OVERVIEW

FORTIFY YOUR DEFENSE WITH DATA-CENTRIC ZERO TRUST

Empower your organization with a Zero Trust approach that keeps your critical data critically secure from the inside out.

To help combat rising cybersecurity threats, federal mandates are pushing organizations across the public sector to adopt Zero Trust solutions. Now is the time to get ahead with a multi-layered Zero Trust architecture that that goes beyond perimeter security to protect your data from the inside out.

Zero Trust can reduce the cost of a data breach by about

$1.51M

Source: IBM Cost of a Data Breach Report 2023

2x

more likely to avoid critical outages due to cyberattacks when using Zero Trust data segmentation

Source: CyberTalk, 12 illuminating Zero Trust statistics 2022

Organizations with Zero Trust implementations increase their security resilience rating by

30%

Source: Cisco Security Outcomes Report, Volume 3

It's all about the data
When setting up a Zero Trust architecture, there are five key pillars: people, devices, networks, applications, and data. In every case, it's always the data that hackers are after—the other four pillars are the means to get to the data. A data-centric security model focuses on treating your data as your most valuable asset, prioritizing its accessibility, security, and control throughout its lifecycle.

A matter of trust
In a trust-nothing world, you can always trust NetApp to keep your data secure. We have 30 years of data patterns to understand how data should behave. By applying AI on top of these data patterns, our technology can detect abnormal behavior, deliver rock-solid data protection and security, and help you quickly restore your data.

For added protection, NetApp is the only enterprise data management provider to offer a Ransomware Recovery Guarantee—if we can't help you restore your NetApp Snapshot™ data, we'll make it right.

Superior data security, protection, and governance
Zero Trust architecture implementations built on NetApp are designed around NIST SP 800-207 and Forrester guidelines with a focus on protecting data from the inside out. Our solutions complement the NIST Cybersecurity Framework, emphasizing five key components of a comprehensive data security strategy: Identify, Protect, Detect, Respond, and Recover. You get robust and resilient security that enables you to maintain data confidentiality, integrity, and availability. Your organization can respond effectively to security incidents and recover quickly from data disruptions.

Identify
Understand your assets, cybersecurity risks, and business context. This component includes asset management, risk assessment, and intelligent data governance. NetApp® BlueXP™ classification scans on-premises and cloud data environments to map and classify data, and to identify personally identifiable information (PII).

Protect
Implement a least-privilege data access model in which access to data, applications, and resources is limited to only authorized entities. The NetApp FPolicy Zero Trust Engine capability of NetApp ONTAP® provides granular, role-based user access controls. Multifactor authentication (MFA) provides another layer of security. NetApp Volume Encryption (NVE) delivers strong data-at-rest encryption.

Detect
Continuously monitor your environment to detect any unusual user or file behavior. NetApp Cloud Insights and the NetApp Active IQ® tool rely on AI and machine learning to detect anomalous behavior, potential threats, and unauthorized access attempts in real time. The NetApp ONTAP Autonomous Ransomware Protection (ARP) feature uses workload analysis to proactively detect and warn about abnormal file activity.

Respond
If an attack occurs, you need to be able to respond instantly. As soon as anomalous user behavior or abnormal data patterns are detected, you can automatically trigger NetApp Snapshot copies to create a safe data recovery point.

Recover
Recovery involves restoring the data affected by a cybersecurity incident and returning to normal operations. NetApp Snapshot technology creates indelible backup copies so that if a malicious event occurs, your data is protected and easily restored to a known state.

Learn more about NetApp Zero Trust architecture and cyber resilience solutions.

Contact Us

About NetApp
NetApp is the intelligent data infrastructure company combining unified data storage, integrated data services, and CloudOps solutions to turn a world of disruption into opportunity for every customer. NetApp creates silo-free infrastructure, then harnesses observability and AI, to enable the best data management. As the only enterprise-grade storage service natively embedded in the world's biggest clouds, our data storage delivers seamless flexibility and our data services create a data advantage through superior cyber-resilience, governance, and applications agility. Our CloudOps solutions provide continuous optimization of performance and efficiency through observability and AI. No matter the data type, workload or environment, transform your data infrastructure to realize your business possibilities with NetApp. www.netapp.com

NetApp

© 2024 NetApp, Inc. All Rights Reserved. NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners. NA-1076-0224