# D.E.F.E.N.D.

## Data Exfiltration Focus with Effective Network Defense

## About Us

NJ TRANSIT is New Jersey's public transportation corporation. Its mission is to move New Jersey and the region by providing safe, reliable and affordable public transportation that connects people to their everyday lives, one trip at a time.

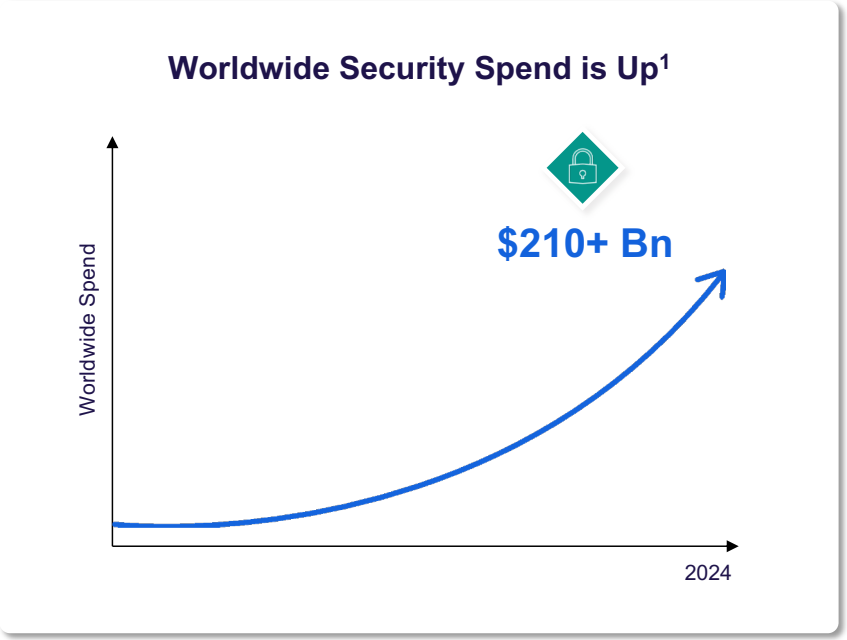
Covering a service area of 5,325 square miles, NJ TRANSIT is the nation's third largest provider of bus, rail and light rail transit, linking major points in New Jersey, New York and Philadelphia. The agency operates an active fleet of 2,221 buses, 1,231 trains and 93 light rail vehicles. On 253 bus routes and 12 rail lines statewide, NJ TRANSIT provides nearly 270 million passenger trips each year.

# Regulatory Compliance

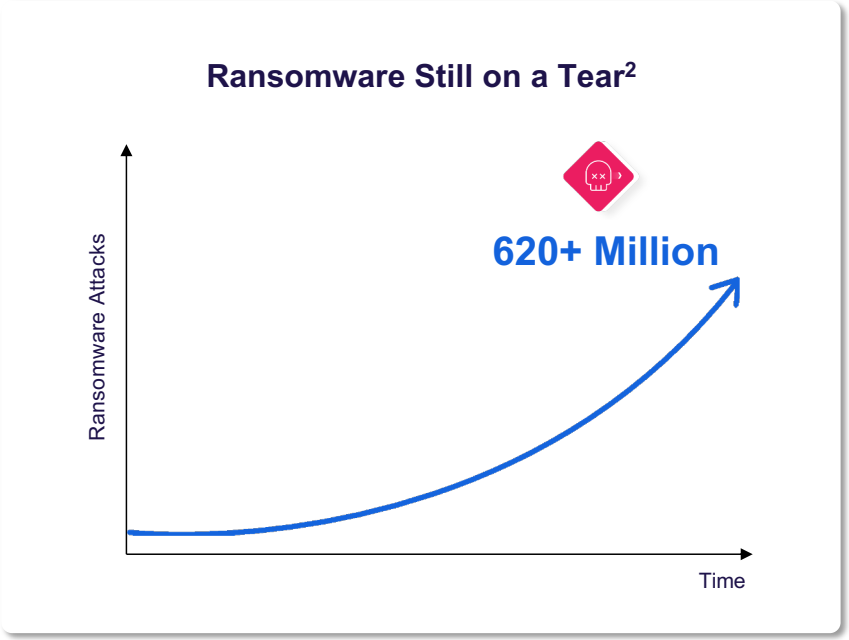


Federal Transit Administration

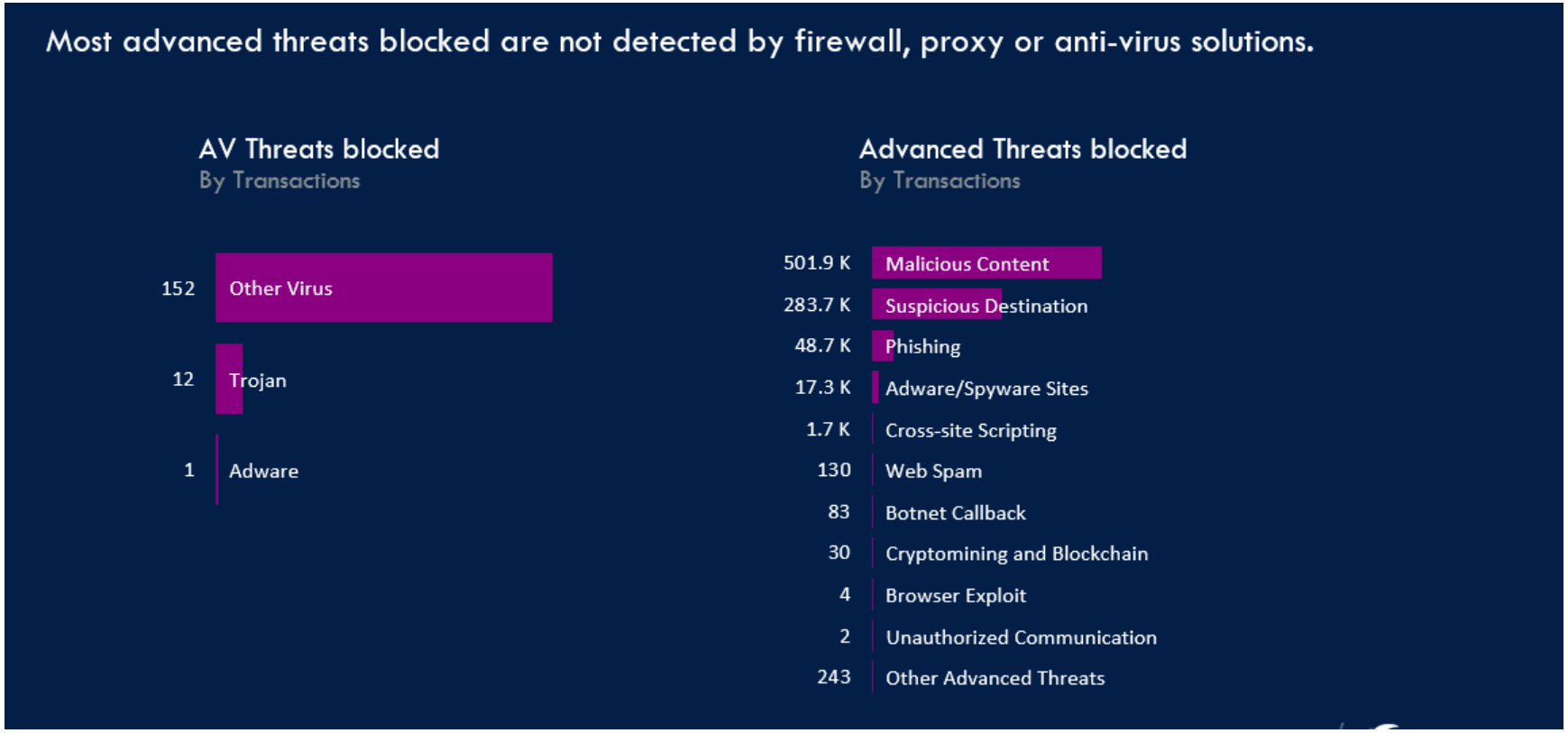
## High Cybersecurity Spend




## Attacks Continue Unabated



# D.E.F.E.N.D. AI Enabled Advanced Threats



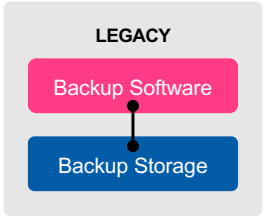
**Realign Focus from**
**Attack Prevention.**

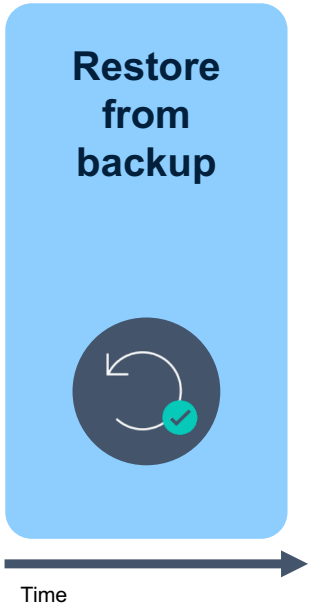

**Focus on**
**Cyber Recovery.**


# Readiness for Cyber Recovery

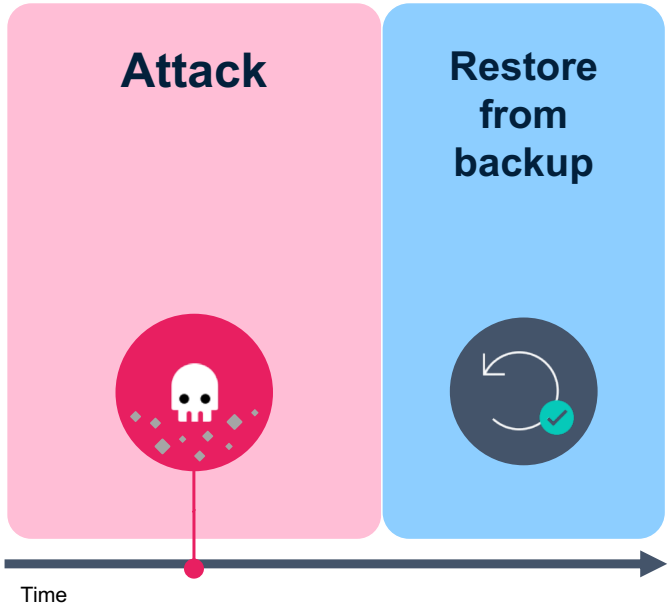

# Focus on Cyber Recovery Time Objective

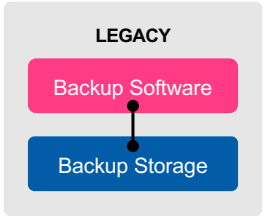
# RTO = Recovery Time Objective



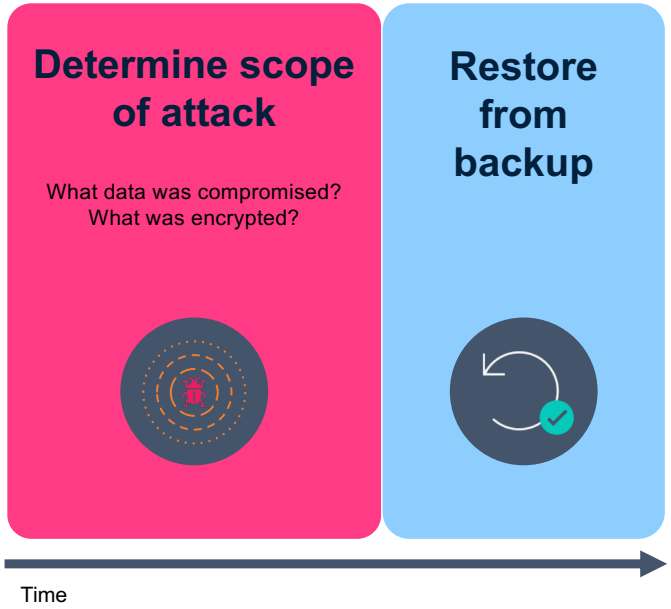



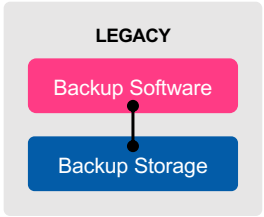
# RTO ≠ Cyber RTO



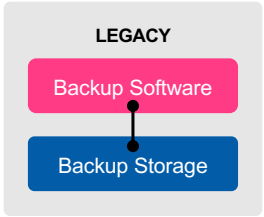



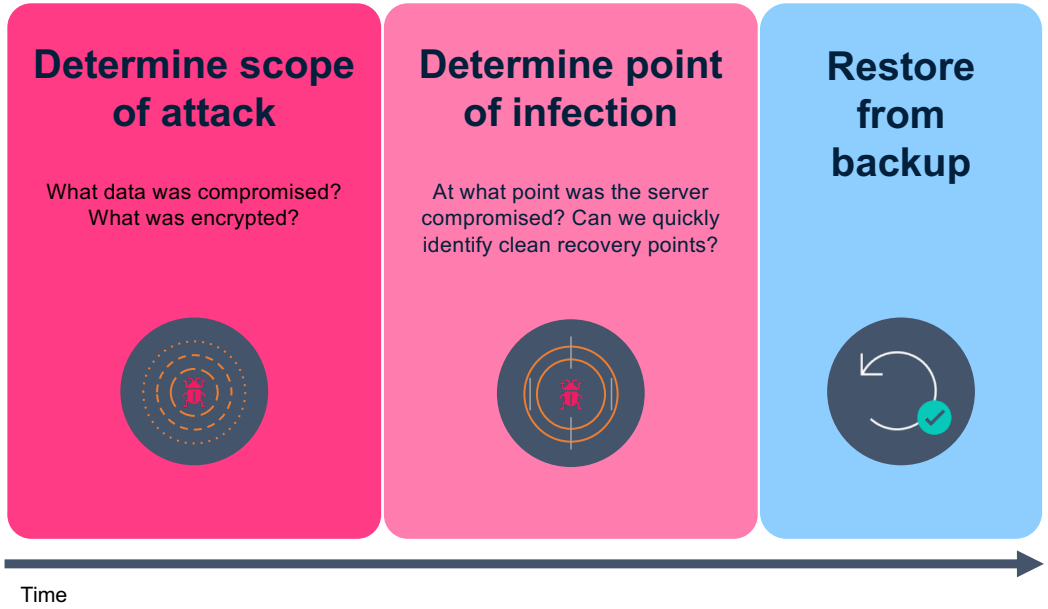
# RTO ≠ Cyber RTO



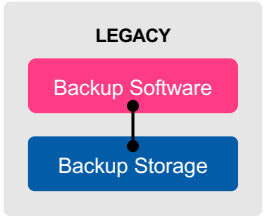



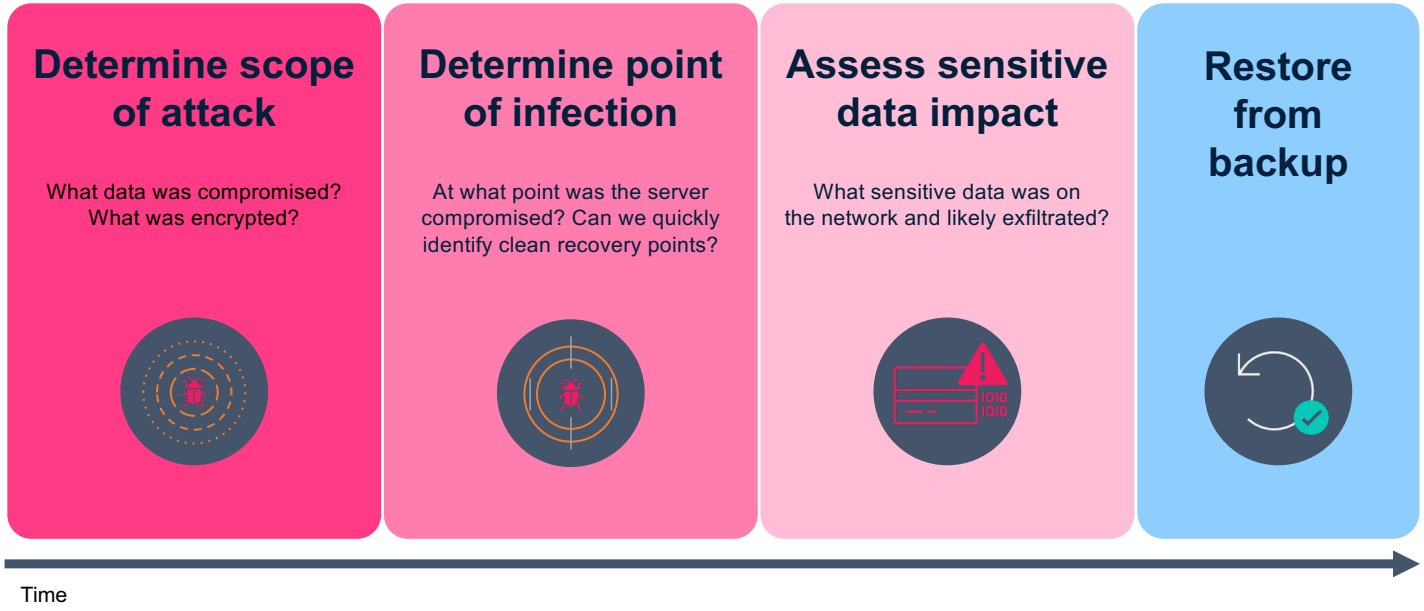
# RTO ≠ Cyber RTO



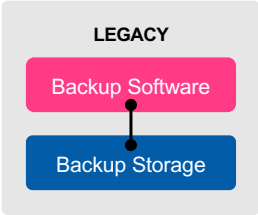



# RTO ≠ Cyber RTO



# Cyber RTO Extends RTO up to 100x




## Determine scope of attack

What data was compromised? What was encrypted?

## Determine point of infection

At what point was the server compromised? Can we quickly identify clean recovery points?

## Assess sensitive data impact

What sensitive data was on the network and likely exfiltrated?

## Find malware and quarantine

Can we find all locations of malware? Can we isolate malware to prevent re-infection?

## Restore from backup

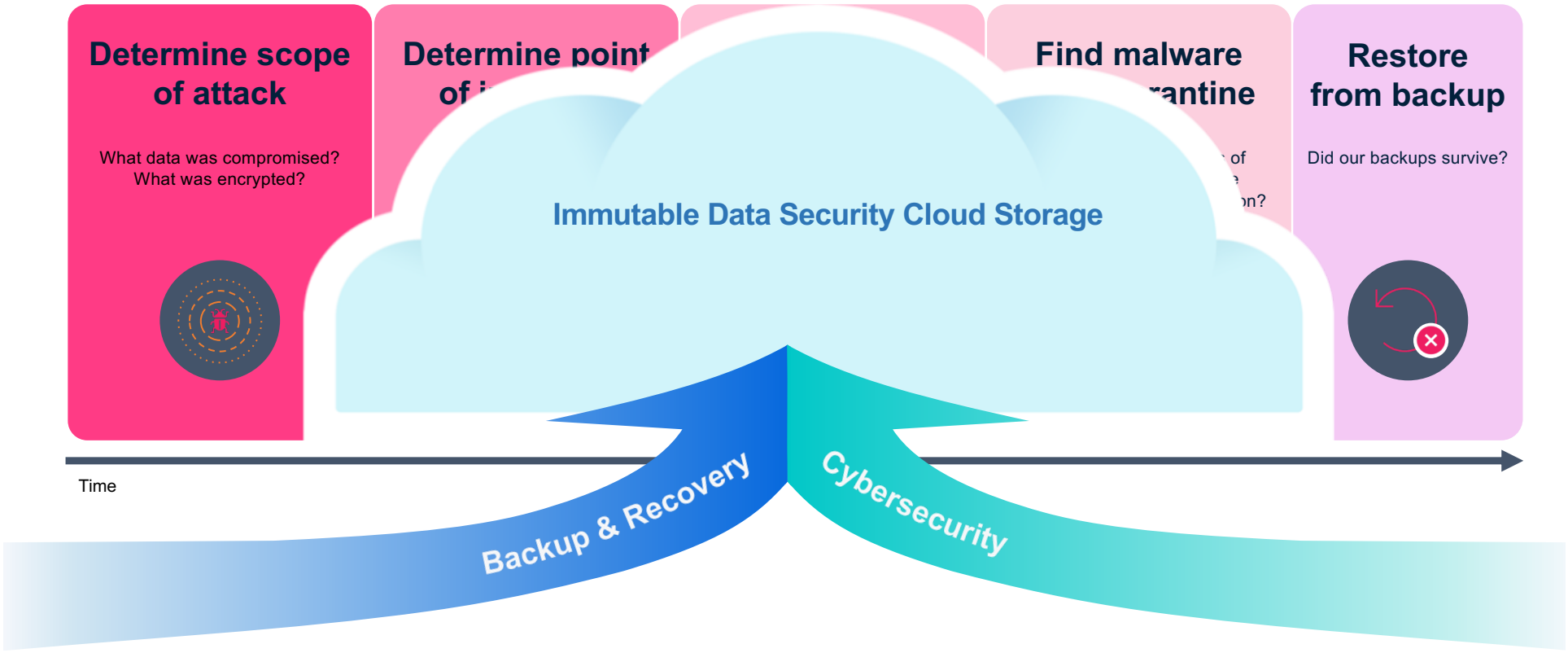
Did our backups survive?

Time

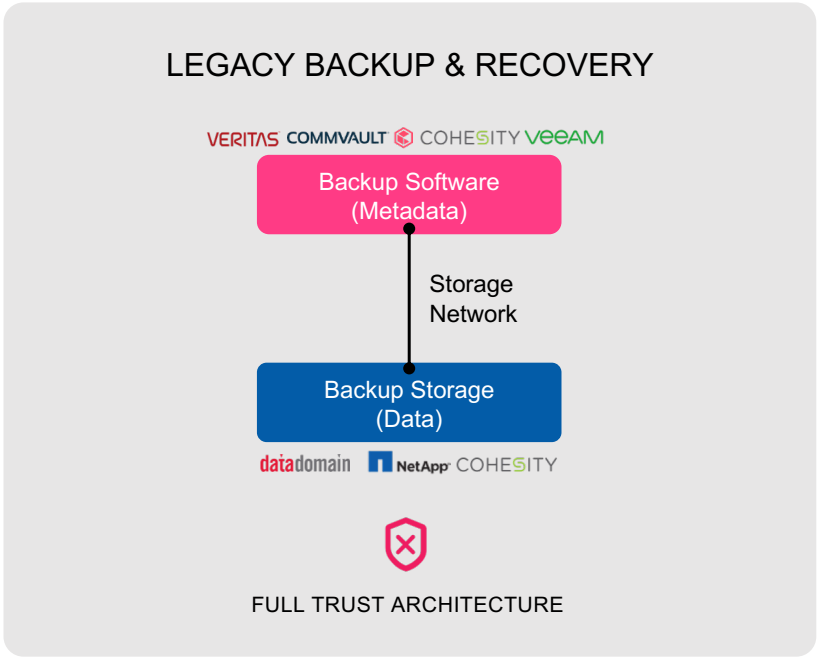
# When Breached, Companies Are Down for Weeks.

# D.E.F.E.N.D.

## Data Exfiltration Focus with Effective Network Defense

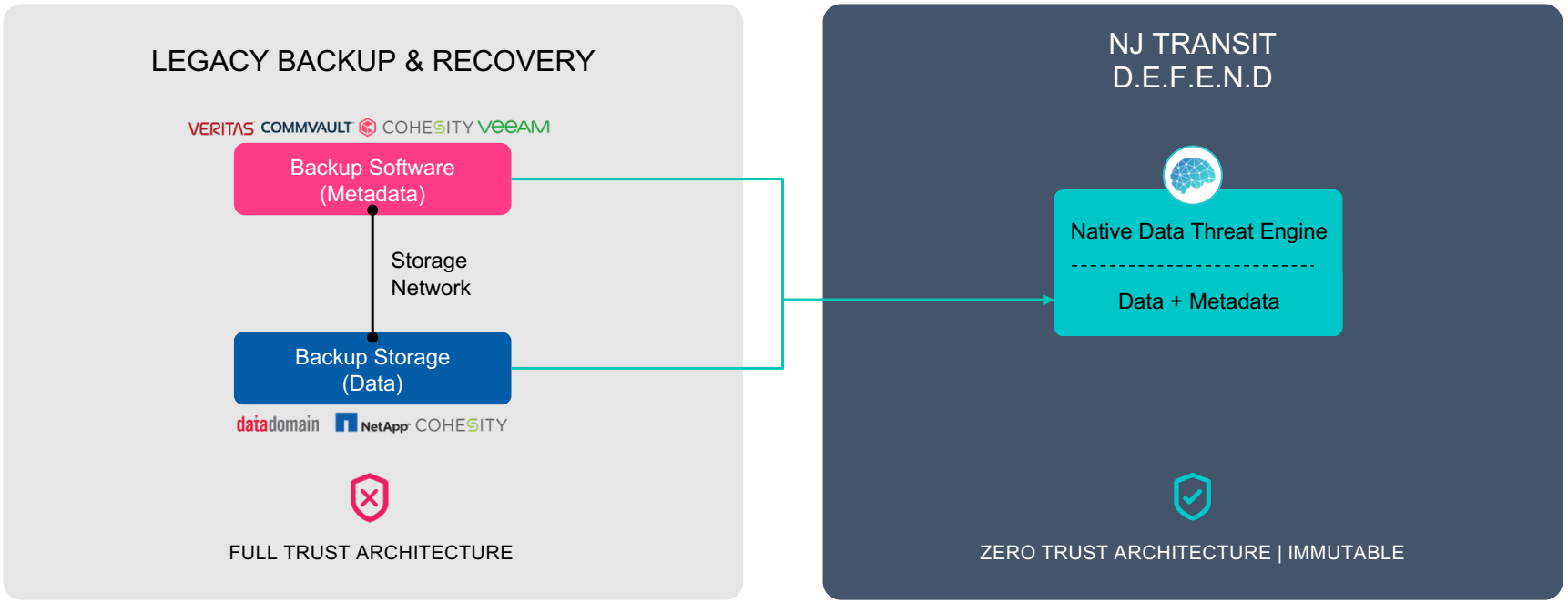


# Legacy Backup & Recovery

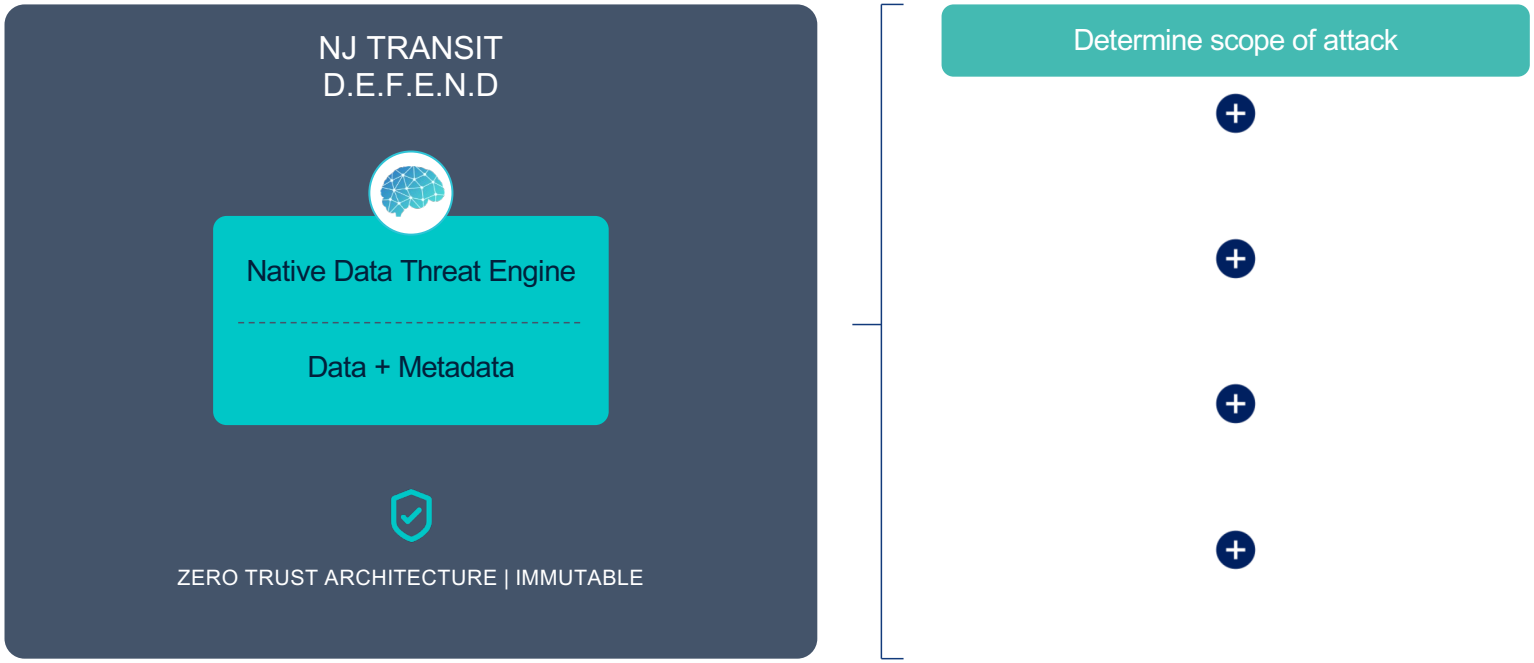


## Legacy Backup & Recovery

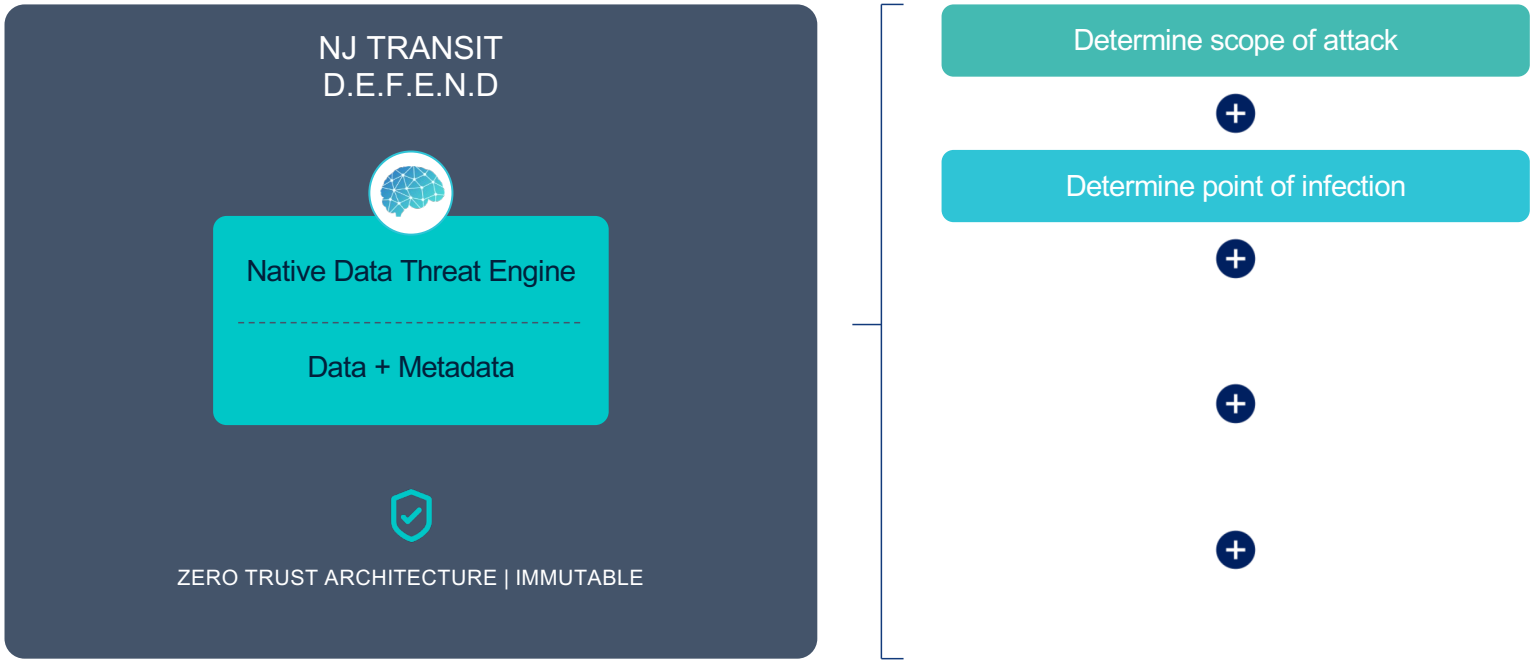
## D.E.F.E.N.D. Architecture



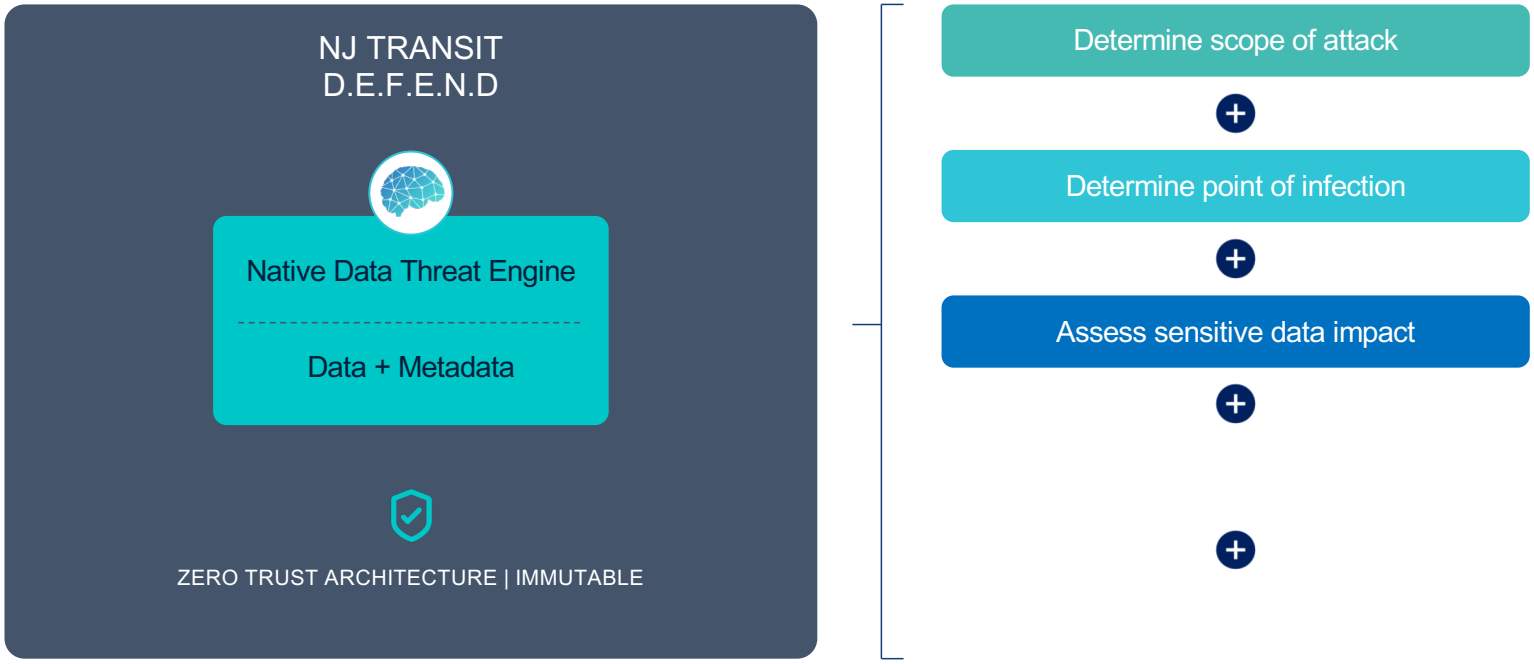
# D.E.F.E.N.D Architecture Delivers 100x Faster Cyber Recovery



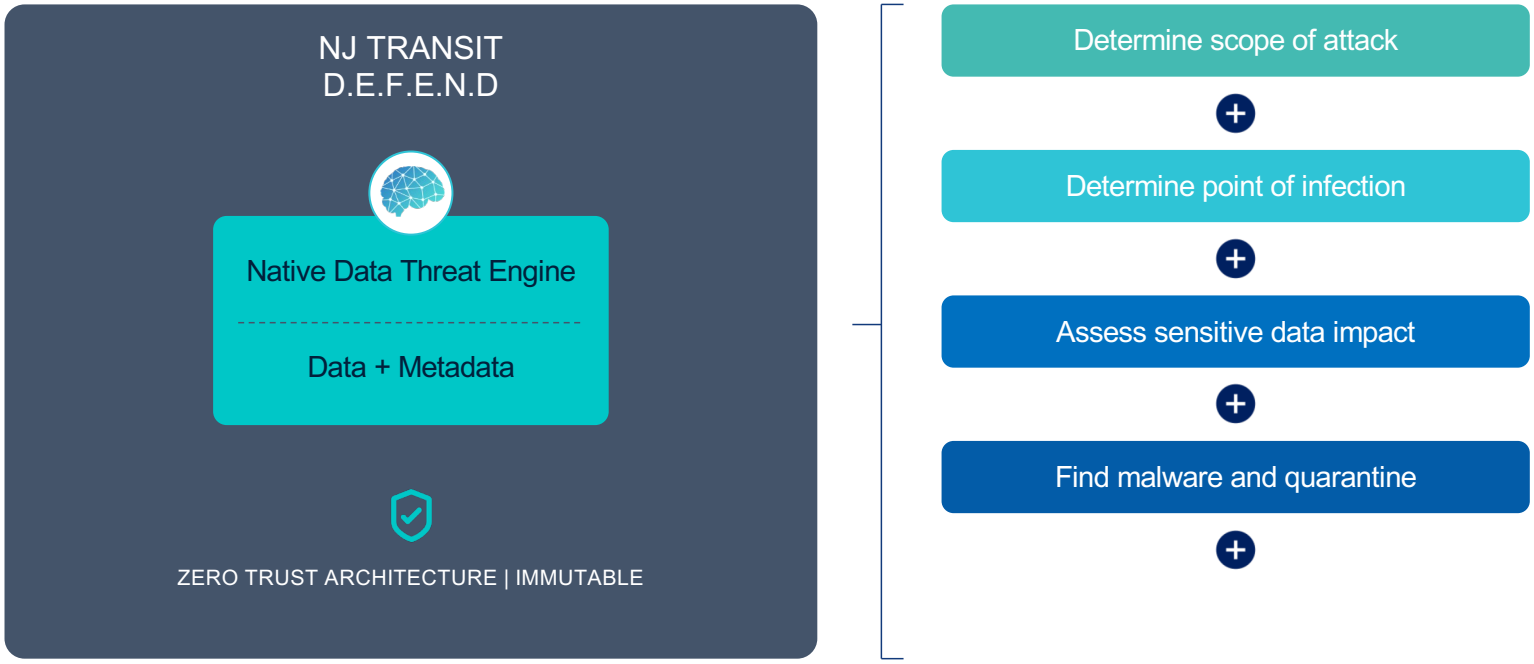
# D.E.F.E.N.D Architecture Delivers 100x Faster Cyber Recovery



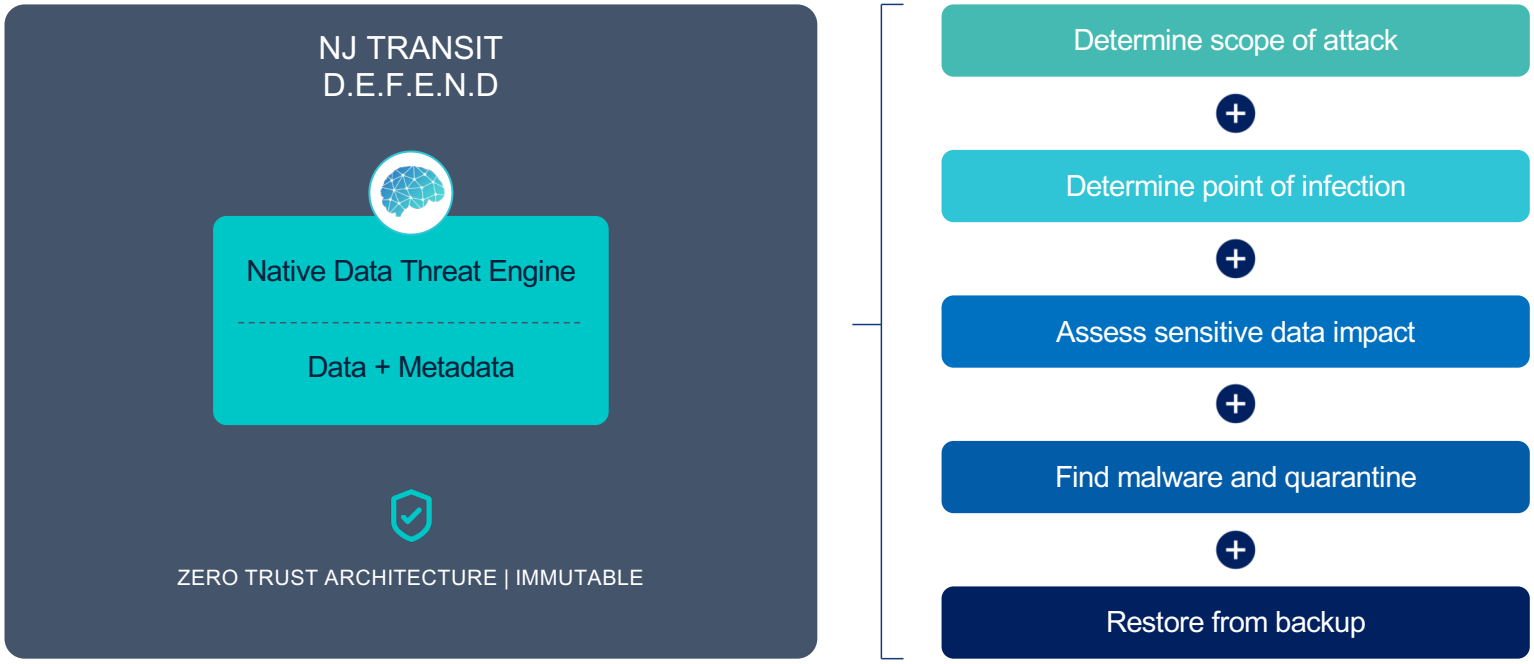
# D.E.F.E.N.D Architecture Delivers 100x Faster Cyber Recovery



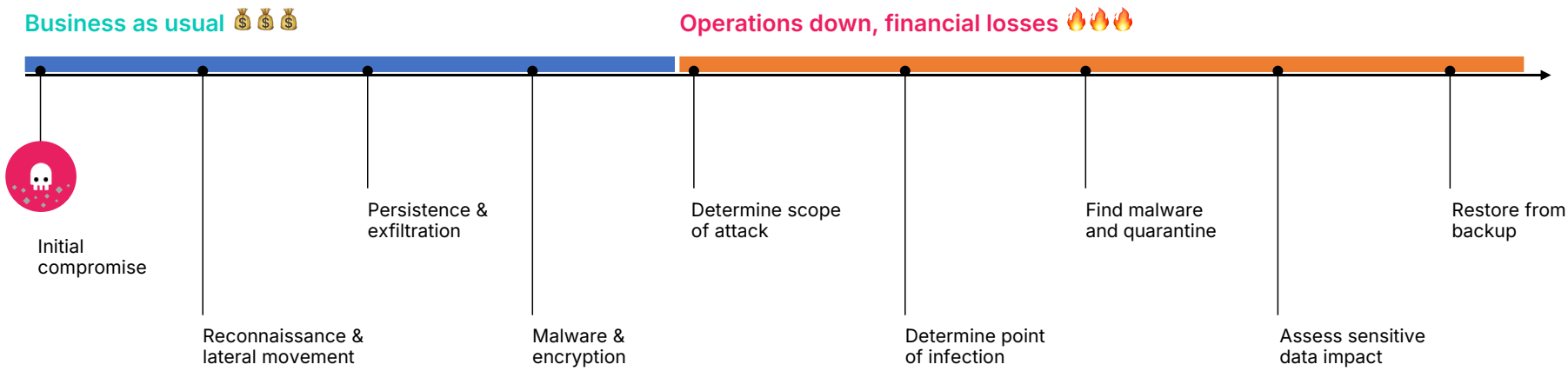
# D.E.F.E.N.D Architecture Delivers 100x Faster Cyber Recovery



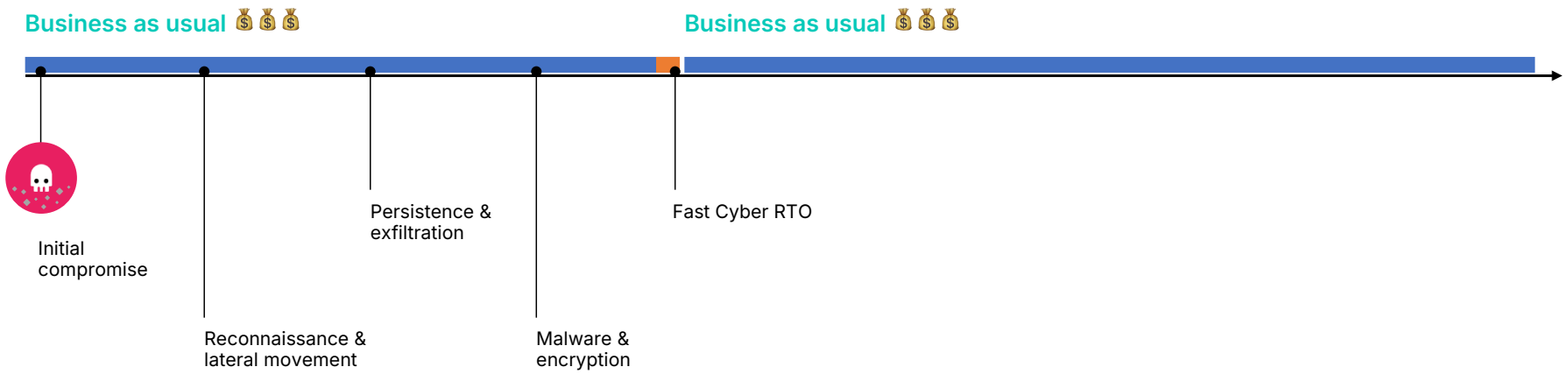
# D.E.F.E.N.D Architecture Delivers 100x Faster Cyber Recovery



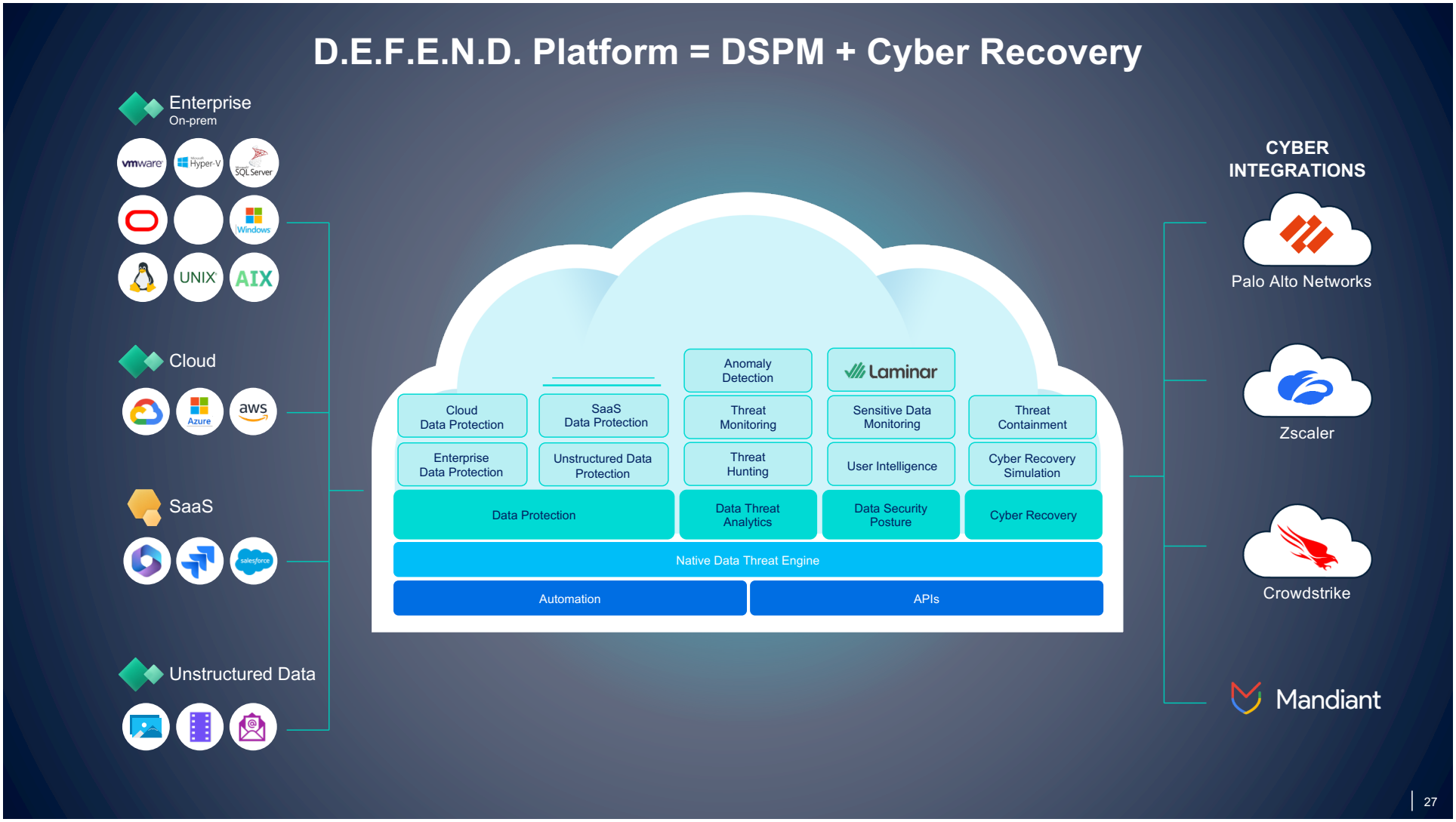
# Before D.E.F.E.N.D.



# After D.E.F.E.N.D.



# D.E.F.E.N.D. Platform = DSPM + Cyber Recovery



# D.E.F.E.N.D. Benefits

### Cyber Recovery

*“Speedy Recovery is Critical. No Payment to Cyber Criminals*

# D.E.F.E.N.D. Security Value

### Cyber Recovery

*“Speedy Recovery is Critical. No Payment to Cyber Criminals*

### Cloud Cost Reduction

*“Cloud Expenses are Reduced. SaaS Backups Are Consolidated.”*

# D.E.F.E.N.D. Benefits

### Cyber Recovery

*“Speedy Recovery is Critical. No Payment to Cyber Criminals*

### Cloud Cost Reduction

*“Cloud Expenses are Reduced. SaaS Backups Are Consolidated.”*

### Cyber Resilience

### Minimize Breach Impact

### (DSPM)

*“Minimized sensitive data exposure and user access.”*

# Zero Trust Data Management




- Retention Lock
- Secure Local Users with TOTP
- Secure AD Logins with MFA & RBAC
- End-to-End Encryption
- No 3rd Party Apps
- Immutable File System

**Bunker-in-a-box**
**Hardened Secure Linux Build**
**Vendor Patched & No Shell Access**
**IPMI/OOB Mgmt Disconnected**

**End-to-End Encryption**
- All data encrypted in-flight using TLS 1.2 SHA-512 hash
- All data encrypted at-rest to FIPS 140-2 Level 2 RSA 2048-bit key
- Key mgmt using TPM or KMIP for key rotation
- No internal NFS/SMB, no ability to spoof, intercept or read from network

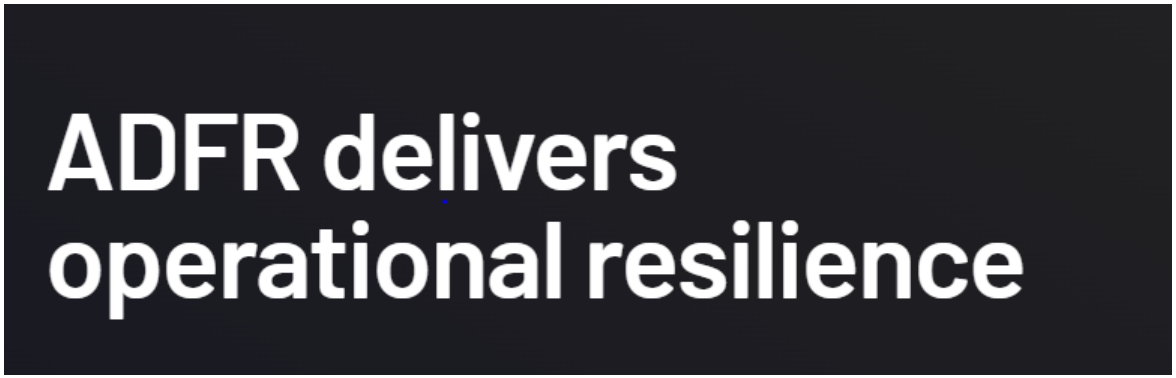
**Secure AD User/Group Logins & RBAC**
- Integrate into RSASecurID, Duo, anything SAML2.0 compliant
- Multi-factor on all AD integrated logins, alerts/syslog for failed logins
- RBAC, read-only admins, least privilege access & API tokens

**Secure Local Admin Logins**
- Built-in TOTP (Time-based One-Time Password)
- Secure local accounts in minutes any Android/IOS device
- Removes backdoor of local account access, also applies to SSH
- Required account for recovery in event of attack (AD compromised)

**Retention Lock (support driven process)**
- Prohibits backup admin from expiring backups prematurely
- No removal of replication, archiving, re-assign, shorten of retention
- Prohibits all node/cluster resets & NTP poisoning/drift (monotonic clock)
- Cohasset validated - SEC 17a-4(f) & FINRA 4511(c) compliant

Logical Air Gap + Immutable + Encryption + Secured Logins + Retention Lock + NTP Protection
= Impenetrable From Ransomware Attacker

# AD is now the #1 target for cyberattackers



# Simplify Disaster Recovery Planning

## Prevent Malware Reintroduction

# Automate AD Forest Recovery

**Widespread attacks that exploit Active Directory can cripple your organization.**

**When a ransomware or wiper attack takes out domain controllers, recovering your AD forest can drag on for days or even weeks, risking malware re-infection in the process.**

**Active Directory Forest Recovery (ADFR), you'll be back in business in minutes or hours rather than days or weeks.**

**If you've lost AD, you've lost your business. It's that extreme.**

# Q/A

NJTRANSIT
The Way To Go.