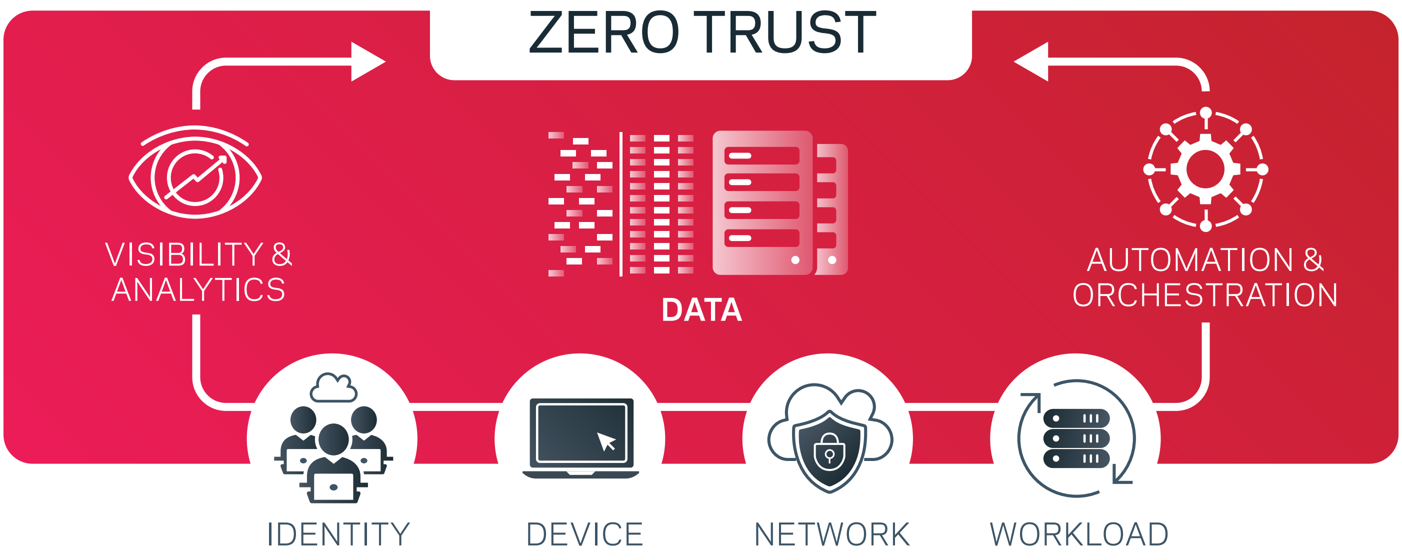
VERITAS

TRUST NO ONE
VERIFY EVERYONE

AT EVERY POINT IN YOUR NETWORK

Cyber criminals are trying to take down your backup and data protection infrastructure by inserting malware into your network months before they trigger a catastrophic cyber event.

Adopting a **Zero Trust policy** with identity and access management (IAM) limits access to your highly sensitive data and backups.



Implementing Zero Trust infrastructure provides:

- Security extended across your hybrid or multi-cloud environment
- Greater visibility and tracking of user activity
- Improved compliance and governance controls

IDENTITY & ACCESS MANAGEMENT

- Role-Based Access
- Multi-Factor Authentication
- Digital Certificates
- Single Sign-On

Combining Zero Trust with IAM reduces your total attack surface and limits the movement of a cyber-criminal within your network. Increase the security of your data, applications, and backups in the event of an attack using granular role-based access controls (RBAC) and multi-factor authentication (MFA) to guard every location within your infrastructure.

ENCRYPT DATA IN TRANSIT AND AT REST

DATA ENCRYPTION
IN TRANSIT
AT REST

Encrypting your data during all activities helps to:

- Strengthen the perimeter that a hacker must break through
- Increase your ability to quickly identify and isolate security events

Explore ways to increase resiliency against threats.

Download the white paper now.

VERITAS

1 (866) 837-4827 ▪ www.veritas.com