Recovery Over Resistance: A New Paradigm In Cyber Defense

Global Resilience Federation Summit on Security & Third-Party Risk

John Anthony Smith, Founder & CSO, Fenix24

JOHN ANTHONY SMITH

- Founder & Chief Security Officer of Fenix24 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—approaching 30 years.
    - 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.

John Anthony Smith
Founder &
Chief Security Officer

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

FENIX24®

Recovery & Restoration

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

ATHENA7®

Strategy & Execution

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

GRYPHO5®

Managed Protection

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™

Asset & Resiliency Software

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

1000+ 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 hundreds of organizations recover from some of the world's most devastating attacks, with a minimum of operational downtime, no other service provider comes close to our capabilities. For that matter, recovery is the new defense.

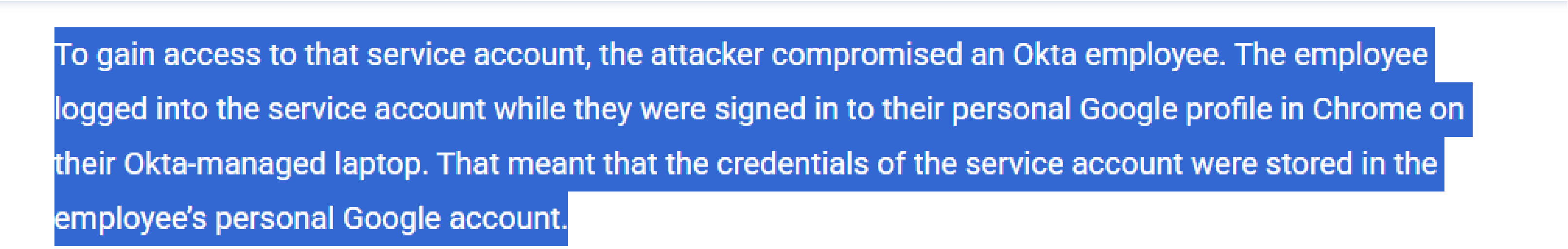
Operating as the "World's First Civilian Cybersecurity Force", Fenix24 is leading a new paradigm in cybersecurity by emphasizing the ability to recover from a breach over the capacity to prevent one. In fact, Fenix24 offers its customers an assurance of recovery, while hardening cyber defenses through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

What Is Breach Context

BREACH CONTEXT: Infrastructure and security control configuration alignment to breach realities. Said differently, comparing threat actor (“TA”) 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.

As an example, OKTA, a leading identity provider, experienced a breach caused by allowing staff to use Gmail (and Chrome) from corporate issued devices — what can we learn from Okta’s breach — many things…

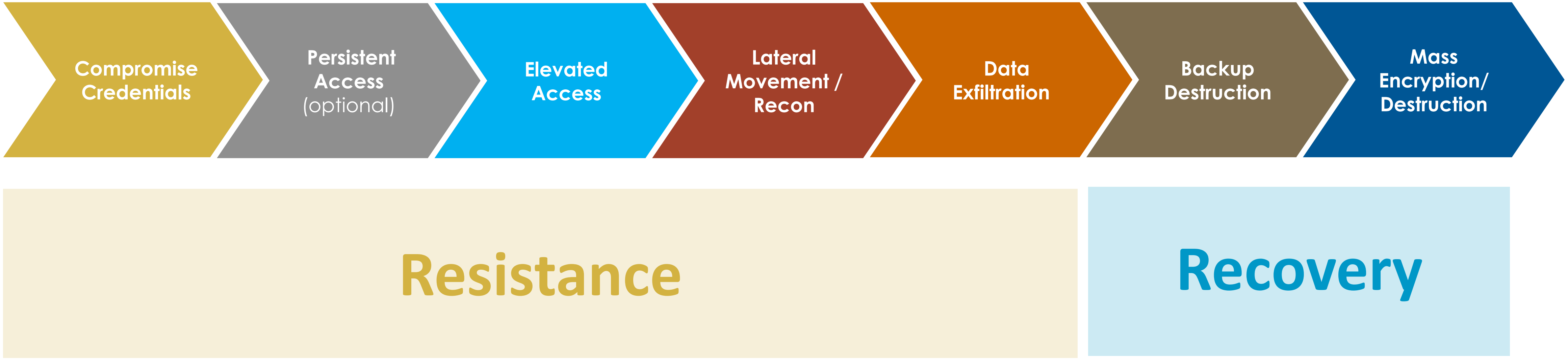


To gain access to that service account, the attacker compromised an Okta employee. The employee logged into the service account while they were signed in to their personal Google profile in Chrome on their Okta-managed laptop. That meant that the credentials of the service account were stored in the employee’s personal Google account.

https://www.threatdown.com/blog/okta-breach-happened-after-employee-logged-into-personal-google-account/

The 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 tranches of the breach patten "Resistance." 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 tranches, Backup Destruction & Mass Destruction, "Recovery Tranches".



Compromise Credentials

Persistent Access (optional)

Elevated Access

Lateral Movement / Recon

Data Exfiltration

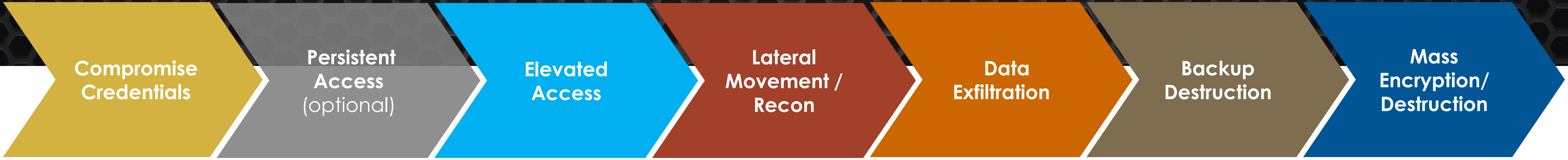
Backup Destruction

Mass Encryption/ Destruction

Resistance

Recovery

How Public OKTA Details Fit into Pattern



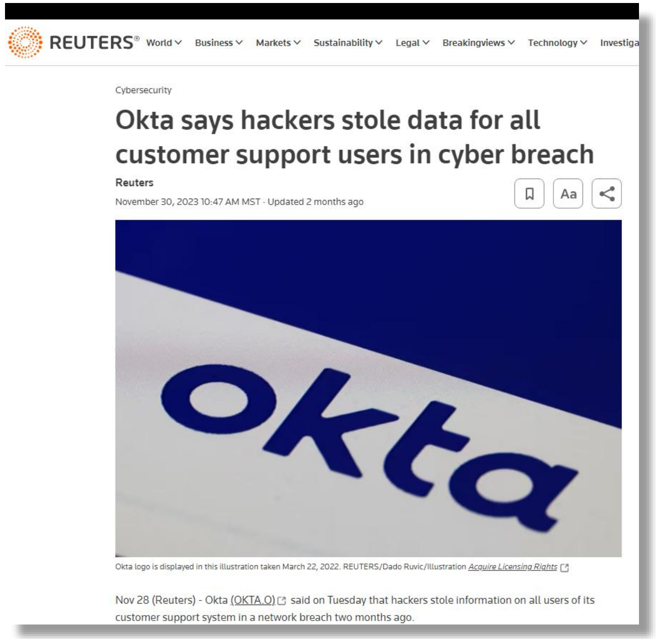
- Password caching allowed in browsers.
- Accounts with no MFA requirement for access to publicly exposed SaaS and remote access platforms.
- No geo-blocking, impossible travel, or malicious logon detection enabled in OKTA for at least some accounts.
- Chrome browser is in use & personal e-mail access is not blocked.
- Personal webmail is not blocked: **cached cred synch is not blocked in browsers.**
- Device & network trust not required for SaaS app access—within OKTA and SaaS apps.
- SaaS, cloud-based tools are accessible off the network (VPN/LAN).

- SaaS apps can be accessed without VPN and corporate device.
- Always-on, full VPN not required.
- SOC minimally involved in kill chain.
- Weak OKTA configuration: privileged accounts with no MFA or other restriction.

- Users permitted to cache credentials in browser: Cached passwords used in the environment.
- Browsers are not restricted from synchronizing credentials to public cloud services.
- Service accounts not restricted to specific purpose from specific location/device.
- SaaS apps have no native IP restriction---ServiceNow does allow this function to be configured.

- MFA is not required for administrative function via PowerShell, WMI, MMC, RDP, and Windows Remote Management.
- MFA is not required while on LAN/VPN.
- Administrative access permitted from public networks.

- VPN split tunnel is used.
- SOC minimally involved in evaluating malicious, anomalous download activities from SaaS tools
- Access to Org data & SaaS apps is not restricted to corporate devices & networks.



Cybersecurity

Okta says hackers stole data for all customer support users in cyber breach

Reuters

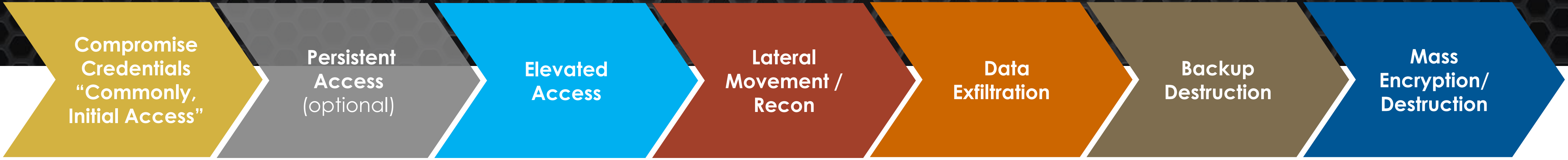
November 30, 2023 10:47 AM MST · Updated 2 months ago

Okta logo is displayed in this illustration taken March 22, 2022. REUTERS/Dado Ruvic/Illustration *Acquire Licensing Rights*

Nov 28 (Reuters) - Okta (OKTA.O) said on Tuesday that hackers stole information on all users of its customer support system in a network breach two months ago.

https://www.securityweek.com/okta-hack-blamed-on-employee-using-personal-google-account-on-company-laptop/

Why Breach Context & Pattern Matter



Compromise Credentials "Commonly, Initial Access"

Persistent Access (optional)

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 attackers end game, not 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.

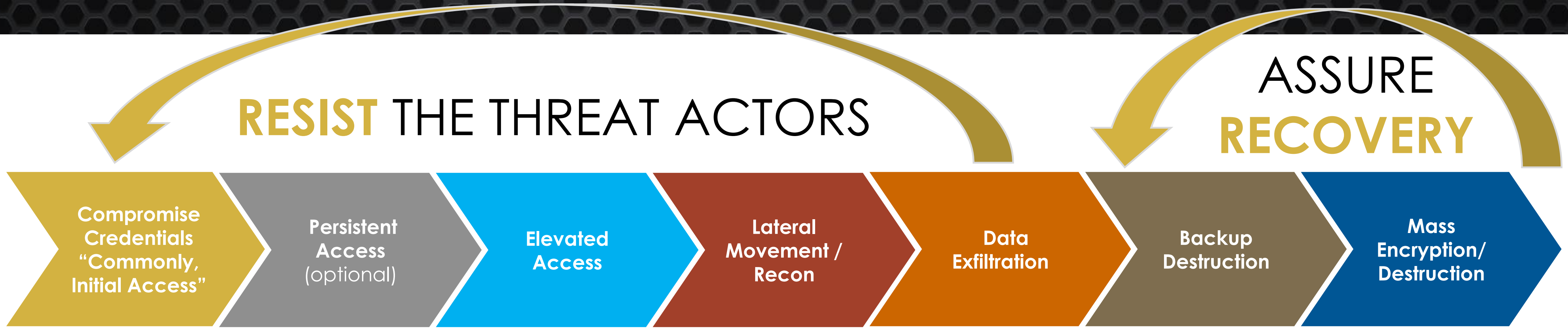
- Despite organizations' best investment & effort, resistance controls and infrastructure are largely orchestrated poorly. There are many reasons for this, but the foundational reason is the LACK of BREACH CONTEXT!

Lack of Breach Context begats destruction.

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

Buy Outcomes, not Products



RESIST THE THREAT ACTORS

ASSURE RECOVERY

Compromise Credentials “Commonly, Initial Access”

Persistent Access (optional)

Elevated Access

Lateral Movement / Recon

Data Exfiltration

Backup Destruction

Mass Encryption/ Destruction

- The entire industry has a “resistance slant,” meaning most investments, emphasis, and understanding are slanted toward the “resistance tranches” of the Breach Pattern.

- Defenders are left to their own best guesses and cyber product vendors suggestions, urgings, and guidance to decide how to resistance harden. Let’s be honest, Microsoft and other vendors are not incentivized to guide clients well — **product vendors are peddling cybersecurity product — not cybersecurity outcomes.**

- Security professionals who commonly talk of resistance methodologies will, commonly, in the same breath say, “It is not a matter of if you will be breached but WHEN…”

- Good resistance hardening will stop lazy TAs and slow down more sophisticated ones, hopefully, to the point of detection before attempted exfiltration or destructive act.

- Assured recovery will ensure that, no matter the TA behavior, the organization CAN recover — and that technical rehydration & recovery is tested, known, understood, and ready (pre-staged). **Assured Recovery is purchasing an OUTCOME, not a product.**

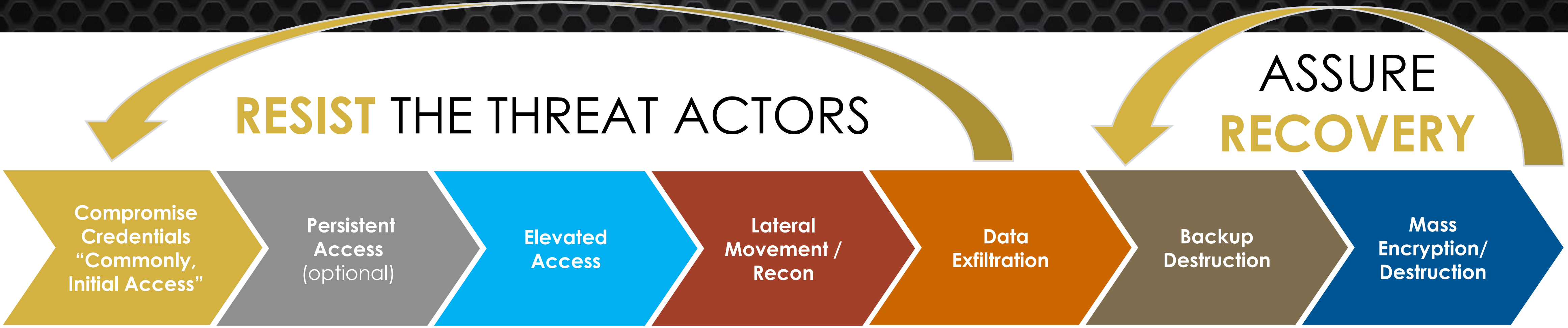
Fenix24 Monthly Update: Items of Interest

- **Compromised Creds**
  - An employee sold his creds to a threat group.
  - A threat actor must commonly only obtain a single user's creds to gain access to VPN, Citrix, AVD, Horizon, etc.
  - VPN is most common point of initial access across all periods; it was the second largest sample in last period.
  - Fileless malware present exfiltrating certificates and credentials using legitimate Cloudflare services.
  - Failure to patch your own software systems within known patches.
  - SonicWall vulnerabilities, overwhelmingly, made up the largest portion of the breaches we worked in last period.
    - **SonicWall backup cloud repository was compromised allowing attackers to target many SonicWall devices.**
  - Outsourced helpdesks are regularly implicated in credential compromise—some more common than others.
  - SMS / phone calls used for MFA.
- **Persistent Access**
  - Threat actors leverage and abuse the reality that ESXi and vCenter do not have EDR installed.
  - Reverse proxy platforms, such as Teleport and Socket, are installed directly on the hosts and vCenter—abusing outbound Internet access from VMWare.
- **Elevated Access**
  - KRBTGT hash obtained and cracked.
  - Forged golden tickets employed to logon as any user.
  - Threat actors are rolling dates forward on Active Directory domain controllers to edit time locked configuration.
  - ESXi / vCenter commonly not logging to SIEM.
  - New VM creation not spawning alerts.

Fenix24 Monthly Update: Items of Interest

- Lateral Movement
  - **Nimble Storage, Cohesity, vCenter, ESXi, & Commvault all easily accessible with production Active Directory domain creds.**
- Backup Destruction
  - Veeam backups have survived due to 3rd party management and **disconnection from Active Directory domain**: 56% of Veeam backups still destroyed.
  - Cohesity backups destroyed due to **disabled data lock and improper hardening.**
  - Threat actors accessed the Nimble storage via production Active Directory integration and deleted all snaps.
  - Couldn’t locate the backup tapes: while tapes are, by default, immutable if removed from the drive, they too are commonly poorly managed.
  - **Virtualized backup infrastructure is destroyed.**
  - **SonicWall cloud backup compromise should come as a wakeup call to all orgs storing backups in “shared” cloud backup platforms.**
- Mass Destruction
  - vCenter & Nimble Storage joined to production Active Directory.
  - TAs have commonly given incorrect decryption keys, even after ransoms are paid.
  - Customers commonly do not understand their environments:
    - One engagement we were told there were six (6) vCenter appliances, and we discovered sixty plus (60+).
    - We were told there were four (4) Active Directory domains, and we located one hundred plus (100+) domains.

When, Not If, An Attack Will Occur



- Proper resistance should be predicated on an assured recovery — **counter cultural paradigm.**
- Recovery can only be assured through constant orchestration and reorchestration 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 a 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.

Mass Destruction
From the Front Lines of Assessment

- **Largely no one is properly protecting their systems from Mass Destruction.**

- **Mass Destruction disruption requires complication and obfuscation of IT access to certain systems and credentials. IT must complicate their own access before complicating user access — counter cultural paradigm.**

- **IT should not be able to access directly or indirectly, with a production AD ("Identity Plane") credential, any critical console that could be leveraged by a TA for destruction.**

- **Further, IT should not be able to open or log into any critical console from the public Internet or user segments.**

- **EDR/AV platforms can, and are, used to orchestrate destruction; yet most companies cojoin to production AD, expose to the public Internet, and do not IP restrict access.**

- **Workday and other HR platforms, in Enterprise, leverage workflow automation products like SailPoint; yet the HR systems are accessible publicly and do not require workflow step review — users are created, disabled, and deleted without a review step. Workflow automation is only as secure as the tool that spawns the workflow!**

- **Mass destruction common causes:**

    - **Critical consoles are cojoined with the organization's production identity planes and/or the identity plane employed is accessible from user segments.**
    - **Critical console credentials, including break-glass accounts, are stored in password vaulting mechanisms, publicly exposed, accessible from user segments, and/or leveraging production identity plane credentials.**
    - **Critical consoles are accessible from user segments and the public internet.**
        - These consoles are not natively IP restricted to a specific administrative segment.
        - The identity plane is not IP restricted to a specific administrative segment.
    - **MFA methodologies are weak, not present, or common to production identity plane methods.**

Mass Destruction
From the Front Lines of Assessment

Backup Destruction → Mass Encryption/ Destruction

Global Financial

- CyberArk transitioning from local accounts w/o MFA to production AD for authentication—credentials are likely cached in browsers.
- Critical consoles, such as AWS, NetApp, vCenter, and CrowdStrike, are likely all largely stored with CyberArk
- No reviewed S3 buckets were marked for proper immutability.
- vCenter, NetBackup, Hitachi, Zscaler, NetApp, iLO (and likely CIMC), CyberArk,, & Cisco UCS Manager are accessible from user segments via production AD credentials.
- vCenter, NetBackup, NetApp, Hitachi, Cisco UCS Manager, ILO (and likely CIMC), Zscaler, CrowdStrike, & CyberArk can be accessed administratively from VPN & Citrix.
- No IP restriction on CrowdStrike console: compromise could lead to mass destruction.
- Hitachi NAS is virtualized and would likely be destroyed by TA VMDK encryption.
- CrowdStrike Real-Time-Response re-authentication for critical actions is turned off.

Hospital

- Secret Server uses production AD for credentialing.
- Critical consoles, such as Data Domain, Networker, Isilon, Extreme IO, Unity, Vmax, Nutanix, Avamar, VxRail, and vCenter, have sensitive credentials in Secret Server.
- vCenter, Networker, and Avamar are domain joined.
- Hypervisor, storage, and backup tools' accessible from user segments and with domain credentials without MFA .
- No separate VLAN, jump box, or ACL to limit access to sensitive infrastructure consoles (with exception of some items like RDP and SSH).
- No IP restrictions on CrowdStrike Console; compromise could lead to mass destruction.
- CrowdStrike console does not require MFA.
- Access to CrowdStrike console available to cloud native CrowdStrike accounts.
- SailPoint could potentially be used to create malicious credentials, or disable accounts

Pharmaceutical

- Veeam, vCenter, iLO, CrowdStrike, ESXi, AWS, Azure, NetApp, and Bitwarden are accessible from user segments.
- No IP restrictions on CrowdStrike Console.
- vCenter, ESXi, Veeam, Azure, & AWS are domain joined.
- Hypervisor & backup tools' accessible from user segments and with domain credentials with no MFA.
- No separate VLAN, jump box, or ACL to limit access to sensitive infrastructure consoles.

Insurance

- CyberArk, vCenter, NetApp, *another storage, Cohesity, Data Domain, Power Max, CrowdStrike, Azure, Zerto, and AWS are all administratively accessible from user segments.
- CyberArk, vCenter, *another storage, NetApp, Cohesity, Data Domain, Power Max, CrowdStrike, Azure, Zerto, and AWS are all administratively accessible with production AD credentials.
- iLO/iDRAC/IPMI (DD/Cohesity) accessible from user segments and with AD credentials.
- Highly privileged accounts are stored in CyberArk accessible from user segments and daily driver accounts.
- No separate VLAN, jump box, or ACLs to limit access to sensitive consoles.
- No IP restriction in CrowdStrike, AWS, & Azure—accessible from public Internet and daily driver accounts.
- Zscaler admin console exposed publicly with no MFA requirement and daily driver access.

Private Equity

- Secret Server, CyberArk, vCenter, *storage, Carbon Black, Pure, Rubrik, iLO, Synergy, Zerto, and Nasuni are all administratively accessible from user segments.
- Secret Server, CyberArk, Carbon Black, AWS, Druva, vCenter, *storage, Rubrik, *another backup tool, iLO, CrowdStrike, Synergy, Pure, and Nasuni are all administratively accessible with production AD credentials.
- Daily driver accounts are leveraged for access to critical consoles: Secret Server, CyberArk, vCenter, *another backup tool, *storage, Rubrik, etc.
- Critical console (*storage, Rubrik, Pure, etc.) creds are stored in Secret Server and CyberArk; these vaults are commonly not properly hardened.
- No separate VLAN, jump box, or ACLs to limit access to sensitive consoles (including Rubrik)---other than AWS.
- CrowdStrike EDR public console not IP restricted and accessible from prod AD creds.
- Secret Server accessible with weak MFA.
- Workday is accessible externally w/ AD creds & allowed to create AD/Okta users.

Mass Destruction Critical Consoles

There are 7 classes of "critical consoles" that must be in a segmented, dedicated, Breach Context-hardened identity plane:

1. Backup Management Consoles & Servers
2. Storage Management Consoles
3. Hypervisor Management Consoles (VMWare, Nutanix, AHV, XenServer, KVM, Proxmox, etc.)
4. Cloud Management Consoles (GCP, AWS, Azure, OCI)
5. EDR/AV Cloud and On-premises Management Consoles (CrowdStrike, McAfee, Symantec, CarbonBlack, SentinelOne, etc.)
6. IPMI/iDRAC/iLO/IP based KVM Management Consoles
7. And IT Password Vaults (CyberArk, Secret Server, 1Password, etc.)

Segmenting critical consoles into segmented identity will eliminate 60% or so of the common reasons that TAs can "simply" mass destroy an environment.

Couple console identity segmentation with critical console access network segmentation from public and user segments — and roughly ~80% of the common causes of "simple mass destruction" can be eliminated.

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

Backup Destruction
From the Front Lines of Assessment

- We meet customers on their worst day (Recovery).

- Despite organizations best efforts, on assessment and recovery, we find that organizations are woefully unprepared and largely do not have backup capabilities that will survive. 84% of time the backups, aka recovery capability, do not survive the TAs attacks. From assessment, 86% have no immutable backup copies.

- Backup destruction & long recovery common causes:

  - Mass recovery was never considered & excess mass recovery capacity was never assured.
  - vCenter, backup technologies, cloud platforms, and storage are cojoined to production Active Directory.
  - Only a single backup copy exists.
  - 75%+ do not have all known critical data backed up.
  - Storage snaps were not taken, storage snap retention was too short, or all volumes were not snapped.
  - Backup infrastructure was virtualized within production Azure, Hyper-V, vCenter, or AWS
  - Storage, hypervisor, and cloud platforms are administratively assessable publicly and/or user segments.
  - No backup copies were maintained in a truly (meaning product vendors misguide orgs) immutable (survivable) fashion.
  - Cloud repositories were the only backup copy that survived.
  - Backup retention was too short.
  - DRAAS & DR technologies are assumed to be survivable for mass destruction.
  - Backup & storage infrastructure creds stored in password vaulting methods—usually in prod AD.

Backup Destruction
From the Front Lines of Assessment

Backup Destruction

Mass Encryption/ Destruction

Global Financial

- Not using 5-4-3-2-1 backup model.
- No immutable backups or snapshots in the environment, except tapes out of library: tapes remain in library every 30 days.
- MFA is not applied to the backup systems.
- NetBackup console directly accessible without jump box & MFA with AD creds (Policy vs. Practice).
- Quest used for AD snapshots but does not have immutability features built in.
- VMW SRM present for replication/DR orchestration between DCs.
- MS365 & ServiceNow not backed up.
- NetApp SSH access enabled, multi approval feature missing, Snap Lock not enabled, and firmware years old.
- All backups and storage are AD joined.
- AWS data is not protected with similar level as on-premise.
- Block storage volumes are not immutably snapped; NAS devices are snapped—but not immutably.
- Production storage highly used, and mass recovery excess capacity is not maintained.
- Cisco UCS 3260 localized backups (on disk) are not immutable.
- Tapes that remain in tape library could be erased/manipulated by TA.
- Mass destruction recovery time likely very long; fastest recovery is always back to source from disk.

Hospital

- Not using 5-4-3-2-1 backup model.
- Backup Admin accounts stored in SS.
- Backup consoles are available from user segments.
- Primary data domain copies of backups, before copied to CyberVault, are not immutable.
- There are no immutable snapshots in the environment.
- Not all data/servers are backed up.
- Data selected by exception for backup, not default.
- Some backups are immutable.
- Hyperconverged infrastructure complicates mass recovery.
- Avamar, Networker, and vCenter domain joined without MFA.
- Vmax, Nutanix, VxRail, and Isilon do not have methods for TPR and immutability enabled.
- All storage volumes are not taking snapshots
- Lack of excess compute may complicate mass recovery.
- Recovery steps are complex with many hops. There are lots of ways recovery can fail.
- Office 365 and workday are not backed up.
- GitHub may not be being backed up – location of Terraform templates.
- Mass destruction recovery time likely very long; fastest recovery is always back to source.

Pharmaceutical

- Most backups are not immutable.
- Not using 5-4-3-2-1 backup model.
- Maintain only a single, non-immutable backup copy.
- The remote, immutable backup copies are 30 days old.
- Backup consoles/devices are accessible from user segments and domain credentials.
- MFA is not applied to the backups.
- All production data/systems are not being backed up.
- NetApp snapshots are not immutable, credentials stored in Bitwarden, and Bitwarden configuration is weak.
- Backup of SaaS providers not under the control of the Org---Workday.
- Office 365 backups are not immutable.
- Mass recovery capability is not tested: Mass destruction recovery time likely very long.
- AWS backups reside in same tenant.
- AWS S3 not backed up.

Insurance

- Data Domain is in domain, no immutability, and no MFA.
- Zerto administration uses AD creds: target volumes not snapped.
- Backup & storage accounts in CyberArk & AD.
- Dev/Non-prod not backed up.
- Cohesity is AD integrated, quorum not enabled, SSH not blocked, and IPMI enabled and accessible.
- Cohesity backups are not replicated, immutably, outside of Cohesity provided storage: tertiary, isolated cloud copy recommended.
- Backup/storage accessible creds likely present in KeePass.
- All production/DR related volumes not snapped, and the snaps that do exist are not immutable.
- No snaps on Infinidat, and snaps on other storage only done upon request: No systematic snapping.
- Azure Recover Services Vault has no copies outside tenant and no immutability.
- AWS data only backed up inside tenant with no immutability.
- Scripted locking of S3 backup objects can be unlocked by a TA.
- Mass recovery capability not tested, and excess recovery capacity not assured.
- Exchange can easily be destroyed by TA, and those systems are not backed up.
- SaaS tools, such as Salesforce, ServiceNow, & M365, are not backed up by Org controlled tools.
- Data Domain backups not immutable and accessible from IPMI, SSH, and production AD creds.
- GitHub & Azure DevOps are not backed up by Org controlled tools.

Private Equity

- Endpoints are backed up with Druva; Druva leverages TPR as immutability. Druva could be manipulated by SIM swapping.
- AWS Backup cloud-based S3 backup copies are not immutable—versioning only.
- Scripted locking of S3 backup objects can be unlocked by a TA—like the locking method.
- Zerto replication is destroyable because replica targets are connected to domain.
- AWS Backup restore points can be deleted.
- "Backup by Request" methodology In use: approximately 50% of prod data not backed up.
- Non-backed up data is replicated via Zerto to opposing datacenter; however, underlying storage, hypervisor, and Zerto itself are at risk.
- Rubrik TPR (Quorum) is enabled; however, configuration change does not require multiple approvals---thus, effectively no immutability.
- FINRA lock is not present or enabled within Rubrik.
- Cloud assets within AWS & Azure, including cloud backups, could be destroyed by a TA.
- Rubrik IPMI is physically connected, and the switch port is not disabled.
- Rubrik is joined to prod AD.
- All prod volumes on all storage platforms are not snapped; however, Pure does snap volumes.
- Pure snapshots are not immutable, because protection groups not locked.
- Nasuni (s3, non-immutable) data is subject to destruction.
- AWS/Azure production and backup data coexist within the same AWS tenant.
- Backup and storage tooling accessible from user and server segments.
- Backup and storage platforms connected to AD with privileged creds in SS.
- AWS S3 and Azure Blobs are not being backed up; however, do contain critical data.
- DevOps and SaaS apps, such as ServiceNow, MS365, Salesforce, ADP, and Workday, are not being backed up by controlled tools.
- Rubrik Azure Blob target is not immutable.
- Rubrik admin creds don't require MFA.

Global Financial: Survivability Heat Map

Critical Business Applications

Recovery Likelihood	Production	Primary	Secondary	Tertiary	Snaps
App1	On Prem	NetBackup	NB Tape Library	Offsite Tape	None
App2	On Prem	NetBackup	NB Tape Library	Offsite Tape	None
App3	On Prem	NetBackup	NB Tape Library	Offsite Tape	None
App4	On Prem	NetBackup	NB Tape Library	Offsite Tape	None
App5	On Prem	NetBackup	NB Tape Library	Offsite Tape	None
App6	On Prem	NetBackup	NB Tape Library	Offsite Tape	None
App7	On Prem	NetBackup	NB Tape Library	Offsite Tape	None
App8	On Prem	NetBackup	NB Tape Library	Offsite Tape	None
App9	On Prem	NetBackup	NB Tape Library	Offsite Tape	None
App10	On Prem	NetBackup	NB Tape Library	Offsite Tape	None
App11	On Prem	NetBackup	NB Tape Library	Offsite Tape	None
App12	On Prem	NetBackup	NB Tape Library	Offsite Tape	None
App13	On Prem	NetBackup	NB Tape Library	Offsite Tape	None
App14	On Prem	NetBackup	NB Tape Library	Offsite Tape	None
App15	On Prem	NetBackup	NB Tape Library	Offsite Tape	None
App16	On Prem	NetBackup	NB Tape Library	Offsite Tape	None
App17	On Prem	NetBackup	NB Tape Library	Offsite Tape	None
App18	On Prem	NetBackup	NB Tape Library	Offsite Tape	None
App19	On Prem	NetBackup	NB Tape Library	Offsite Tape	None
App20	On Prem	NetBackup	NB Tape Library	Offsite Tape	None
App21	On Prem	NetBackup	NB Tape Library	Offsite Tape	None
App22	SaaS	Unknown	Unknown	None	Unknown

Enterprise Applications

Recovery Likelihood	Production	Primary	Secondary	Tertiary	Snaps
App23	On prem	NetBackup	NB Tape Library	Offsite Tape	Unknown
ServiceNow	SaaS	Unknown	Unknown	None	Unknown
Proofpoint	SaaS	Unknown	Unknown	None	Unknown
App24	SaaS	Unknown	Unknown	None	Unknown
RSA SecurID / Duo	On prem	NetBackup	NB Tape Library	Offsite Tape	None
ADFS	On prem	NetBackup	NB Tape Library	Offsite Tape	None
Duo	SaaS	Unknown	Unknown	None	Unknown
M365	SaaS	Unknown	Unknown	None	Unknown

Infrastructure

Recovery Likelihood	Production	Primary	Secondary	Tertiary	Snaps
Active Directory	On prem	NetBackup	NB Tape Library	Offsite Tape	None
CyberArk	On prem	NetBackup	NB Tape Library	Offsite Tape	None
CrowdStrike	SaaS	Unknown	Unknown	None	Unknown
Proofpoint	On prem	NetBackup	NB Tape Library	Offsite Tape	None
Firewall Configs	On prem	NetBackup	NB Tape Library	Offsite Tape	None
App25	On prem	NetBackup	NB Tape Library	Offsite Tape	None
Cisco ISE	On prem	NetBackup	NB Tape Library	Offsite Tape	None
DNS	On prem	NetBackup	NB Tape Library	Offsite Tape	None
VPN	On prem	NetBackup	NB Tape Library	Offsite Tape	None
Network Configs	On prem	NetBackup	NB Tape Library	Offsite Tape	None
Zscaler	SaaS	Unknown	Unknown	None	Unknown

- **Red:** Critical Risk
- **Orange:** High Risk
- **Yellow:** Moderate Risk
- **Green** Low Risk
- **None =** No Backup
- **? (Unknown) =** Assume weak controls

Insurance Co: Survivability Heat Map

RBRA Average: 1.9

Critical Business Applications

Recovery Likelihood	Production	Primary	Secondary	Tertiary	Snaps
App1	On Prem	Cohesity*	Cohesity*	Zerto	SAN
App2	On Prem	Cohesity*	Cohesity*	Zerto	SAN
App3	Mainframe	*	*	None	IBM
App4	Cloud	AWS	AWS	None	AWS
App5	On Prem	Cohesity*	Cohesity*	Zerto	SAN
App6	Cloud	AWS	AWS	None	AWS
App7	Cloud	AWS	AWS	None	AWS
App8	On Prem	Cohesity*	Cohesity*	Zerto	SAN
App9	On Prem	Cohesity*	Cohesity*	Zerto	SAN
App10	Cloud	AWS	AWS	None	AWS
App11	On Prem	Cohesity*	Cohesity*	Zerto	SAN
App12	Cloud	AWS	AWS	None	AWS
App13	On Prem	Cohesity*	Cohesity*	Zerto	SAN
App14	Cloud	AWS	AWS	None	AWS
App15	SaaS	Unknown	Unknown	None	Unknown
App16	On Prem	Cohesity*	Cohesity*	Zerto	SAN
App17	Cloud	AWS	AWS	None	SAN
App18	Cloud	AWS	AWS	None	SAN

Enterprise Applications

Recovery Likelihood	Production	Primary	Secondary	Tertiary	Snaps
App19	*	*	*	*	*
App20	*	None	None	None	None
App21	SaaS	Unknown	Unknown	None	Unknown
SCCM (MS Patching)	On Prem	Cohesity*	Cohesity*	Zerto	SAN
CyberArk	On Prem	Cohesity*	Cohesity*	Zerto	Power Max
Proofpoint	SaaS	Unknown	Unknown	None	Unknown
SharePoint	Cloud	None	None	None	None
O365	Cloud	None	None	None	None
Zscaler	SaaS	Unknown	Unknown	None	Unknown

Infrastructure

Recovery Likelihood	Production	Primary	Secondary	Tertiary	Snaps
Active Directory	On Prem	Quest	Cohesity*	Cohesity*	Zerto
Citrix	On Prem	Cohesity*	Cohesity*	Zerto	SAN
Entra ID	SaaS	Unknown	Unknown	None	Unknown
Firewall configs	On Prem	Cohesity*	Cohesity*	Zerto	SAN
Switch config	On Prem	Cohesity*	Cohesity*	Zerto	SAN
OKTA	SaaS	Unknown	Unknown	None	Unknown
Exchange	On Prem	None	None	None	DAG Group
ESXi configurations	On Prem	Cohesity*	Cohesity*	Zerto	SAN
vCenter	On Prem	Cohesity*	Cohesity*	Zerto	SAN

- **Red:** Critical Risk
- **Orange:** High Risk
- **Yellow:** Moderate Risk
- **Green** Low Risk
- **None =** No Backup
- **? (Unknown) =** Assume weak controls

Private Equity: Survivability Heat Map

Critical Business Applications

Recovery Likelihood	Production	Primary	Secondary	Tertiary	Snaps
App1	SaaS	Unknown	Unknown	None	Unknown
App2	On Prem	Rubrik	Rubrik	None	Pure
App3	On Prem	Rubrik	Rubrik	None	Pure
App4	SaaS	Unknown	Unknown	None	Unknown
Salesforce	SaaS	Unknown	Unknown	None	Unknown
Workday Inc.	SaaS	Unknown	Unknown	None	Unknown
App5	SaaS	CLD BKP	Unknown	None	Unknown

Enterprise Applications

Recovery Likelihood	Production	Primary	Secondary	Tertiary	Snaps
AWS IaaS	IaaS	AWS	AWS	None	AWS
Zscaler	SaaS	Rubrik	Rubrik	None	Pure
Wkst. Data and Config	On Prem	Druva	None	Druva	None
App6	SaaS	Unknown	Unknown	None	Unknown
SharePoint	SaaS	CLD BKP	Unknown	None	Unknown
O365	SaaS	CLD BKP	Unknown	None	Unknown
Teams	SaaS	CLD BKP	Unknown	None	Unknown
Box.com	SaaS	CLD BKP	Unknown	None	Unknown

Infrastructure

Recovery Likelihood	Production	Primary	Secondary	Tertiary	Snaps
Active Directory	On Prem	Rubrik	Rubrik	None	Pure
Entra ID	SaaS	Azure	Unknown	None	None
Splunk	SaaS	Unknown	Unknown	None	Unknown
Firewall configs	On Prem	Rubrik	Rubrik	None	Pure
Switch config	On Prem	Rubrik	Rubrik	None	Pure
OKTA	SaaS	CLD BKP	Unknown	None	None
ESXi configurations	On Prem	AWS	None	None	None
vCenter	On Prem	Rubrik	Rubrik	None	Pure

- **Red: Unlikely to Survive**
- **Orange:** High Risk of Not Surviving
- **Yellow:** Moderate Risk
- **Green:** Low Risk
- **None:** No Backup

Decision to Pay by the Numbers

> "The factor with the largest reduction in the probability of paying was the InfoSec community's darling, fully recoverable backups. Only 11% of such victims paid a ransom.
>
> However, the favourite child partially or completely failed 58% of the time, although even partial backups reduced the likelihood of payment.
>
> There were also more surprising results:
>
> - Victims with insurance were slightly less likely to pay.
> - Data exfiltration made victims slightly more likely to pay.
> - Victims with more revenue were slightly more like to pay.
>
> However, the sample size was small enough that these results might have resulted from a statistical fluke at the 5% significance level. By contrast, the effect from fully recoverable backups was significant at the 0.01% level (a very reliable result)."

https://www.linkedin.com/pulse/what-works-cybersecurity-backups-daniel-woods-rrtie/

Attackers Target Backups & EDR

> “One way to get at causality is studying how attacker behavior is impacted by controls.
>
> Evidence that ransomware groups discuss the efficacy of EDR products and invest in EDR bypasses (see last post) supports the idea that EDR works.
>
> We have comparable evidence for backups:
>
> - “96% of ransomware attacks target backups” (Veeam, a backup provider)
> - “94% of organizations hit by ransomware in the past year said that the cybercriminals attempted to compromise their backups during the attack” (Sophos, not a backup provider)
> - “Analysis of incidents shows that in the early stages of a destructive ransomware attack, actors often target backups and infrastructure, deleting or destroying the data stored there” (NCSC)
>
> So clearly backups are making attackers' jobs harder, but we don't know how much harder.”

https://www.linkedin.com/pulse/what-works-cybersecurity-backups-daniel-woods-rrtie/

Woeful Resistance — Lacks Breach Context

Compromise Credentials

- No forced password hygiene.
- Passwords length is too short (8 characters); systems requiring short passwords possess AD cred integration.
- Cred capture likely for all creds/user access to Citrix from non-org devices.
- Device trust: domain, Intune, & certificate not required to allow authentication.
- Okta temporary group allows external IPs to auth to internal apps without MFA.
- Okta for O365 allows weak MFA forms (phone calls + SMS) and is exposed publicly.
- There is a group of apps exposed publicly that use domain creds—some users do not have MFA.
- Vendors are permitted to leverage weak MFA (SMS).
- Authentication tokens are not device pinned.
- RSA components virtualized and could be destroyed by VMDK encryption.
- Okta MFA is not required internally.
- Okta authentication tokens are allowed to live for 12 hours without reauthentication and subject to capture.
- Browser cred caching is permitted on workstations and servers.
- Self-service password reset leverages Google Authenticator.
- User creds can be harvested from personal e-mail and storage services—Chrome/Google, Edge/OneDrive.

Persistent Access

- VPN (AnyConnect) could likely be accessed without a corporate device (creds + MFA).
- No MDM policies to prevent authenticator app backup.
- MFA self-enrollment allowed (for on prem & VPN).
- Unauthorized code execution is not blocked.
- Citrix accessible from non-corporate devices—no device or network trust.
- Weak forms (Google Authenticator & phone calls) of MFA observed on Citrix, & 3rd parties permitted access.
- Remote access platforms are accessible from privileged accounts.
- No stacked blocking of remote access tools, proxies, hacking tools, personal e-mail, etc.
- Always-on, full VPN not used.
- Weak Okta configuration: daily driver accounts used for administration.
- Citrix NetScaler in use and not rigorously patched.
- Alerts not present for VM creation in Azure, AWS, VMWare.

Elevated Access

- Users permitted to cache credentials in browser (observed in several sessions).
- Daily driver accounts used for access to privileged credential vault (CyberArk) and Zscaler.
- SSPR is enabled for admins, weak forms of MFA are allowed for reset (e-mail, mobile, office).
- Service account usage not restricted to specific source and target nodes.
- Service acct passwords are not regularly changed.
- Zscaler and Palo Alto likely allow third-party password vaults: no categorical blocks.
- Break glass and admin. accounts for sensitive and foundational infrastructure stored in CyberArk.
- Admins can leverage Google Authenticator which is permitted to be backed up by Google and iCloud.
- Azure admin login does not require MFA.
- Highly privileged creds are stored in KeePass.
- Azure PIM elevation is self-approved.

Lateral Movement / Recon

- Complex identity Mgmt: AD comprised of many separate domains/forests with some trusts.
- MFA is not required for administrative function via PowerShell, RDP, WMI, MMC, & WinRM.
- Sensitive critical consoles accessible directly from user segments and VPN.
- Segmented admin Azure AD tenant does not exist: Sensitive infrastructure is co-joined to production user AD.
- Servers accessible from user segments by RDP directly—no jumping.
- No rapid SOC isolation of node, identity, e-mail, IP, & cloud change.
- Network segmentation not used as a security tool—no critical console isolation.
- Zscaler & Palo Alto administrative accounts integrated with AD.

Data Exfiltration

- Remote connectivity via split tunnelling.
- Exec. DNS filtering less restricted than most users (e.g., blanket allow for file sharing).
- Server segments are permitted to browse the Internet.
- 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.
- No effective blocking of file sharing, online storage, online backups, personal storage, remote access services, password vaults, hacking tools, & other commercially & maliciously available software used for exfiltration.
- Apps require no MFA or authentication challenge when conencted to VPN or on-prem.
- Some users permitted to use personal e-mail services.
- SaaS and DevOps tools are accessible off the VPN.

- Even the largest companies are woefully unaligned with Breach Context.
- This organization could be "gotten" with great ease—but that's the point.
- Defense contractors we have assessed have SIMILAR issues.
- Recovery Assurance = Resilience

Common Defense Control Issues

In an assessment of clients over the past ~2.5 years, our assessments 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

Assessments 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

Our assessments 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: By the Numbers

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 password 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

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.

COME CHAT WITH US

FENIX 24®
Recovery & Restoration

ATHENA 7®
Strategy & Execution

GRYPHO 5®
Managed Protection

ARGOS 99®
Asset & Resiliency Software

Scan to download this presentation

SCAN TO DOWNLOAD