CU LEADERSHIP CONVENTION

DISCOVER.
EXPERIENCE.
GROW.

FENIX24®

Threat Actor Trends and Your Most Important Security Controls

Heath Renfrow
Co-Founder & Chief Information Security Officer (CISO)
Fenix24

CU LEADERSHIP CONVENTION DISCOVER. EXPERIENCE. GROW.

Heath Renfrow
Co-Founder & Chief Information Security Officer (CISO)
Fenix24

Heath Renfrow is Co-Founder and CISO of Fenix24 (a Conversant Group company), an industry-leading cyber disaster recovery and restoration company battling threat actors as *The World's First Civilian Cybersecurity Force*. Heath has more than two decades of experience as a high-level information security specialist, much of it as CISO in the United States Department of Defense, where he tackled some of the nation's most significant cyber challenges.

FENIX24

CU LEADERSHIP CONVENTION DISCOVER. EXPERIENCE. GROW.

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 TAs.

Athena7 constantly assesses the tools, processes, and policies organizations are currently using to successfully protect against cyberattacks.

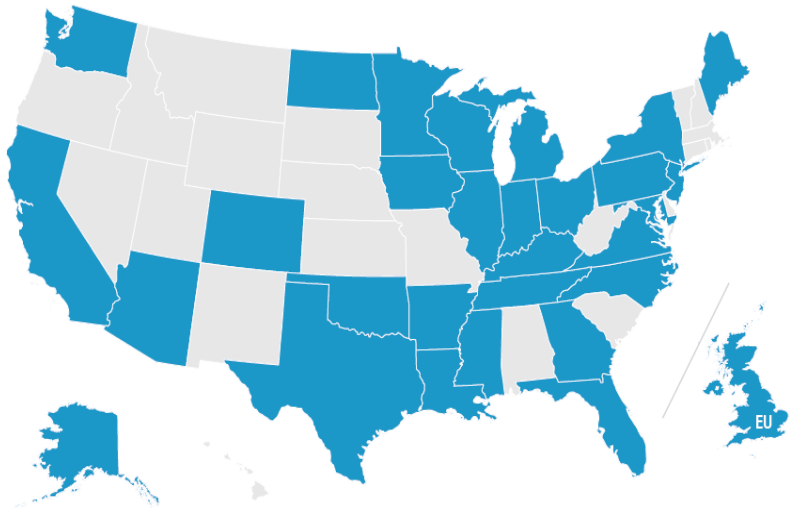
Grypho5 leverages data from both current TA tactics and proven cyber tools and processes to offer the most comprehensive and evolving protection.

Argos99 is an automated software platform that gives businesses unmatched visibility into their assets, critical dependencies, and policies.

Fenix24's Global Footprint

Fenix24 has technical resources in ~30 U.S. states and throughout the U.K.—and served customers in ~40 countries

Technical Experts Located Throughout the U.S. and EU



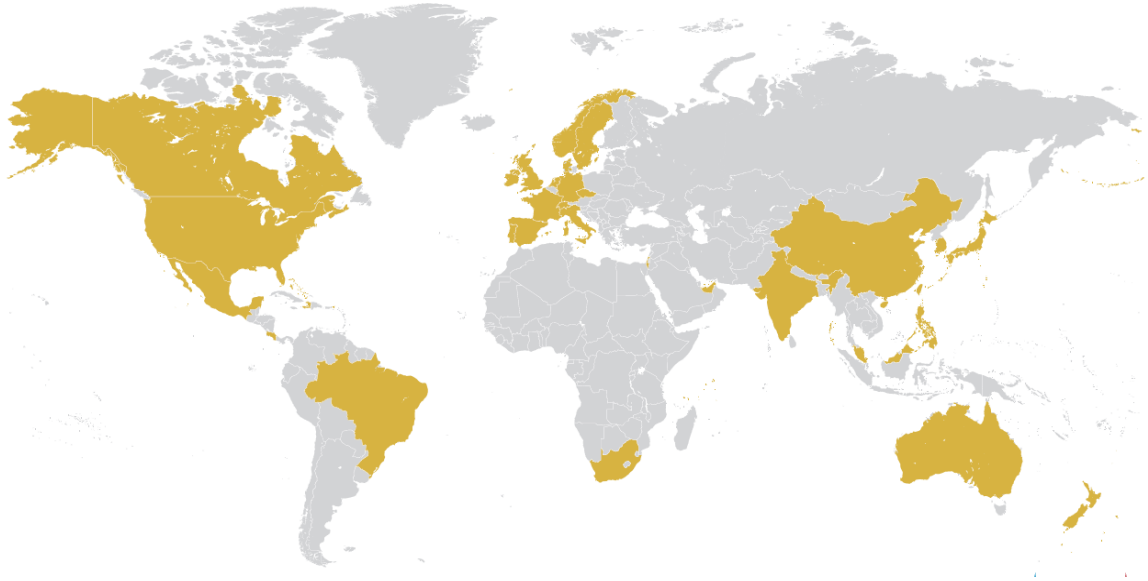
THE FENIX24 ADVANTAGE

COVERAGE. Worldwide, multi-state, and remote access coverage to ensure the fastest response for security incidents.

SPEED & EXPERTISE. A unique methodology: we partner with DFIR companies, law firms, cyber insurers, and internal teams immediately following incidents to determine the fastest path to recovery (up to 50% faster than traditional approaches).

EFFICIENCY. We complete projects significantly under budget 71% of the time* due to our software, automation, and process efficiencies.

Countries We've Served



Credit Union Breaches in the News

- August 2024: California-based Patelco Credit Union breached
- Breach impacts 726,000 customers and employees
- RansomHub ransomware group steals databases
- Threat actor auctions data containing personal information when financial settlement cannot be reached
- Backups rendered useless; Recovery Time Objectives shattered

Credit Union Breaches in the News

August 2024: First Commonwealth Credit Union breached

Breach impacts 99,000 customers

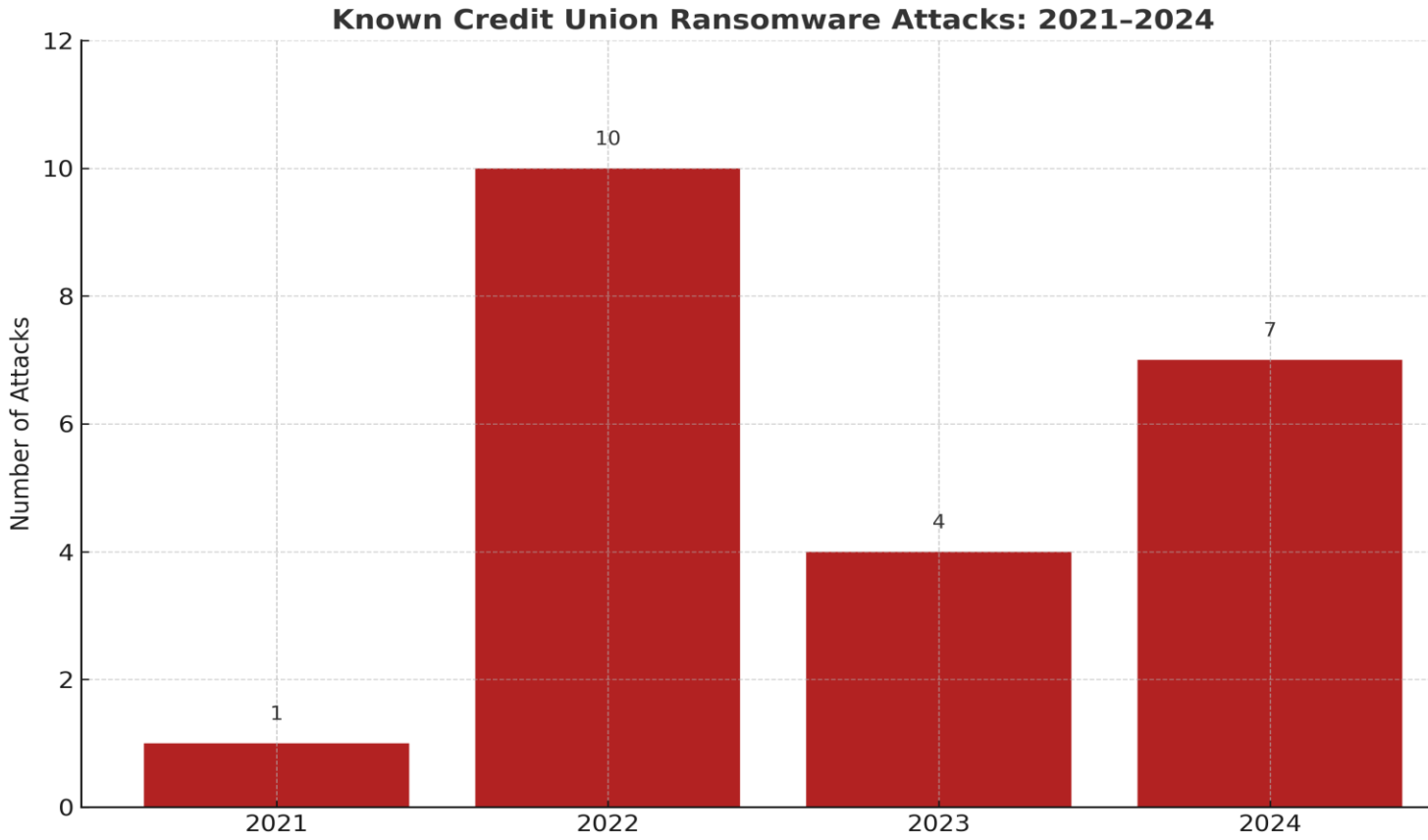
Meow ransomware claims responsibility for attack

Threat actor steals over 400GB of data, including contracts, accounting records, bank files, financial details, and tax info

Breach is believed to have occured on June 26, 2024, but consumers not notified until August 2

Credit Union Known Attacks

National Credit Union Association reports CUs suffer 892 cyber incidents between September 2023 and May 2024.



Examples: 2021: Clinchfield Federal CU; 2022: Lake Charles Telco CU, Mid-Hudson Valley FCU, Unknown CU Breaches (7); 2023: SRP Federal CU, Lafayette FCU, Cross Valley
DataHEALTH CU Clients; 2024: Patelco CU, FedComp Supply Chain, Multiple NCUA-Reported CU Events (5)

What is Ransomware Backup and Resiliency Assessment (RBRA)?

RBRA is a first-of-its-kind, intelligence-led evaluation born from real-world incident response experience.

Fenix24 has reverse engineered more than 200 of the world's most devastating cyberattacks, using firsthand knowledge to build this specialized assessment. It's not theoretical. It's what actually happens when ransomware hits.

What the RBRA Delivers

Backup Survivability Testing Against Ransomware: Not just disaster recovery, but destructive attack simulation

Credential Compromise Risk Assessment: Understand how identity exposure impacts recovery

Critical Business Application Survivability Heat Map: Know which apps will recover, and which won't

Real-Time RTO Analysis & Recovery Recommendations: Stop guessing & start planning with hard data

Backup Solution Evaluation: Insights into what's truly restorable, and what's just noise

Runtime Objectives (RTOs) for Credit Union Cybersecurity: Ensuring Operational Resilience and Data Protection

What are RTOs?

- RTOs refer to the expected system behavior and security posture during live operations.
- RTOs are essential for maintaining trust, uptime, and compliance.
- RTOs focus on real-time monitoring, threat detection, and resilience.

Why RTOs Matter to CUs

- Handles sensitive member financial data.
- Must comply with regulations (NCUA, GLBA).
- High expectations for availability, integrity, and confidentiality.
- Downtime or breaches damage reputation and trust.

Key Runtime Objectives

Continuous Monitoring

- Real-time visibility into systems, networks, and transactions
- Detect anomalies, intrusions, and policy violations

Threat Detection & Response

- Runtime behavior analysis (e.g. EDR)
- Immediate isolation or mitigation of threats

Secure Application Execution

- Validate runtime permissions, control access, sandbox apps
- Prevent execution of unauthorized code

Best Practices for Credit Unions

- Regularly update runtime security policies
- Conduct runtime incident drills
- Integrate monitoring tools with fraud detection systems
- Train staff on recognizing and responding to live threats

Console Segmentation and Readiness — By the Numbers

Fenix24's Athena7 battalion found, that of assessed organizations:

- 73% have critical consoles assessable from user segments
- 100% have critical consoles co-joined to production AD
- 55% had non-existent or non-restricted MFA
- 45% had access to IPMI/iLO/iDRAC
- 65% had same consoles AD joined
- 87% had no IP restrictions on publicly accessible systems

Console Segmentation and Readiness: Risks Abound

Athena7 assessments showed that nearly all had these risks…

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

Vendor "Immutability" Is Not Enough

IMMUTABILITY: A security principle that states the data in storage cannot be changed, encrypted, or deleted by any means. Even if a threat actor were able to gain access to the data, they would not be able to modify or destroy it because there are no IT administrative technical overrides to the retention lock.

In Fenix24's (2000+) actual breach experiences, of data thought to be immutable…

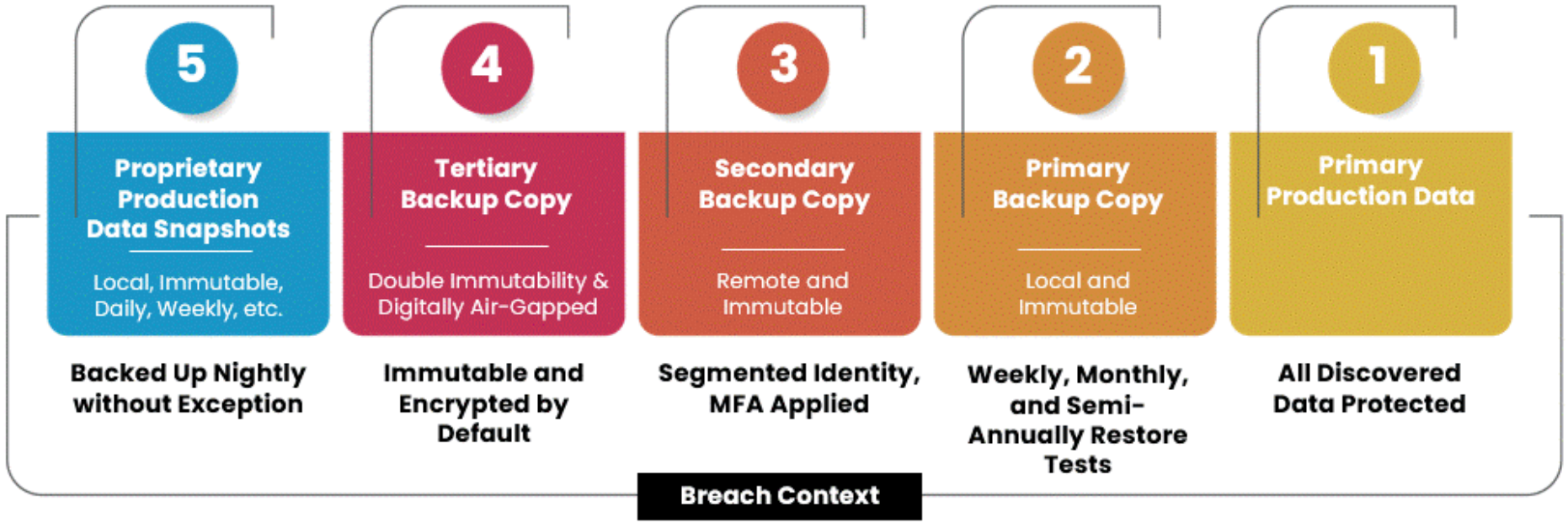
84%

DOES NOT SURVIVE!

If threat actors gain access, they can change settings and destroy / encrypt data believed to be "immutable."

Survivability, 5-4-3-2-1

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



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 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

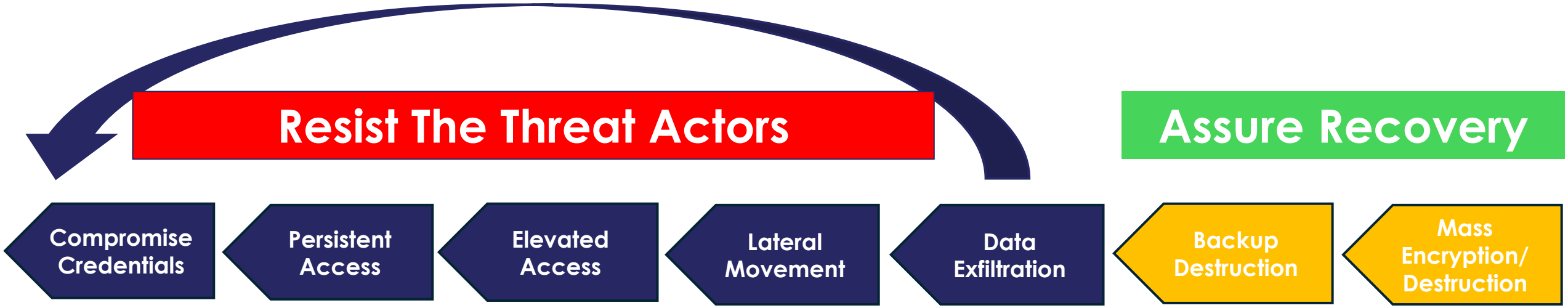
Athena7 Intel:

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

Harden in Reverse: Assured Recovery



WHAT TO DO NOW: Actions Credit Unions Can Take

- Assess the CU's recovery capabilities against breach contact (Athena7).
- Establish retainer with a restoration company (Fenix24).
- Align leadership to mass recovery realities – point and time (Athena7).
- Prioritize mass recovery. Mass destruction most likely form of disaster for CUs.
- Establish a recovery zone where mass restoration can be safely tested and RTO measured (Grypho5).
- Regularly test and harden recovery capabilities to establish predictable recovery timelines (Grypho5).
- Complicate and obfuscate critical console administrative identity (Grypho5).