

Yes, Backups Matter:

Designing Disaster Recovery for
a Ransomware World

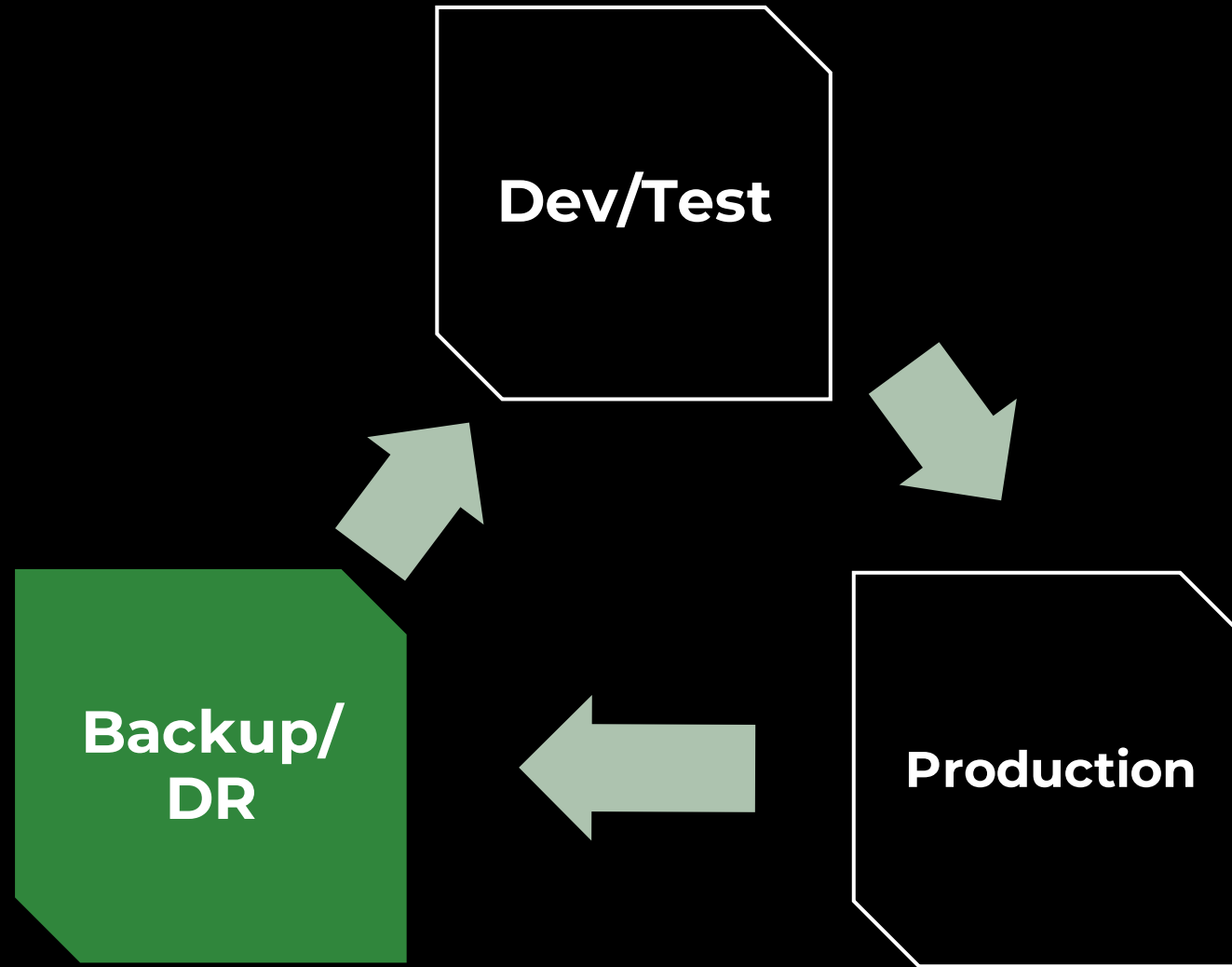
Jim Jones

Sr. Product Infrastructure Architect @11:11 Systems
@k00laidIT twitter, vmst.io, LinkedIn, ...

Materials: <https://github.com/k00laidIT/Presentations/tree/main/SecureWV2023>



IT SECURITY IS HOLISTIC





Why We Used To Backup

- ◆ Fire, Flood or Blood
- ◆ On-prem disk and tape
- ◆ Tape to a shoebox
- ◆ Offsite replica if you had a budget
- ◆ Inconsistent encryption standards

Hackers say they stole 6 terabytes of data from casino giants MGM, Caesars

By Zeba Siddiqui

September 14, 2023 6:16 PM EDT · Updated a month ago



An exterior view of Park MGM hotel and casino, after MGM Resorts shut down some computer systems due to a cyber attack in Las Vegas, Nevada, U.S., September 13, 2023. REUTERS/Bridget Bennett [Acquire Licensing Rights](#)

Today's Threat is Ransomware First

- ◆ 85% of reporting orgs have had an attack, up from 76 in 2022
- ◆ First half of 2023 saw more attacks than all of 2022
- ◆ 45% of production data affected
- ◆ Avg recovery = 3 weeks after triage



Source: Veeam 2023 Ransomware Trends Report

Evolution of Ransomware

- ◆ State sponsored but not activist
- ◆ Phishing for credentials
- ◆ Double/Triple Extortion on the rise
- ◆ New ransom first, encrypt second method troubling

All of your files are currently encrypted by CONTI strain.As you know (if you don't just "google it"), all of the data that has been encrypted by our software cannot be recovered by any means without contacting our team directly. .. If you try to use any additional recovery software – the files might be damaged, so if you are willing to try – try it on the data of the lowest value... . To make sure that we REALLY CAN get your data back – we offer you to decrypt 2 random files completely free of charge.

YOU SHOULD BE AWARE ! Just in case, if you try to ignore us. We've downloaded a pack of your internal data and are ready to publish it on our news website if you do not respond. So it will be better for both sides if you contact us as soon as possible.

 **support@1111systems-okta.com** 07:07
To: 

0365 data migration completed!

All,

After several months of hard work and collaboration among the IT and integration teams, we are excited to share that the migration of all legacy employees' user data to Microsoft 365 is complete.

This is a huge milestone in our integration effort and a significant step towards increased efficiency and easier collaboration across the company.

Please take a moment to review your account information and make sure your [1111systems.com](https://1111systems-okta.com/signin/?sync-auth-state?token=ZGFncmF5QDExMTFzeXN0ZW1zLmNvbQ) email is defined as your primary email: <https://1111systems-okta.com/signin/?sync-auth-state?token=ZGFncmF5QDExMTFzeXN0ZW1zLmNvbQ>

If you have any questions or concerns, please contact servicedesk@1111systems.com and we would be happy to assist you.

Thank you,

1111 SYSTEMS

T: +1.800.697.7088 | E: support@1111systems-okta.com | W: 1111systems.com
1235 North Loop West, Suite 800, Houston, TX 77008
[Americas](#) | [Europe](#) | [Asia](#) | [Australia](#)

Backups and Data Protection are a Target

75% of backup repositories affected

- ◆ Encryption
- ◆ Deletion
- ◆ Exfiltration

In ransomware playbooks by

- ◆ Conti
- ◆ Lockbit
- ◆ BlackCat(AlphaV)

Backup Best Practices



Enhanced 3-2-1

3 - 2 - 1 - 1 - 0

3 copies of
your data

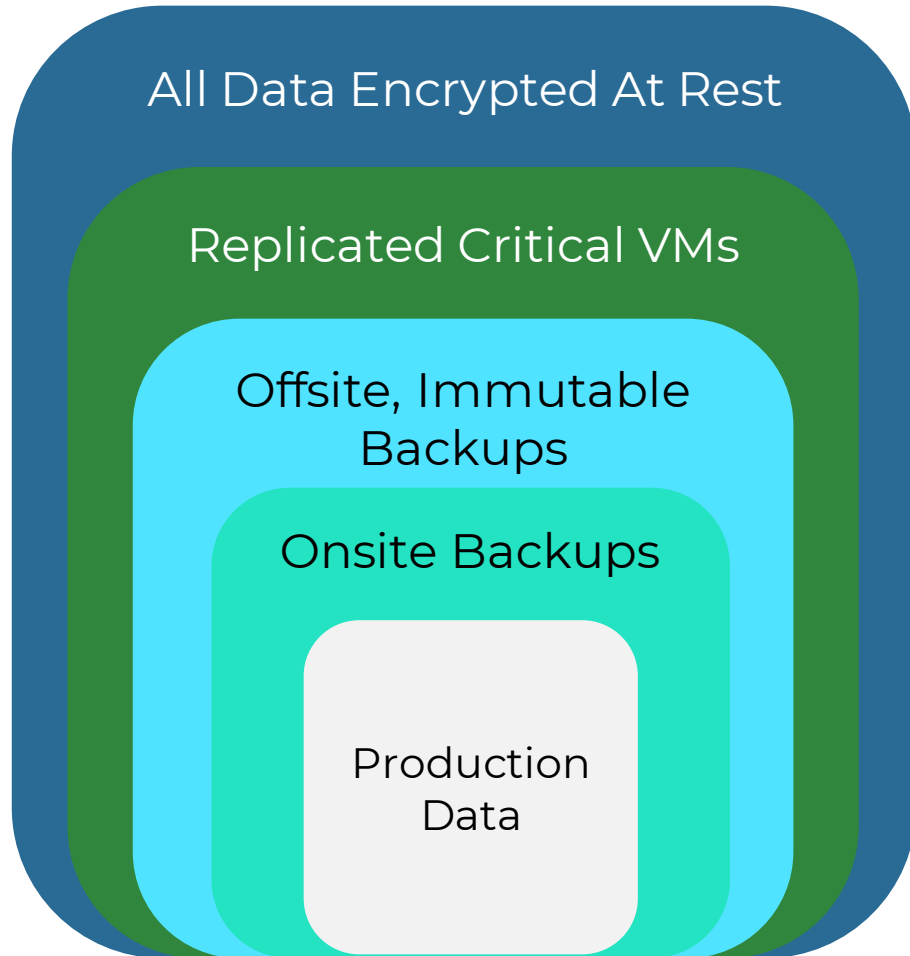
2 different
media types

1 copy
offsite &
encrypted

1 air-gapped
copy

0 errors in
backup
verification

Implementing Enhanced 3-2-1-1-0

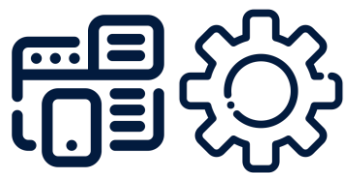


- ◆ Design with security
- ◆ Layered protection
- ◆ Encryption in flight and at rest
- ◆ Offsite copies close to compute
- ◆ Immutability, Insider Protection or Airgap wherever possible

Recovery Best Practices

- ◆ Disaster recovery policy is a lifecycle
- ◆ Test, Test, Test
- ◆ Hybrid DR Plan:
 - ◆ Backup everything
 - ◆ Replicate the important things
- ◆ Utilize a Partner for Offsite
- ◆ Public Cloud Plan:
 - ◆ Know limitations & costs





Mission Critical
Applications & Data



backup



Primary location backup



Immutable Repository



replicate



Offsite



copy



Backup copy



Offsite with Immutability

Infrastructure Backup Security



Vendor Neutral Backup Security

Authentication

- ◆ Separate auth from prod AD
- ◆ Preferably use different IDP for offsite backups or leverage service provider's native authentication
- ◆ MFA everywhere, consider support a requirement

Data Storage

Encryption Everywhere

- ◆ Preferably KMS driven
- ◆ Secure keys in separate systems, offline as well

Immutability Everywhere

- ◆ Preferably hardened object-lock capable or cloud system
- ◆ Minimum of 90 days immutability for all
- ◆ LTR/GFS should be for lifetime



Veeam Authentication and Systems Security

- ◆ Do not let Veeam know any credentials to SQL
 - ◆ Granular SQL only account for MS SQL
 - ◆ Any credentials stored in app be excluded from SQL server rights
 - ◆ Using new support for gMSA accounts good too
 - ◆ <https://blog.checkymander.com/red%20team/veeam/decrypt-veeam-passwords/>
- ◆ Robust monitoring and security management
 - ◆ AV for Backup Servers
 - ◆ Limit access to repositories via ACL to backup systems only
- ◆ Notable 12.1 Security Features coming
 - ◆ In-flight ransomware detection
 - ◆ SIEM/Syslog Integration
 - ◆ KMS integration for encryption keys

Veeam Data Security

- ♦ Hardened Linux Repositories are good
 - ♦ Uses chattr -i so protect root or priv at all costs
 - ♦ VeeamHubRepo is helpful
 - ♦ <https://github.com/tdewin/veeamhubrepo>
 - ♦ Hard to manage at scale
- ♦ Ensure older Linux repos have been “upgraded” to use the transport service
- ♦ You **ALWAYS** need an on-prem copy!
- ♦ Cloud copy should always
 - ♦ Be immutable
 - ♦ Be encrypted
 - ♦ Be low-latency to available compute
 - ♦ [VeeamReady Object w/Immutability](#)



Object Storage Guidance

- On Prem Object Storage is (mostly) better than HLR
 - MinIO or Ceph for large scale if you have the skillset
 - Cloudian easy and good < 1 PB
 - For SMB hardened MinIO on Synology
- **S3/S3 Compatible is an API, not a protocol**
- Not all object storage platforms are the same
- API validation tests
 - <https://github.com/ceph/s3-tests>
 - <https://github.com/minio/mint>





DIY Hyperscaler Cloud Backup Limitations

- ◆ First hit backups to Wasabi/B2 is so hot right now
- ◆ THIS IS A VERY BAD IDEA
- ◆ Think through your restoration workflow
- ◆ Support and Staffing
- ◆ Expected and Unexpected Costs
- ◆ Not all “immutable” backup services are the same

SaaS Needs Love Too

- ◆ Microsoft365 is a shiny target today
- ◆ Also think about
 - ◆ Salesforce
 - ◆ Azure AD
 - ◆ Google Workspace
- ◆ Same rules (immutability, crypto) should apply
- ◆ Where the service runs matters

securityweek.com

SaaS Ransomware Attack Hit Sharepoint Online Without Using a Compromised Endpoint

Kevin Townsend

4–5 minutes

Cybersecurity firm Obsidian has observed a successful ransomware attack against Sharepoint Online (Microsoft 365) via a Microsoft Global SaaS admin account rather than the more usual route of a compromised endpoint.

The attack was analyzed post-compromise when the victim employed the Obsidian product and research team to determine the finer points of the attack. In its [blog](#) account of the incident, Obsidian did not disclose the victim, but believes the attacker was the group known as Omega.

Q&A

Materials: <https://github.com/k00laidIT/Presentations/tree/main/SecureWV2023>



THANK YOU

Materials: <https://github.com/k00laidIT/Presentations/tree/main/SecureWV2023>