACH RESTORATIONS

Breaches Are Inevitable: The Hard Truth

FENIX24

There are two types of organizations: Those that have been hacked and those that will be hacked.

No defense is impenetrable; assume a breach will happen at some point.

Many assumed defensive resistance strategies and technologies are not effective.

Threat actor tactics are evolving among nation-states, ransomware gangs, and insider threats.

Emerging challenges:

- SaaS proliferation
- Work from home/BYOD
- Cloud adoption
- Commercially available software malicious use / ingress abuse
- Software/hardware manufacturer-led security
- AI-driven malware
- Supply chain attacks
- Zero-days
- Data extortion
- Deep fakes — Very easy to hire a threat actor

Now is the time to shift from prevention-first to a resilience-first strategy!

EVERYONE THINKS BACKUPS WILL SURVIVE…
But Reality Serves Up a Wake-Up Call

FENIX24

Fenix24 Intel:

84%

of critical backups did not survive threat actors' behaviors

of the 16% that survive

50%

of backups that survive cannot provide a suitable recovery timeline

And even when ransom is paid

33%

of the data will be unrecoverable: corrupted / damaged / deleted

Athena7 Intel:

90%

cannot meet their stated RTOs

86%

have no survivable backup copies

76%

knowingly do not have all known critical data backed up

WHY TRADITIONAL CYBERSECURITY DEFENSES ARE FAILING

- Threat actors now use commercially available tools
- Slow detection and response cycles, short dwell time
- Ease of lateral movement
- Complex and fragmented IT environments
- IT teams don’t obfuscate their own admin access to systems
- Solutions are implemented without breach context awareness

Why Traditional Cybersecurity Defenses are Failing

Improper data backup orchestration — *or no backups at all*

Alert fatigue and resource constraints

Gaps in defense

- Blind spots in cloud, SaaS, and OT environments
- Slow response to lateral movement
- Limited visibility and detection gaps
- Lack of asset inventory
- Insufficient breach alignment
- Insufficient complexity of IT access

Common Defense Control Issues

In an assessment of clients over the past ~2.5 years, Athena7 found these most common security issues…

- **85%** allow SaaS exposure to the public internet while having those apps SSO integrated
- **92%** allow commercially available remote access solutions — no stacked blocking at endpoint and perimeter
- **69%** allow users to use any password vault
- **92%** allow users to cache credentials in browsers

Common Defense Control Issues

Athena7 also uncovered these security issues…

- 85% allow users to access personal file and e-mail services
- 0% of the assessed organizations have administrative identity segmentation — critical consoles — 100% have critical consoles co-joined with AD
- ~14% of organizations had one (1) loosely survivable backup copy. Conversely, 86% do not have one (1) survivable backup copy
- Only 13% of organizations with cloud environments back up their cloud with an immutable copy outside of the tenant (GCP, AWS, and Azure specifically)

Console Segmentation and Readiness: By the Numbers

Athena7 battalion found…

- **100%** have critical consoles accessible from user segments
- **100%** had critical consoles AD-joined
- **87%** had no IP restrictions, or similar restrictions, on publicly accessible systems
- **55%** had non-existent or non-restricted MFA
- **45%** had AD access on IPMI/iLO/DRAC

Console Segmentation and Readiness: Risks Abound

FENIX 24

Nearly all assessed orgs had the following risks…

- Using daily driver accounts for critical console access
- Allowing credential caching in browsers
- Allowing production AD SSO joined IT vaults
- Allowing IT vaults to store break glass creds
- Having self-service pwd reset enabled (users & admins)
- No lateral movement protections for system admin functions (e.g., MMC, WMI, RDP, WinRM, PowerShell)
- No admin segment/VLAN for critical consoles
- Critical consoles accessible from prod AD creds.
- Immutability not configured, and if configured, commonly will not hold up

Know the Enemy: Scattered Spider

Who is Scattered Spider?

Scattered Spider is a highly-active threat actor group known of its use of social engineering, identity-based, and ransomware attacks.

This threat actor is dangerous for:

- Known for manipulating user facing systems and processes to gain initial access – ServiceNow, SSPR, & Help Desk.
- Commonly performs double extortion: Exfiltration + Encryption
- Commonly successfully targets backup systems/data
- Has targeted technology, telecommunications, hospitality/gaming, healthcare, & critical infrastructure.
- Most recently, Scattered Spider has attacked retail, insurance, & airline companies.

Notably, Scattered Spider attacked MGM Resorts and Caesars Entertainment in September 2022, resulting in major service disruptions and multi-million-dollar losses.

TA Gains Access to Victim's Systems

FENIX24

1 Threat actor calls help desk, requests password/MFA reset for non-privileged acct.

2 TA then obtains access to a publicly accessible ServiceNow instance.

3 Organization unwittingly provides TA with documentation to reset the privileged credential, via ServiceNow instance.

4 TA obtains enough data to answer all password / MFA reset questions.

5 TA calls help desk again and receives a privileged credential / MFA reset.

6 Credential reset allows TA to access organization's VPN and gain persistent access.

How Orgs are Vulnerable

FENIX24

- Threat actor calls help desk, requests password/MFA reset for non-privileged acct.
- Many companies outsource help desk functions to third parties: reference the lawsuit between Clorox & Cognizant.
- It is virtually impossible, without verification steps, for a help desk to know all users' voices and appearances.
- With AI, it is easily possible for a TA to simulate the voice or appearance of a user.
- Leaders/owners, in many companies, demand to not be bothered with identity verification processes, and thus, company help desks do very little identity verification to reset credentials / MFA.

- Asking for internal extension number or employee ID is not sufficient identity verification.
- At minimum, video, ID, and one-time passcode verification is necessary to safely reset credentials and MFA.

  However, there are technologies, such as Nametag, Polyguard, & Clarity, that can make these processes faster/easier.
- Though not a tactic traditionally of Scattered Spider, remote hiring processes must evolve; drug screening is an "easy" way to verify identity.
-

  SaaS applications, such as Workday, ServiceNow, Office 365, iManage, NetDocs, etc. are exposed publicly.

Persistent Access to Systems

FENIX24

1. TA bypasses MFA because help desk resets password and MFA for them.

2. TA uses credentials to log into Cisco AnyConnect VPN.

3. TA moves laterally into VMWare vCenter, a centralized management platform for the VMWare virtualization environments—directly from the VPN.

4. vCenter allows admins to manage multiple ESXi hosts and their association virtual machines from a single location.

How Orgs are Vulnerable

- VPN, Citrix, AVD, and/or Horizon commonly do not have MFA—shockingly.
- Weak forms of MFA are allowed, such as SMS, E-mail, & Phone Call.
- Remote platforms do not establish device trust. Verify that the connecting device is company-owned and/or safe.
- VMWare vCenter is connected, administratively, to Active Directory.
- Privileged credentials can log into VPN, Citrix, AVD, and/or Horizon — or other forms of remote access.
- vCenter, and other critical consoles, are accessible from the remote access platforms — they are not segmented away from these network segments.
- Backup infrastructure is virtualized — and therefore destroyed.
- VMWare vCenter, ESXi hosts, and servers are permitted to browse out to the public Internet on any port.

Mandiant is Catching On

“To effectively safeguard critical Tier 0 assets operating within the vSphere environment — specifically systems like Privileged Access Management (PAM), Security Information and Event Management (SIEM) virtual appliances, and any associated AD tools deployed as virtual appliances — a multilayered security approach is essential. These assets must be treated as independent, self-sufficient environments. This means not only isolating their network traffic and operational dependencies but also, critically, implementing a dedicated and entirely separate identity provider (IdP) for their authentication and authorization processes. For the highest level of assurance, these Tier 0 virtual machines should be hosted directly on dedicated physical servers. This practice of physical and logical segregation provides a far greater degree of separation than shared virtualized environments.”

https://cloud.google.com/blog/topics/threat-intelligence/vsphere-active-directory-integration-risks

Elevated Access Achieved

FENIX24

1 TA achieves elevated access to organization's environment once help desk resets privileged credential.

2 TA now logs into CyberArk instance: Organization uses CyberArk privileged credential vaulting

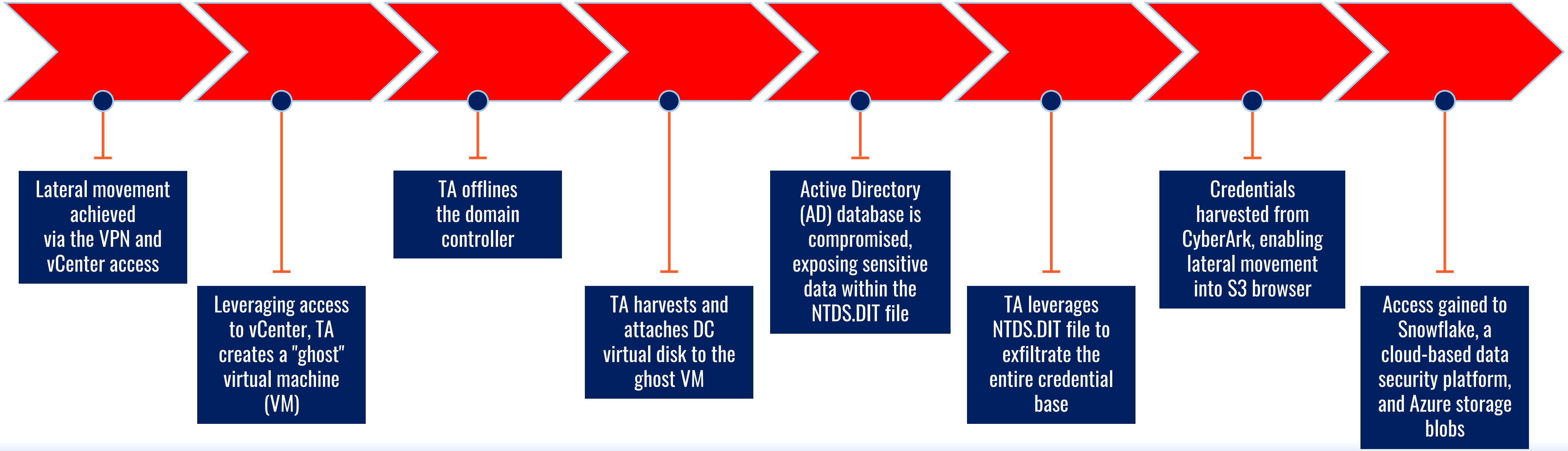
3 Evidence suggests TA harvested additional credentials to access even more data from CyberArk.

4 Access gained to the very tooling that the organization uses to protect its credentials.

5 Leveraging, essentially the entire credential basis, the TA accessed anything desired with great ease

Lateral Movement / Exfiltration

Scattered Spider Moves Latterly Within the IT Environment



Lateral movement achieved via the VPN and vCenter access

Leveraging access to vCenter, TA creates a "ghost" virtual machine (VM)

TA offlines the domain controller

TA harvests and attaches DC virtual disk to the ghost VM

Active Directory (AD) database is compromised, exposing sensitive data within the NTDS.DIT file

TA leverages NTDS.DIT file to exfiltrate the entire credential base

Credentials harvested from CyberArk, enabling lateral movement into S3 browser

Access gained to Snowflake, a cloud-based data security platform, and Azure storage blobs

How Orgs are Vulnerable

- No alerts when virtual machines are created, brought offline, or deleted. The TA shutdown a non-FSMO Active Directory role holder. Detached the disk and reattached the disk to a new VM to harvest the NTDS database.

- **Privileged password vault/PAM cojoined to production Active Directory.**

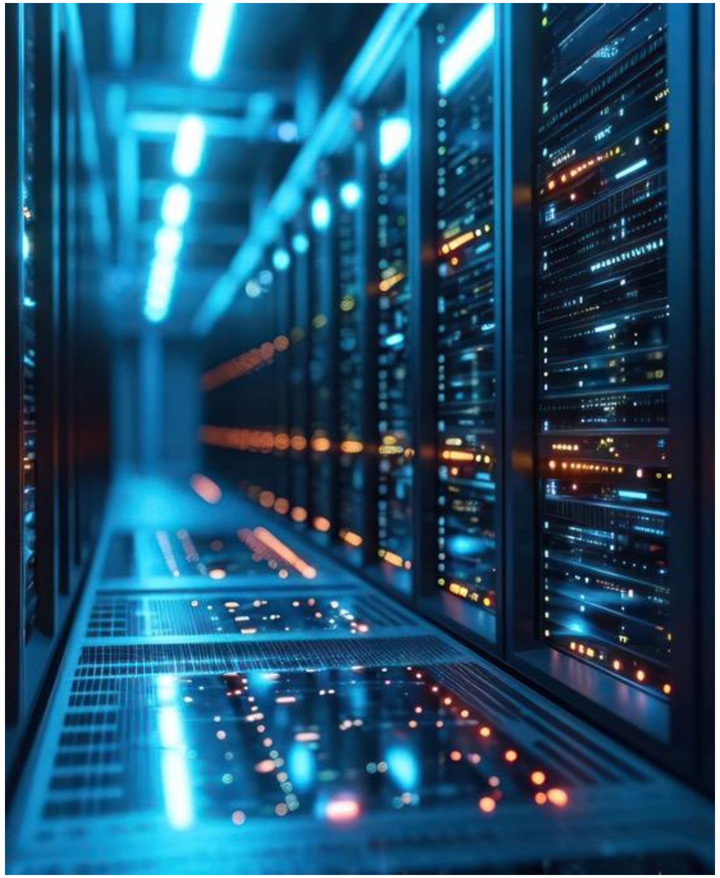
- Weak MFA enabled on privileged creds — or none.

- Password vault / PAM accessible publicly or from user segments, such as AVD, Horizon, Citrix, & VPN. Cloud, publicly exposed vaults are dangerous as normally implemented—per vendor guidance.

- RDP is commonly broadly accessible to all user segments — without MFA.

- Self-Service Password Reset methods enabled and require very little to orchestrate a reset.

- Cloud services consoles do not have MFA, credentials are placed in password vaults cojoined to Active Directory, or cloud services consoles are cojoined to AD themselves.



Lateral Movement / Exfiltration

Scattered Spider moves freely inside the environment to exfiltrate data

Harvested creds to exfiltrate data from Snowflake

Data backups not encrypted

Hard shutoff of network access rapidly evicts TA

TA does not have sufficient time to locate backups

In an alternate scenario…backups survive but are encrypted because they are misconfigured

How Orgs Are Vulnerable

- Many companies' IR plans likely do not contain plans for disabling all Internet access — all locations.
- In the example, the disablement of Internet access prevented recovery capability damage.
- When backups are stored or orchestrated through integrations with storage, vCenter, and Active Directory, they are commonly encrypted or deleted.
- vCenter, backup systems, and storage should be completely detached from production Active Directory.
- Integration with storage snaps for backup, commonly, put production storage and all snaps at risk of destruction.
- Administrative integration of vCenter with backups and storage allow TAs to easily destroy storage and backups.
- You should stop buying into backup product companies' strategies for backup data preservation.

Backup Destruction

FENIX 24

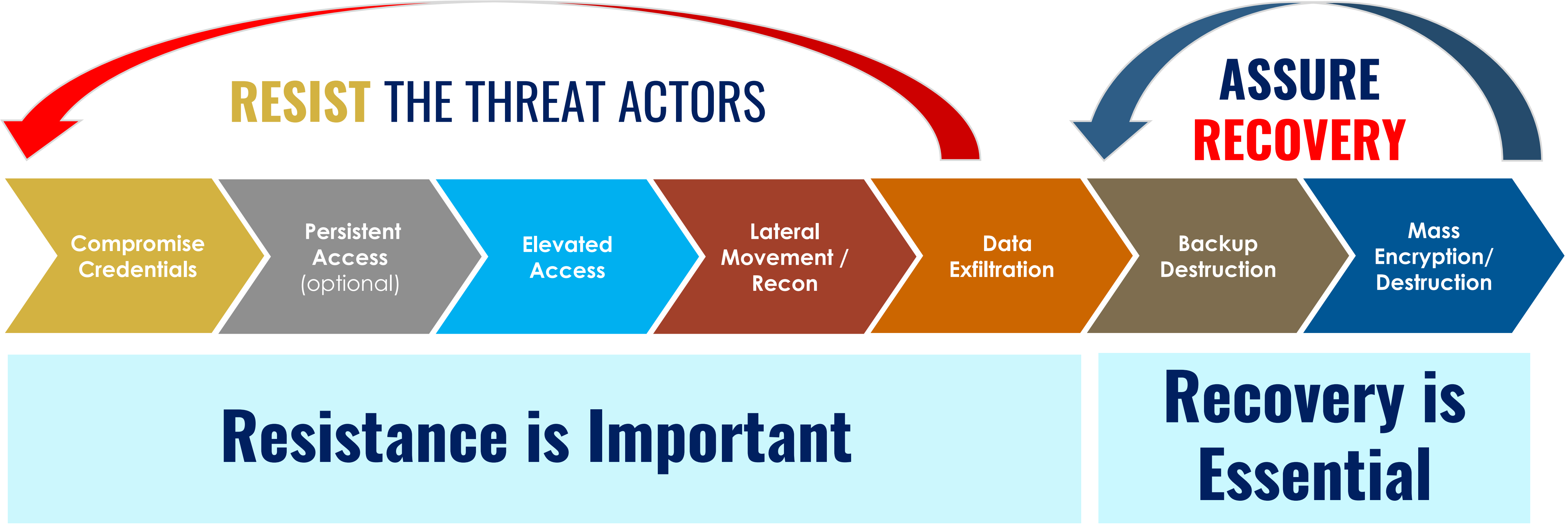
★ What did the organization do right?

- **Veeam not inside the domain.**
- Pivotally, rapid eviction of the TA (hard shutoff of the network) enabled survival of the backups.

🚫 What did the organization do wrong?

- Veeam could have been destroyed because its creds were likely in CyberArk.
- Veeam had elements that were virtualized and VMWare is a common target.
- Data domain had creds in the CyberArk (password vault).
- CyberArk instance was connected to the production AD domain.
- The proper processes for resetting privileged credentials were lacking.
- MFA not enforced on all Snowflake accounts.
- Admin creds, to all critical consoles, should have required verified MFA push.
- Snowflake console was not IP limited, although this context probably would not have saved them, as the TA was in their environment.
- In a best-case scenario, the Snowflake admin console would not have been publicly accessible.

BREACH PATH:
Changing Tactics But a Consistent Pattern



SECURITY SHOULD BEGIN WITH YOUR ATTACKER'S END GAME IN MIND

BECAUSE YOU KNOW THE END GAME

FENIX24

RECOVER > RESIST

HARDEN IN REVERSE: ASSURED RECOVERY

Compromise Credentials

- No forced password hygiene.
- Password length too short (12 char).
- Password caching allowed in browsers.
- Weak forms of MFA permitted - SMS and phone call; strong MFA not in use.
- Passwords & tokens likely cached on personal devices
- No geo-blocking, impossible travel, or malicious logon detection enabled in MS Authenticator or Okta.
- Vendors have access to VPN.
- There is no standard web browser: Chrome browser is in use & personal e-mail access is not blocked.
- Personal webmail and social media platforms are not blocked.
- Device trust is not required for VPN.
- SaaS, cloud-based tools are accessible off the VPN.

Persistent Access

- VPN could be accessed without corporate device.
- Always-on, full VPN not used.
- SOC minimally involved in kill chain, requires explicit approval from client.
- No geo-blocking of outbound and inbound traffic.
- RBAC and least privilege are not uniformly enforced across admin consoles.
- No complimentary AV/EDR platform on endpoints.
- Unauthorized code permitted to execute.
- Commercially available remote access tools are not blocked.
- Unrestricted egress possible from Org offices.
- MFA self-enrollment permitted.
- Weak OKTA configuration: daily driver accounts used for administration.

Elevated Access

- Users permitted to cache credentials in browser (observed in several sessions).
- Daily driver accounts used for access to privileged credential vault.
- Service account usage not restricted to specific source and target nodes.
- Some storage administratively integrated with vCenter.
- Service acct passwords are likely not regularly changed.
- PAM (and user password vault since it has privileged credentials) accessible from user segments.
- Firewall & web filtering likely allow third-party password vaults: no categorical blocks.
- User Password Vault is used for privileged credentials and is integrated with prod AD.
- Break glass and admin. accounts for sensitive and foundational infrastructure stored in PAM.
- Admins can leverage MFA authenticators permitted backed up to Google and iCloud, Google Authenticator.

Lateral Movement

- MFA is not required for administrative function via PowerShell, WMI, MMC, & WinRM.
- Apps do not require MFA when on VPN.
- RDP to servers is enabled without MFA.
- Sensitive admin systems accessible directly from user segments (and VPN).
- Segmented admin Azure AD tenant does not exist: Sensitive infrastructure is co-joined to production user AD.
- EDR is not natively IP restricted to dedicated mgt/admin segment.
- No rapid SOC isolation of node, identity, e-mail, and IP.
- MFA, on-prem, can likely be interrupted by shutting down virtual machines.

Data Exfiltration

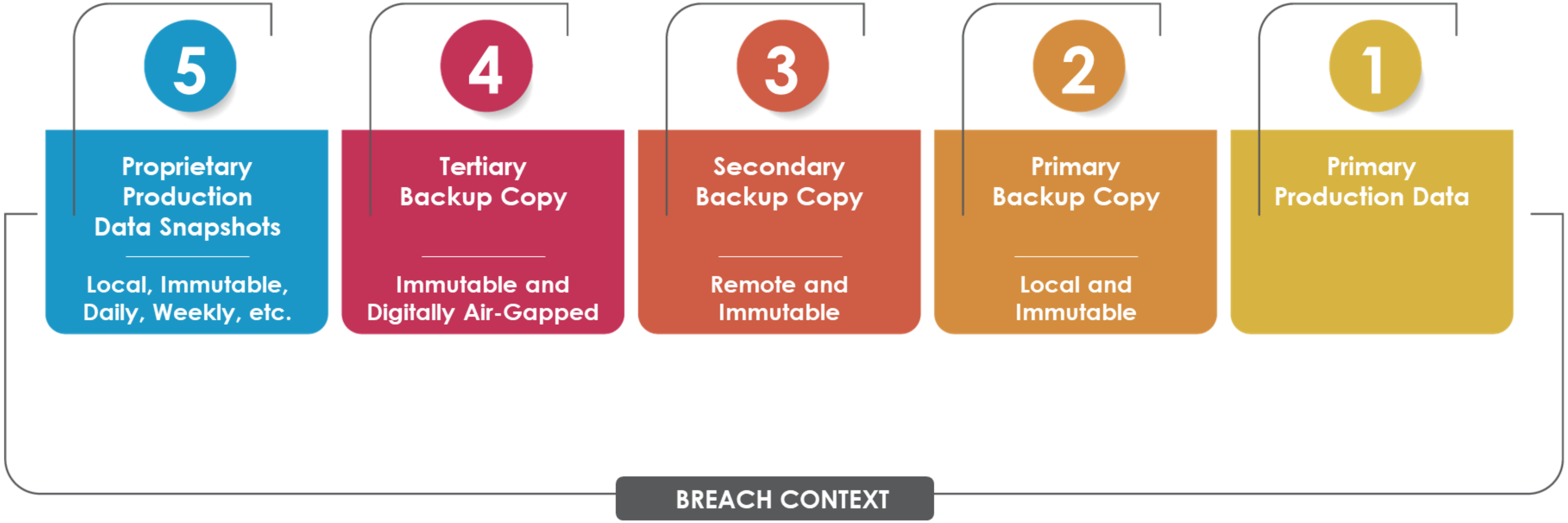
- Remote connectivity via split tunnelling.
- Exec. DNS filtering less restricted than most users (e.g., blanket allow for file sharing).
- Limited to no port restriction at the perimeter.
- Server segments are permitted to browse the Internet.
- Firewall and web filtering solution administratively integrated with AD.
- Effective stacking of categorical web blocking not present: remote access technologies, peer to peer, etc are also not blocked.
- Limited outbound geoblocking.
- DOH, DOT, and Tor likely not blocked.

Mass Encryption/ Destruction

- iLO/iDRAC likely accessible from user segments and possibly AD credentials.
- PAM, storage product, vCenter, EDR, Azure, user password vault, replication product, and AWS are all administratively accessible from user segments.
- PAM, replication product, storage product, user password vault, vCenter, EDR, Azure, & AWS are all administratively accessible with production AD credentials.
- Critical console creds are stored in Secret Server.
- No separate VLAN, jump box, or ACLs to limit access to sensitive consoles.
- No IP restriction in EDR—accessible from public Internet.

Survivability: 5-4-3-2-1

5-4-3-2-1 Grypho5 Proprietary Method



5

Proprietary Production Data Snapshots

Local, Immutable, Daily, Weekly, etc.

4

Tertiary Backup Copy

Immutable and Digitally Air-Gapped

3

Secondary Backup Copy

Remote and Immutable

2

Primary Backup Copy

Local and Immutable

1

Primary Production Data

BREACH CONTEXT

Across all copies

- Backed up nightly without exception
- Immutable and encrypted by default
- Least privileged IAM policies by default
- Weekly, monthly, and semi-annually restore tests
- All discovered data is protected

Actions You Can Take Now

Assess the organization's recovery capabilities against breach contact (Athena7).

- Evaluate the efficacy of the organization's key applications' data and critical infrastructure.
- Measure survivability, usability, and timely recoverability against a proper definition of immutability, breach context, and breach context born principles.

Establish retainer with a restoration company (Fenix24).

Align leadership to mass recovery realities: point and time (Athena7).

Prioritize mass recovery, as mass destruction is the most likely form of disaster for most companies.

- Assure recovery from mass & backup destruction.
- Reassure recovery continually (Grypho5).

Establish a recovery zone where mass restoration can be safely tested and RTO regularly measured (Grypho5).

Regularly test and harden recovery capabilities to establish predictable recovery timelines (Grypho5).

Complicate and obfuscate critical console administrative identity (Grypho5).

- Segment critical consoles, such as password vaulting, EDR, vCenter, and storage.
- Apply MFA to all administrative functions.

Fenix24 and ILTA Release 2025 Research Report

International Legal Technology Association | FENIX24

JULY 2025

Security at Issue:
State of Cybersecurity in Law Firms

Results of the ILTA • Fenix24/Conversant Group Cybersecurity Survey

See us for your own printed copy of the report.

Key Insights from the report:

- Phishing is seen as the top security threat (new to the 2024 survey results), followed by data exfiltration, ransomware, and social engineering.
- There is a decrease in user behavior (#5 on the list), which was seen as the top security threat in the previous year's report.
- Backup solutions are increasing as a top security tool, #4 on the list, but only 27% of respondents name them as *critical*, up from 11% in the previous year's survey.
- Only 50% of responding firms have at least one backup system capable of immutability.
- Law firms exhibit a sharp rise in assessments / tabletop exercises / pentesting as a driver of change.
- IR planning correlates closely with overall security confidence. In fact, 90% of law firms rate themselves *extremely secure. A*nd 84% of firms that rate themselves as *very secure* have updated their IR plans within the last 12 months. Notably, it is maintaining the IR plan itself — not testing — that correlates with improved confidence.

COME CHAT WITH US

FENIX24

FENIX24 — A CONVERSANT GROUP COMPANY — Recovery & Restoration

ATHENA7 — A CONVERSANT GROUP COMPANY — Strategy & Execution

GRYPHO5 — A CONVERSANT GROUP COMPANY — Managed Protection

ARGOS99 — A CONVERSANT GROUP COMPANY — Asset & Resiliency Software

If you would like a copy of the presentation, please scan the QR code.

FLOWCODE

PRIVACY.FLOWCODE.COM

SCAN TO DOWNLOAD

THANK YOU!