FENIX 24®

CONVERSANT GROUP®

# Anatomy of a Cyberattack: A Live Walkthrough

ILTACON 2025

John Anthony Smith, Founder & CSO, Fenix24

# JOHN ANTHONY SMITH

- 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.
- Takes cyberattacks personally.
- Outspoken advocate for tougher sanctions on nation-states harboring cybercriminals.
- Fervent believer in locating, investigating, and prosecuting cybercriminals.

John Anthony Smith
Fenix24
Founder &
Chief Security
Officer

# 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.*

## 2000+ BREACH RESTORATIONS

# Fenix24 on the Battlefield Every Day

*In 2025, we underwent a rebrand whereby the Fenix24 battalion ascended to the new name of our company. That's because, first and foremost, we are the world's leading ransomware restoration and recovery company. Truly, based on our work helping thousands of organizations recover from some of the world's most devasting attacks, with a minimum of operational downtown, no other service provider comes close to our capabilities. For that matter, recovery is the new defense.*

*Operating as the "World's First Civilian Cybersecurity Force, Fenix24 is leading a new paradigm in cybersecurity by emphasizing the ability to recover from a breach over the capacity to prevent one. In fact, Fenix24 offers its customers an assurance of recovery, while hardening cyber defenses through its comprehensive Securitas Summa program.*

# Fenix24 Breach & Threat Actor Stats

**Threat Actors Groups Tracked 2025**

Aid Locker 1
Akira 18
BERT 1
Blackcat 1
BlackNevas 1
Cactus 2
CL0P 1
Embargo 1
Fog Group 2
Hunters International 1
IMN 1
Inc Ransom 1
Insider Threat 1
InterLock 1
LockBit 1
LockBit 3.0 1
Lynx 3
Medusa 5
Mimic 1
Play 2
Prophet Spider 1
Qilin 4
Ran Some Wares 1
RansomHub 6
Rhysida 2
SafePay 1
Scattered Spider 5
Standalone Actor 1
Unknown 15

**2025 Engagements: 83**

**Unique Threat Actors: 27**

# Fenix24 Breach & Threat Actor Stats

## Threat Actors Groups Tracked 2024

Qilin 1
.flocker .fog 1
8Base 1
Abyss 1
Akira 30
Alpha 1
BianLian 1
BlackBasta 12
BlackByte 3
Blacksuit 13
Cactus 1
Cicada 3301 1
Duram 1
Embargo 1
Faust 1
Fog Group 15
HelloKitty 1
Hunters International 6
Inc Ransom 5
KalajaTomorr 1
Lockbit 4
LockBit 3.0 7
Lynx 3
LynxCrypt 1
Medusa 5
Nebula Group 1
Notchy 1
Play 9
Prophet Spider 1
Punk Spider 1
Qilin 8
Rancoz 2
Ransomhub 9
RecessSpider 1
Rhysida 4
SafePay 2
Scattered Spider 7
Standalone Actor 1
The Underground 1
U-Bomb 1
Unknown 21
Wandering Spider 1

**2024**
**Engagements: 188**
**Unique Threat Actors: 50**

# The Enemy: Scattered Spider

## Who is Scattered Spider?

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

**This threat actor group is dangerous for:**

- Blending nation-state level social engineering with financially motivated ransomware attacks
- A cloud-first focus that makes traditional endpoint-based defense insufficient
- Being highly adaptive, switching tools and infrastructure frequently

## Primary Targets

**US companies across various industries, including technology, telecommunications, hospitality/gaming, healthcare, and critical infrastructure. More recently, Scattered Spider has attacked insurance and retail organizations.**

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

# The Enemy: Scattered Spider

## Scattered Spider First Seen

Active since mid-2022, with sharp rise in activity through 2023-2024.

## Origin

Believed to be native English-speaking members, often based in the U.S. and U.K., which makes them unusual among financially-motivated threat groups.

## Affiliations

Formerly affiliated with ALPHV/BlackCat ransomware group, possibly independent operators with links to ransomware-as-a-service (RaaS) ecosystems.

## Tactics, Techniques and Procedures (TTPs)

Scattered Spider is infamous for its TTTs involving social engineering, MFA fatigue attacks, cloud and identity exploitation, data theft and ransom, and Living Off the Land.

# BREACH PATH:
## Changing Tactics but a Consistent Pattern


### RESISTANCE

- Resist the threat actors

**Resistance is Important**

### RECOVERY

- Ensure recoverability

**Recovery is Essential**

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

# Anatomy of a Cyberattack: Compromised Credentials

## Scattered Spider Gains Access to Risk Management Organization's IT Network

1.) Threat actor calls help desk, requests password reset for non-privileged account.

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

3.) Organization unwittingly provides TA with documentation to reset the privileged credential.

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

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

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

# Anatomy of a Cyberattack: Persistent Access

## Scattered Spider Maintains Persistent Access to the Organization's IT Network

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 EXSi hosts and their association virtual machines from a single location.

# Anatomy of a Cyberattack: Elevated Access

## Scattered Spider Achieves Elevated Access to the IT Environment

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

2.) TA now has access to CyberArk instance. Organization uses CyberArk for identity management and privileged access management.

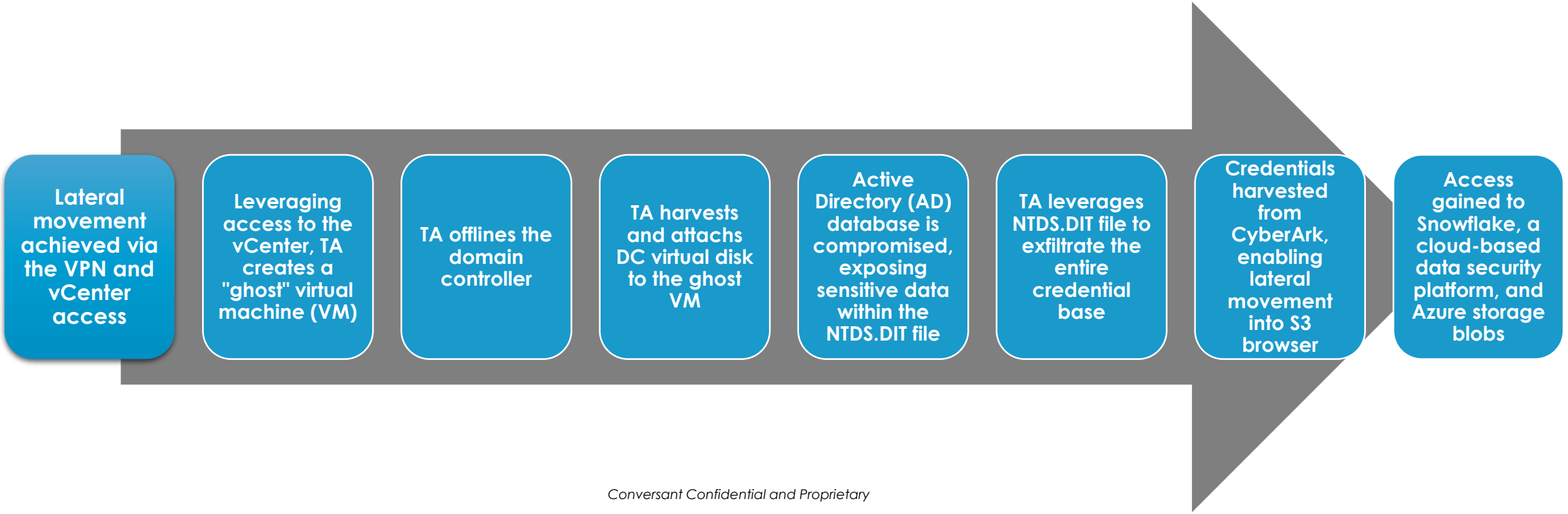
3.) Evidence suggests TA harvested additional credentials to access even more data from CyberArk.

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

5.) TA can now actually violate the credentials to gain more credentials and continue to elevate access.

# Anatomy of a Cyberattack: Lateral Movement

## Scattered Spider Moves Latterly Within the IT Environment



# Anatomy of a Cyberattack: Data Exfiltration

Scattered Spider moves freely inside the environment to exfiltrate data

Harvested credentials 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

# Anatomy of a Cyberattack: Mass Destruction

**TA leverages access to vCenter to fully encrypt all Virtual Machine Disks (VMDKs) using DragonForce**

**What did the organization do wrong?**

- vCenter connected to the domain
- VCenter accessible from user segments
- CyberArk connected to the domain, accessible from user segments

# Anatomy of a Cyberattack: Backup Destruction

## 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 probably had elements that were virtualized and, likely, VMWare is a common target.
- Data domain likely 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.

# HARDEN IN REVERSE: Assure Recovery

FENIX 24

## RESIST THE THREAT ACTORS

## ASSURE 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.
- Active Directory DCs not hardened for lateral movement and credential capture.
- Some users permitted to use personal e-mail services.

### 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.

### Backup Destruction

- Not following 5-4-3-2-1.
- Most backups are not immutable.
- Replication product administration uses AD creds: target vol's not snapped.
- Backup admin accts in SS & AD.
- AWS S3 and Azure Blobs are not being backed up; however, do contain critical data.

Backup console is AD integrated.

Most volumes/data are not immutably, natively snapped on shared storage.

CIFS/NFS NAS data is not backed up.

Backup solution Azure Blob target is not marked for immutability and exists in the primary Azure tenancy.

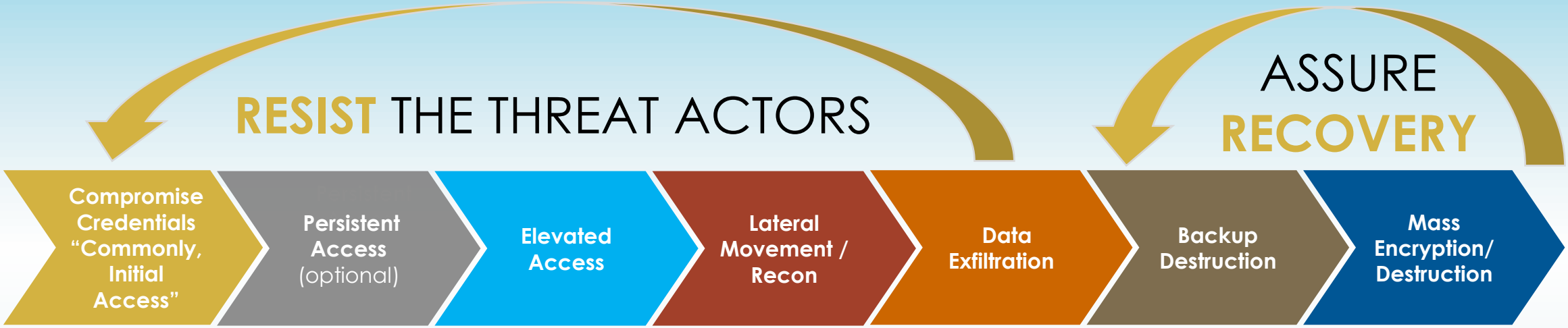
IPMI is connected on backup devices.

- Two-person rule is not enabled on the backup devices.
- Some critical SaaS applications are likely not backed up.
- DevOps tools and projects are not being backed up by controlled tools.
- Mass recovery capability not tested.

### 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.

# HARDEN IN REVERSE: A Matter of When, Not If




- Proper resistance should be predicated on an assured recovery — **counter cultural paradigm.**
- Recovery can only be assured through **constant orchestration and re-orchestration** to Breach Context.
- Breach Context, and the correlating orchestration, with a committed investment in breach context orchestrated, pre-staged, and regularly tested **mass recovery capability are the MISSING link to reducing costly business interruption (downtime).**
- The single biggest expense in breach **is business interruption — 60-80% of the cost.**
- If we really believe that ALL breaches are IMPOSSIBLE to prevent, then we must believe and **commit to an assured recovery outcome** — we believe this to be true — Securitas Summa.

# Survivability: 5-4-3-2-1

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

**5 — Proprietary Production Data Snapshots**
Local, Immutable, Daily, Weekly, etc.
Backed Up Nightly without Exception

**4 — Tertiary Backup Copy**
Immutable and Digitally Air-Gapped
Immutable and Encrypted by Default

**3 — Secondary Backup Copy**
Remote and Immutable
Least Privileged IAM Policies by Default

**2 — Primary Backup Copy**
Local and Immutable
Weekly, Monthly, and Semi-Annually Restore Tests

**1 — Primary Production Data**
All Discovered Data Protected

**BREACH CONTEXT**

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

## Fenix24 Intel:

**84%**
Critical backups did not survive threat actors' behaviors

of the 16% that survive

**50%**
Cannot provide a suitable recovery timeline

And even when ransom is paid

…AND

**33%**
Of the data will be unrecoverable: corrupted / damaged / deleted

## Athena7 Intel:

**90%**
Cannot meet their stated RTOs

**86%**
Have no survivable backup copies

…AND

**76%**
Knowingly do not have all known critical data backed up

# Breaches Are Inevitable

## The Hard Truth…

- **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!***

# WHAT TO DO NOW:
# Actions You Can Take

FENIX 24

**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


## 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*. And 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.