FENIX 24®

2025

The Evolution of Security Operations: What's Working, What's Not, What's Next

NYS Cybersecurity Conference

John Anthony Smith, Founder & CSO, Fenix24

EVOLVING OFFENSE REQUIRES EVOLVING DEFENSE™

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 over 400 companies.
  - Currently serving as a vCIO and trusted advisor for several companies.
  - Former Director of IT for a law firm.
  - Designed the ILTA first annual cybersecurity benchmarking survey.
  - Worked with law firms all over the world: U.S, U.K., Australia, New Zealand, Netherlands, Japan.
- Led his first breach response over 14 years ago and many more since.
- Takes breaches personally.
- Outspoken advocate for tougher sanctions on nation-states harboring cyber criminals.
- Fervent believer in locating, investigating, and prosecuting cybercriminals.

John Anthony Smith
Fenix24
Founder & Chief Security Officer

FENIX24

WE ARE 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.

AGENDA

FENIX24

- Introductions
- Evolution of Cybersecurity
- What's Working, What's Not, What's Next
- Breaches are Inevitable: High-Profile Breaches in the News
- Common Defense Control Issues
- Critical Console Identity Segmentation & Readiness
- Why Traditional Cyber Defense are Failing
- The Evolving Threat Landscape
- What is Breach Context & Pattern
- The Path to Recovery
- Hardening in Reverse
- Modern Defense Strategies / Survivability
- Actions You Can Take Now

The Evolution of Cybersecurity

The Early Days (1970s – 1990s): Reactive Defense

- **Focus:** Physical security and basic password protection
- **Milestones:**
  - 1971: First computer virus ("Creeper")
  - 1988: Morris Work highlights need for network security
- **Tools:** Firewalls, antivirus software, basic intrusion detection systems
- **Approach:** Reactive — defend against known threats

The Internet Age (2000s): Perimeter Security

- **Focus:** Protecting the network edge
- **Milestones:**
  - Rise of personal and enterprise internet use
  - Proliferation of worms (e.g. Code Red, SQL Slammer)
- **Tools:** Firewalls, IDS/IPS, VPNs, endpoint protection
- **Limitations:** Couldn't prevent insider threats or sophisticated external breaches

Advanced Threat Era (2010s): Defense in Depth

- **Focus:** Multi-layered security; threat detection and response
- **Milestones:**
  - Target, Sony, and OPM breaches signal the rise of APTs
  - Growth of zero-day vulnerabilities
  - Proliferation of financially motivated ransomware
- **Tools:** SIEMs, EDR, sandboxing, threat intelligence platforms
- **Approach:** Proactive threat hunting, behavior analytics

Cloud & Mobility (Late 2010s – 2020s): Zero-Trust & Identity Centric Security

- **Focus:** Identity and data as the new perimeter
- **Milestones:**
  - Explosion of Saas, remote work, BYOD
  - Nation-state threats and ransomware-as-a-service
  - Explosion of financially motivated TA activities
- **Tools:** Zero-Trust Architecture, SASE, MFA, CASBs
- **Trends:** Shift-left security in DevOps, "security as code," automation, *recovery over resistance*

What's Not Working

Over-Reliance on Legacy Systems & Insufficient Patching

- Many critical IT networks run outdated software
- Patch delays create persistent vulnerabilities
- Most organizations prioritize public exposed infrastructure and largely ignore internal

Insufficient Standard & IT User Awareness

- Phishing, social engineering remain top attack vectors
- Training programs are often too sporadic and ineffective
- IT access to systems is commonly not complicated & obfuscated
- IT users are commonly governed by different rules — or not at all

Fragmented Toolsets & Alert Fatigue

- Too many tools, improper orchestration
- Tooling configuration not keeping up with breach
- Defenders don't have good access to breach data

Improper SaaS, BYOD, & MFA Restriction

- Authentication and credential theft can occur with great ease
- SIM swapping and external email compromise are common.
- BYOD device backups create easy cred and MFA theft.

Third-Party & Supply Chain Risks

- SolarWinds, MOVEit show deep impact of vendor breaches
- SaaS & cloud proliferation have destroyed the perimeter, making information protection & governance nearly impossible
- Third-party tooling is commonly violated

Disintegration of Network Perimeter

- The network perimeter has been redefined.
- Most organizations do not have control of the perimeter.
- Threat actors commonly use commercial tooling to gain/maintain access and exfiltrate data.

What's Working

Recovery Over Resistance

- Immutable data backups as best defense
- Assumes inevitability of breach; alignment orchestration is necessary
- Tooling must keep up with breach truth; data backup configuration is born from breach
- Configurations must regularly be compared and modified to a gold standard, born from breach
- Detect, contain, & recover quickly; minimize impact; regular testing for mass recovery

Zero-Trust Architecture

- Assumes breach; verifies every request
- Widely adopted in cloud-first and hybrid environments
- Orchestrate all security tooling leveraging breach realities

Multi-Factor Authentication (MFA), Limiting Public SaaS Exposure, Ending BYOD (disaster)

- Properly configured SaaS, MFA, & Authentication Token hardening reduces account takeover significantly
- Increasingly mandatory across industries
- Administrative identity segmentation reduces risk of destructive TA acts; remove consoles out of AD & identity plane

Security Operations Center Monitoring with Automatic Isolation

- Dwell time is commonly short---identities, endpoints, cloud change, and IP addresses believed potentially malicious should automatically isolate

What’s Next

- Recovery is the New Resistance: Immutable Data Backups
- Securing from IT Identity Risk
- Reestablishing a Perimeter
- Threat Intelligence — Configuration Keep Pace with Breach Truth
- Security Operations Enhanced by AI & ML
- Zero-Trust Architecture, Block First
- Identity-Centric Security

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 TA

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

High-Profile Breaches in the News

July 2024: Walt Disney Co. Slack Accounts Hacked

- Hacker group NullBulge claims responsibility for breach.
- Disney employee downloads malware disguised as AI tool.
- Attacker gains access to login credentials and infiltrates Disney’s Slack environment.
- Attacker accesses and leaks over 1.1 TBs of data, compromising 44 million+ Slack messages, exposing sensitive company data.

https://www.msn.com/en-us/news/technology/a-disney-worker-downloaded-an-ai-tool-it-led-to-a-hack-that-ruined-his-life/ar-AA1zOQRm

September 2022: Uber Slack Workspace, Internal Tools Targeted

- Hacker group Lapsus$ compromises Uber contractor’s account by likely purchasing their corporate password on the dark web after contractor’s personal device is infected with malware.
- Attacker contacted contractor via WhatsApp, impersonating Uber’s IT support, convincing contractor to approve MFA request and thereby granting access.
- Attacker accesses Uber’s Slack, other systems.

https://www.theregister.com/2022/09/16/uber_security_incident/

High-Profile Breaches in the News

April 2025: Marks & Spencer Cyberattack

- UK retailer Marks & Spencer suffers cyberattack that disrupts its digital services, including contactless payments and online deliveries.
- Some internal process are moved offline as a precautionary measure to protect shareholders. Some customers face delayed orders.
- Marks & Spencer assures customers that their data is secure and reports the incident to government authorities. No ransom demand is made.

https://www.bleepingcomputer.com/news/microsoft/microsoft-entra-account-lockouts-caused-by-user-token-logging-mishap/

June 2024: NHS Ransomware Attack

- NHS England confirms patient data managed by pathology testing organization Synnovis was stolen in a ransomware attack on June 3, 2024.
- Attack causes widespread disruption to NHS services in southeast London. More than 10,000 appointments and 1,700 elective medical procedures are postponed.
- Qulin, a Russian cybercrime group, shares almost 400GB of private information on their dark web site, including more than 300 million patient records, after Synnovis declines £40 million ransom demand.

https://www.bbc.com/news/articles/c9777v4m8zdo

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% (maybe more) 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% - None 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.
- 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

Fenix24's Athena7 battalion found…

Of Assessed Orgs:

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

Console Segmentation and Readiness: Risks Abound

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

Why Traditional Cybersecurity Defenses are Failing

Threat actors have moved beyond using “malicious” code. They now use commercially available and commonly blanket allowed methods — PowerShell, ScreenConnect, TeamViewer, Google Drive, OneDrive, etc.

Slow detection and response cycles

Lack of targeted identity, network segmentation and blocking tactics.

Complex and fragmented IT environments.

Lack of IT complicating and obfuscating their own administrative access to systems.

No clear way to understand breach realities in context existing tooling configuration.

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

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

FENIX24

Fenix24 Intel:

84%

Critical backups did not survive threat actors' behaviors

of the 16% that survive

ONLY

50%

Of backups that survive cannot provide a suitable recovery timeline

And even when ransom is paid

ONLY

33%

Of the data will be unrecoverable--corrupted / damaged / deleted

Athena7 Intel:

90%

Cannot meet their stated RTOs

ONLY

86%

Have no survivable backup copies

…AND

76%

Knowingly do not have all known critical data backed up

The Evolving Threat Landscape

The cybersecurity threat landscape is becoming more dynamic.

Organizations must stay agile and proactive to defense against these evolving threats…

- **Phishing and social engineering**
- **Ransomware attacks**
- **Advanced Persistent Threats (APTs)**
- **Supply chain attacks — third- and fourth-party vendor vulnerabilities**
- **Insider threats and lateral movement**
- **Cloud security challenges**
- **IoT vulnerabilities**
- **AI and machine learning threats outpacing defense innovation**
- **Zero-day exploits**
- **Human error — *but it's not the user's fault***
- **Cybersecurity skills shortage**

What is Breach Context?

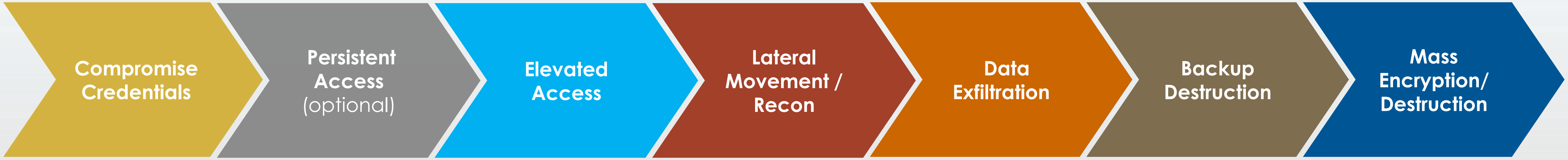
BREACH CONTEXT: Infrastructure and security control configuration alignment to breach realities. Said differently, comparing threat actor technical tactics and methodologies to any company's actual technical control and infrastructure configuration.

How will the infrastructure and control configurations stack up against what TAs can, will, and are doing in breach?

- For example, SaaS providers encourage integration of identity with Active Directory (AD) and use from non-corporate devices.
- In Breach Context, however, SaaS exposure commonly exposes AD credentials and authentication tokens to capture; it actually simplifies TA access.

What is Breach Pattern?

BREACH PATTERN: All breaches follow a similar high-level pattern. Threat actors attempt to gain initial access, create persistent access, elevate permission, move laterally, and commonly attempt data exfiltration. We call these phases of the breach pattern “Resistance Tranches.” After a TA has moved laterally, their ultimate end is one or more of the following: data exfiltration, backup destruction, and/or mass destruction. We call the last two phases, “Backup Destruction & Mass Destruction,” or “Recovery Tranches.”



Compromise Credentials

Persistent Access (optional)

Elevated Access

Lateral Movement / Recon

Data Exfiltration

Backup Destruction

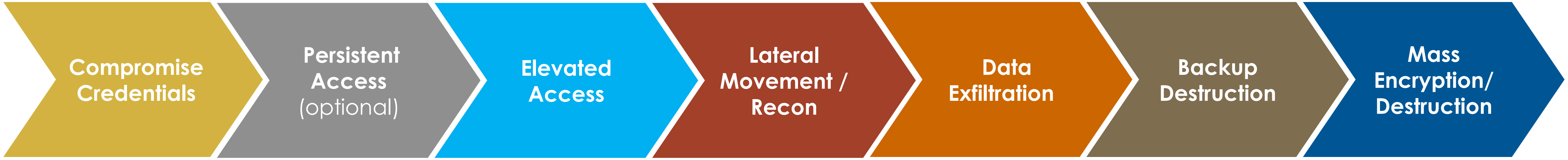
Mass Encryption/ Destruction

Resistance

Recovery

BREACH PATH:

Changing Tactics But a Consistent Pattern



Compromise Credentials

Persistent Access (optional)

Elevated Access

Lateral Movement / Recon

Data Exfiltration

Backup Destruction

Mass Encryption/ Destruction

RESISTANCE

- Resist the threat actors

Resistance is Important

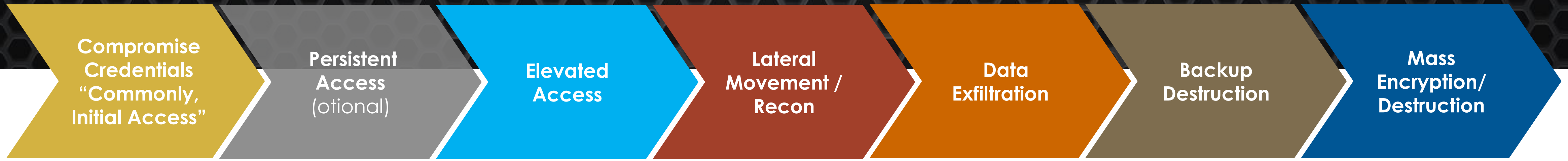
RECOVERY

- Ensure recoverability

Recovery is Essential

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

Why Breach Context & Pattern Matter



Compromise Credentials "Commonly, Initial Access"

Persistent Access (otional)

Elevated Access

Lateral Movement / Recon

Data Exfiltration

Backup Destruction

Mass Encryption/ Destruction

- If this pattern is to be disrupted, **disruption must be done in reverse (right to left)** — starting with the attacker's end game, not the following the flow of the attack (left to right) — which is the common defense philosophy.

- Basically, all organizations are **overinvesting in the first five tranches** and largely ignoring the last two tranches.

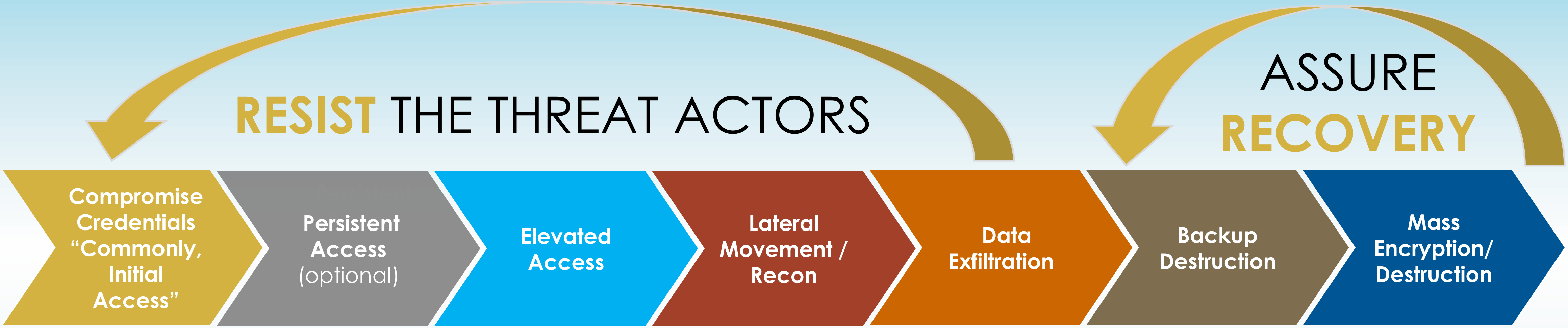
- Despite organizations best investment and effort, resistance controls and infrastructure are largely orchestrated poorly. There are many reasons for this, but the foundational reason is the **LACK of BREACH CONTEXT!**

Lack of Breach Context Causes Destruction

- Breach context, if leveraged as a guide to Breach Pattern disruption, commonly will dictate **configuration that is contrary to industry "best practice" or a "common IT understanding."**

- Without Breach Context, defenders are left to their own best judgment about how systems should be orchestrated and, therefore, **commonly make significant missteps** that will exacerbate TA destructive possibility.

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.

The Path to Recovery:

RESTORATION TIME (MTTR)

A recovery timeline requires multiple steps

Forensics & Containment

A cyberattack is a crime scene.

Forensics capture, containment, & isolation are requisite to restoration.

Readiness

Beyond having data:

Does infrastructure exist to rehydrate?

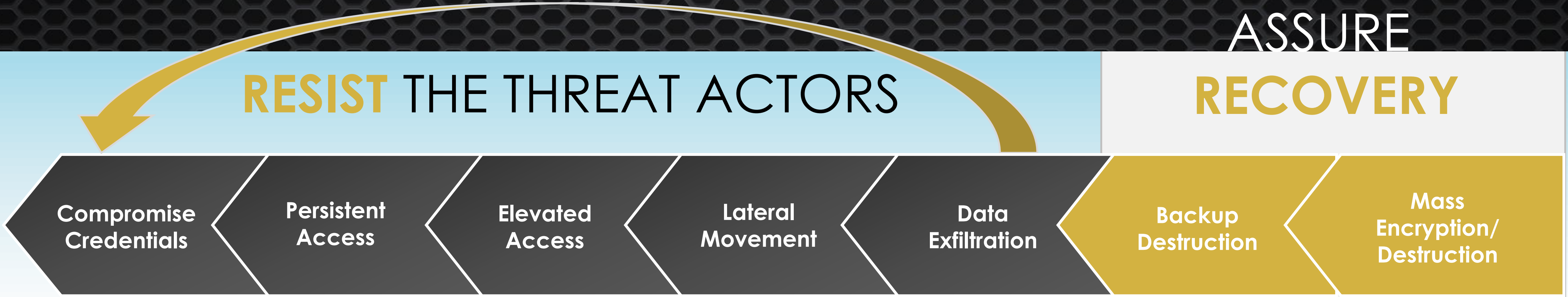
Do you have sufficient storage to support forensics, decryption, and protection?

Transfer

Data, snapshots, and systems may be stored in multiple locations.

HARDEN IN REVERSE: Assured Recovery

FENIX24



ASSURE

RESIST THE THREAT ACTORS

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.

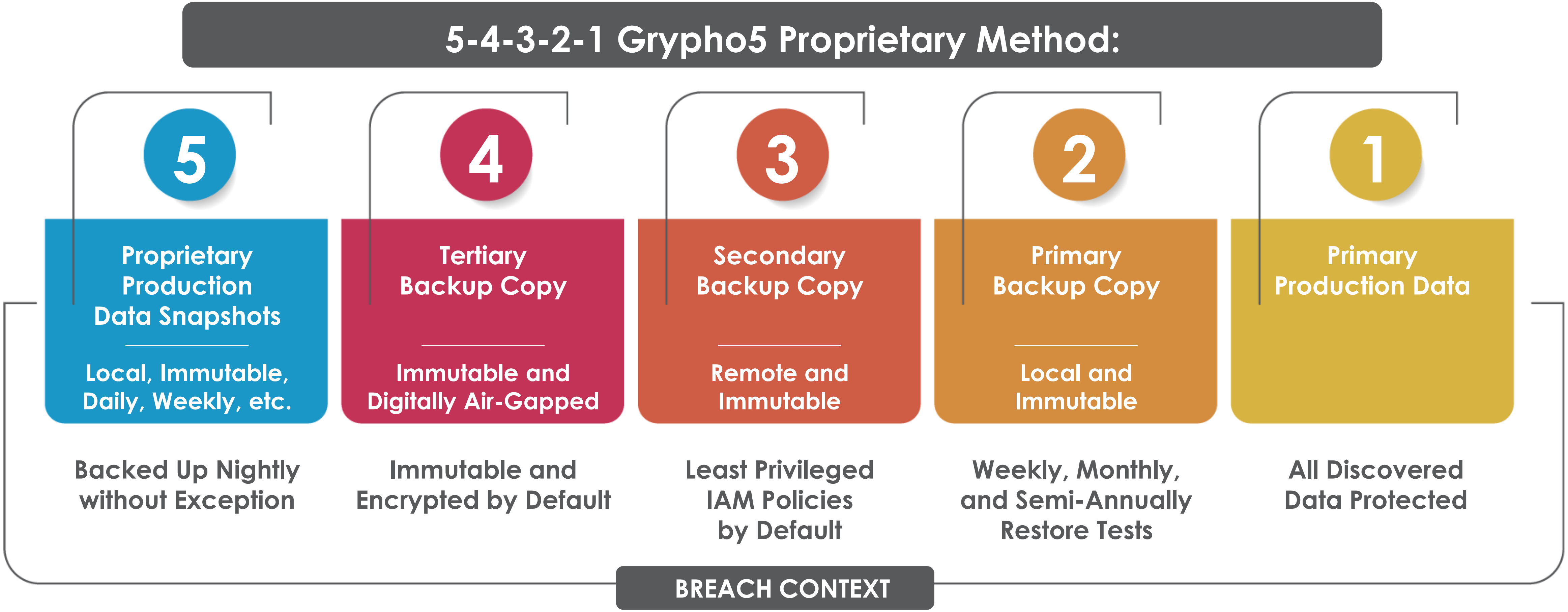
Mass Encryption/ Destruction

- 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.

Modern Defense Strategies

- Zero-trust architecture
- Network segmentation and blast radius containment
- Vulnerability management and patch prioritization
- Integrated business continuity and disaster recovery plans
- Supply chain and third-party risk management
- Red/Blue/Purple teaming; tabletop exercises
- Continuous user education and phishing resistance
- Embedding resilience into organizational DNA — *it's not just IT's problem*
- Immutable, offline backups and recovery readiness

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

WHAT TO DO NOW: Actions You Can Take

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.