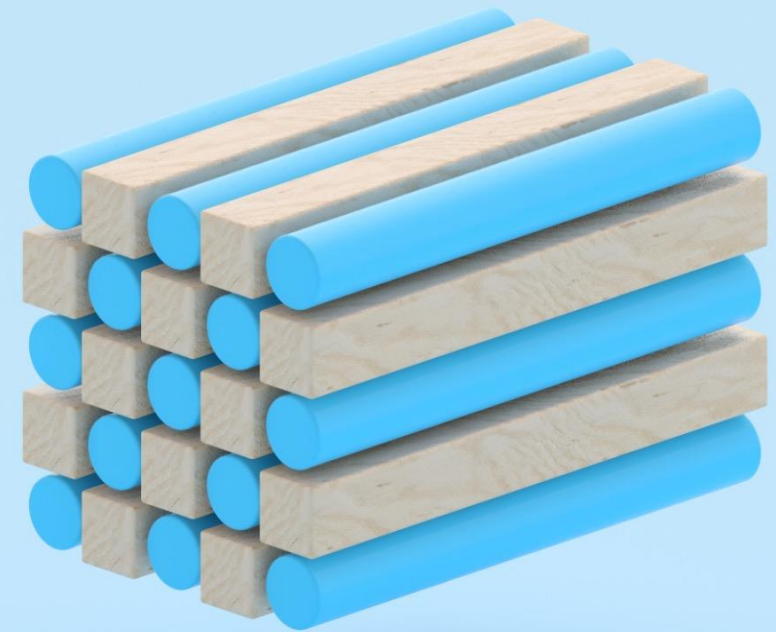# Protect your data from ransomware with NetApp

Explore a data-centric approach to ransomware protection

NetApp

Priya Munshi
Tech Partner Manager
16 Nov 2022

Ransomware is a universal threat

Headlines that organizations can't ignore

$5.9M ransomware attack on major agriculture group poses risk to US grain, pork, chicken supply

Lucas Manfredi · 1 hr ago

UHS hospital network hit by ransomware attack

UHS operates more than 400 hospitals across the US and UK. Some US hospitals have been down since Sunday.

By Catalin Cimpanu for Zero Day | September 28, 2020 -- 15:19 GMT (08:19 PDT) | Topic: Security

JBS says it paid $11 million ransom after cyberattack

IBM: Ransomware attacks surged in Q2, ransom demands rising

IBM Security examined several concerning ransomware for this year, as well as an exponential increase in ransom demands and massive spike in attacks during the spring.

By Arielle Waldman, News Writer   Published: 28 Sep 2020

Colonial Pipeline CEO admits to authorizing $4.4 million ransomware payment

A patient has died after ransomware hackers hit a German hospital

This is the first ever case of a fatality being linked to a cyberattack.

by Patrick Howell O'Neill   September 18, 2020

Disaster Recovery and Business Continuity During COVID-19

Among the vast array of challenges posed by the global COVID-19 pandemic, cybersecurity issues have bubbled to the surface, including an increase in remote workers and cybercriminals taking advantage of the situation. How can organizations focus on disaster recovery and business continuity in light of the shifting threat landscape? Explore the series of blogs for advice from cybersecurity professionals about disaster recovery and evolving threat intelligence in the wake of COVID-19.

See the articles

3

Today's threat environment

Source: Verizon 2021 Data Breach Investigations Report

Incidents 29,207	Breaches 5,258

Top industries breached
1. Public
2. Professional
3. Healthcare

24% **of breaches involved internal actors**
85% **of breaches involved a human element**

Top breach methods
1. Social engineering
2. Basic web application attacks
3. System Intrusion

70% of breaches were financially motivated

Top compromised data
1. Credentials
2. Personal
3. Medical

30% of breaches took months or longer to discover
13% of non-DoS incidents were ransomware
10% of breaches involved ransomware

How much does ransomware cost?

$5B

Insurance premiums

20%-30% annual growth**

$1,850,000

Average cost*
to remediate a ransomware attack in 2021 ($768,106 in 2020)
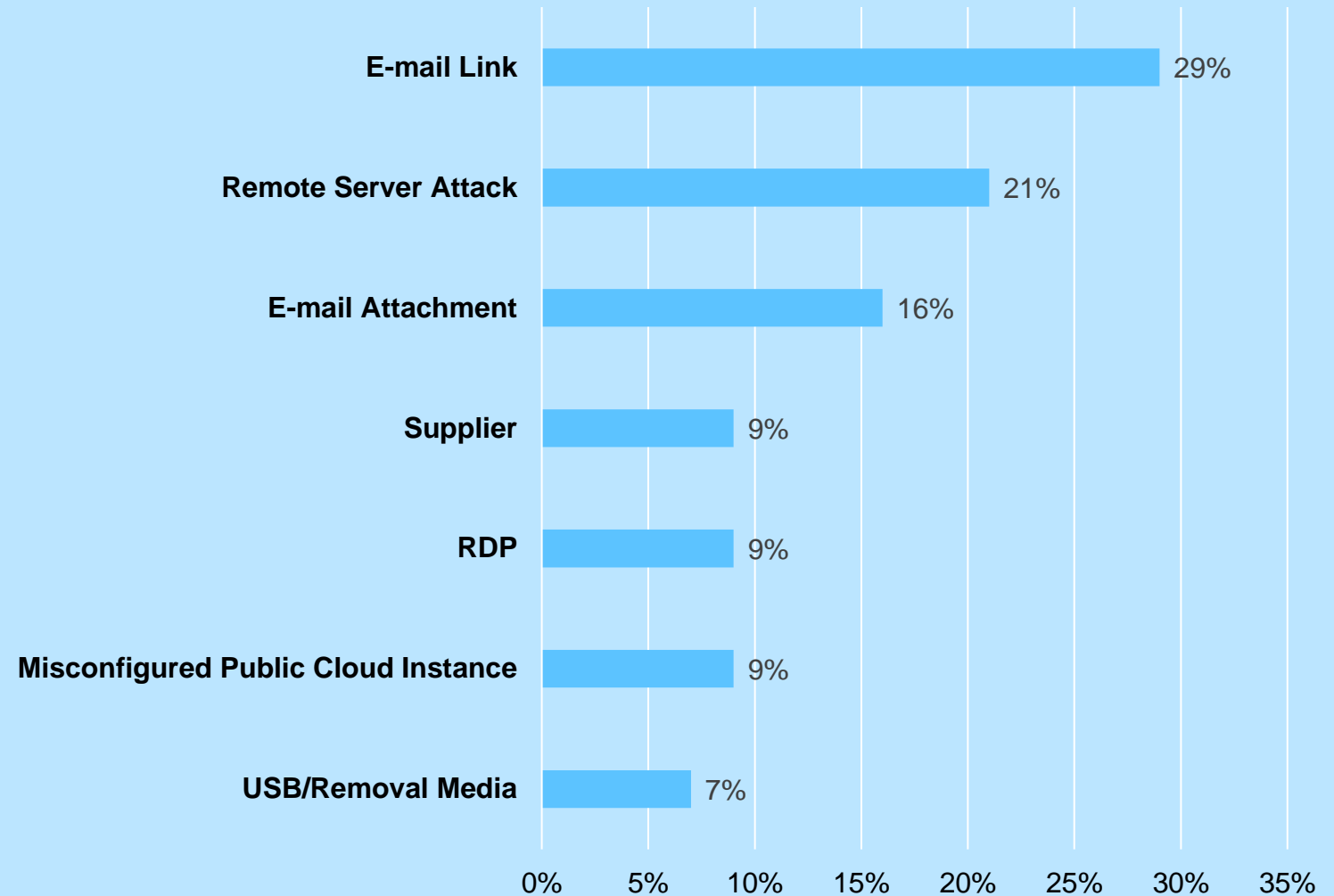
10X

Downtime and recovery time

Cost to remediate is10 times the average ransomware payment

*Sophos report survey data of 5,400 IT manager on "The State Of Ransomware 2021" Average cost was for U.S. companies.
** Standard and Poor's report.

Ransomware attack techniques*

Ransomware attack techniques

- E-mail Link — 29%
- Remote Server Attack — 21%
- E-mail Attachment — 16%
- Supplier — 9%
- RDP — 9%
- Misconfigured Public Cloud Instance — 9%
- USB/Removal Media — 7%

*Sophos report survey data of 5,000 IT manager on "The State Of Ransomware 2020"

NetApp can help

Criminals want your data!

NetApp knows how to protect it.

Identify

- Assess your data protection and security posture
- Classify type of data, location, and permissions

Protect

- Block malicious data from being written to disk
- Create granular, immutable copies to thwart infection
- Prevent data deletion with indelible data copies

Detect

- Monitor user behavior for suspicious activity
- Detect storage behavior anomalies

Respond

- Initiate NetApp® Snapshot™ copies if an attack is identified
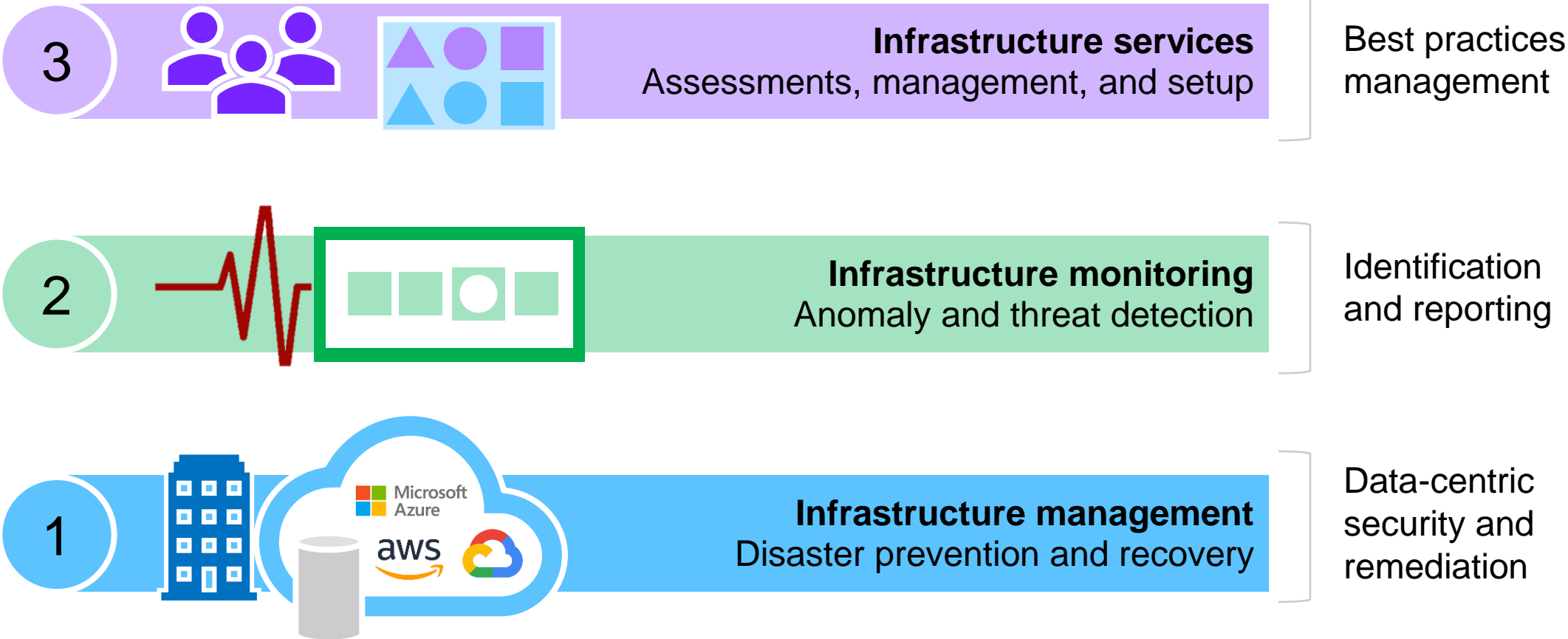- Block malicious user accounts

Recover

- Restore data in minutes and bring applications back online
- Apply intelligent forensics to identify the source of the threat

NetApp

User Endpoints

Network

Applications
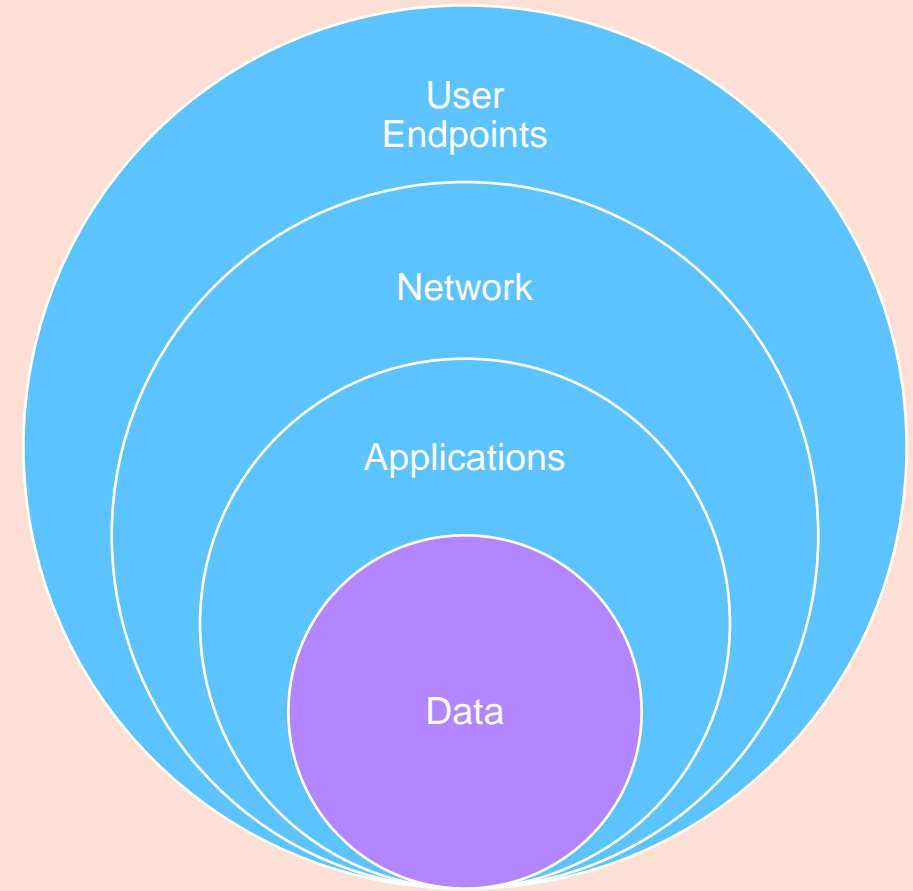
Data

NetApp delivers data-centric ransomware protection

NetApp helps users protect their data effectively through active management, monitoring, and remediation.

3 **Infrastructure services**
Assessments, management, and setup

Best practices management

2 **Infrastructure monitoring**
Anomaly and threat detection

Identification and reporting

1 **Infrastructure management**
Disaster prevention and recovery

Data-centric security and remediation

NetApp ONTAP powers your Zero Trust architecture

Native ransomware detection, protection, and recovery across your hybrid cloud

Protect	Detect	Recover
• Block malicious files before they are written to disk.	• Identify anomalous storage behavior that can indicate malware attacks.	• Recover data in seconds with in-place Snapshot copies.
• Create read-only NetApp® Snapshot™ copies to thwart file infection.	• Detect suspicious file access patterns with on-box anti-ransomware analytics.	• Restore data quickly from efficient remote copies, or fail over to remote storage.
• Establish a "logical air gap" to prevent unwanted backup deletion with NetApp SnapLock® write once, read many (WORM) volumes.	• Integrate with NetApp Cloud Insights or third-party user behavior analytics solutions.	• Analyze logs and apply file level forensics to isolate the threat.

NetApp integrated data protection for rapid recovery

NetApp® ONTAP® to ONTAP

- Highly efficient array-based data protection
- Native format that enables reuse of secondary data

+

ONTAP to object

- Cost-effective backup/archiving
- Back up to object for simplicity and affordability
- Available cloud service
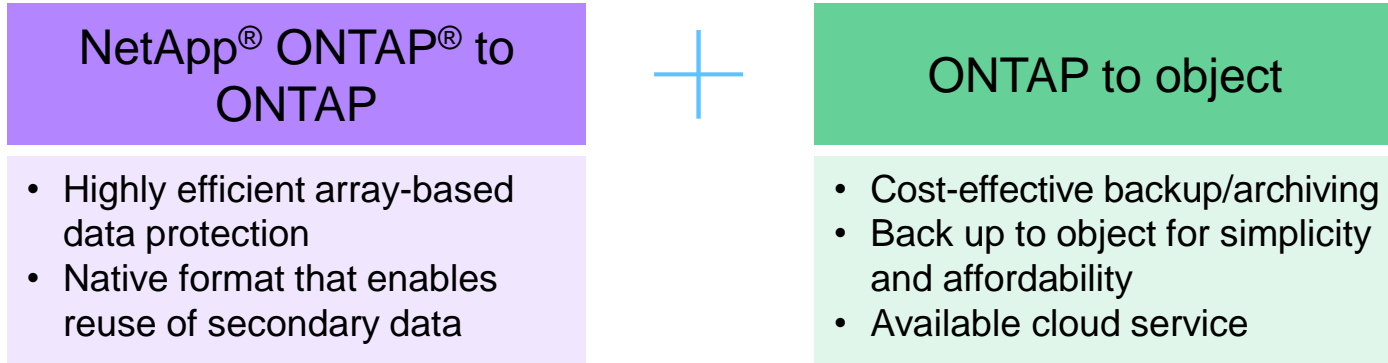
NetApp Cloud Manager

ONTAP 9 → NetApp SnapMirror® → ONTAP 9 → Cloud Backup → StorageGRID®

aws
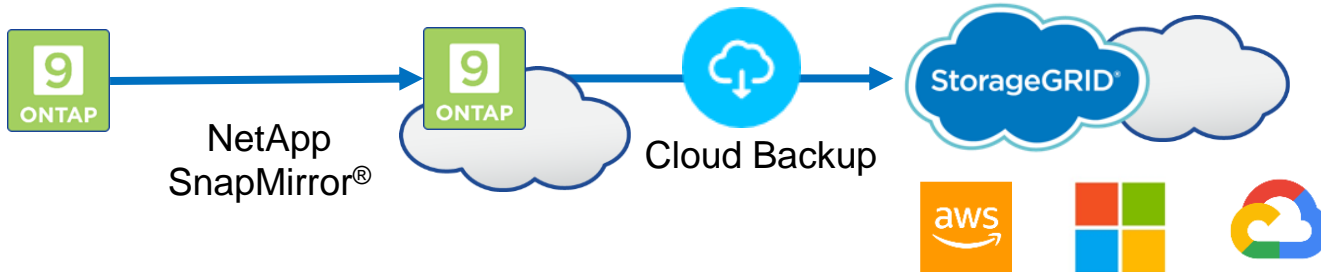
Supported by leading backup software vendors

Benefits
Fully redundant hybrid cloud
File and block protection
Common API/UI
End-to-end data efficiencies
Backup and tiering to object
Unified backup and DR
Data reuse

Microsoft Azure
aws

Active IQ Digital Advisor

Active IQ® Ransomware Defense

A set of prescriptive wellness checks to help protect customers against ransomware and to recover quickly if they are impacted.

Checks cover Snapshot™ count, retention, and auto delete settings, FPolicy, and encryption.
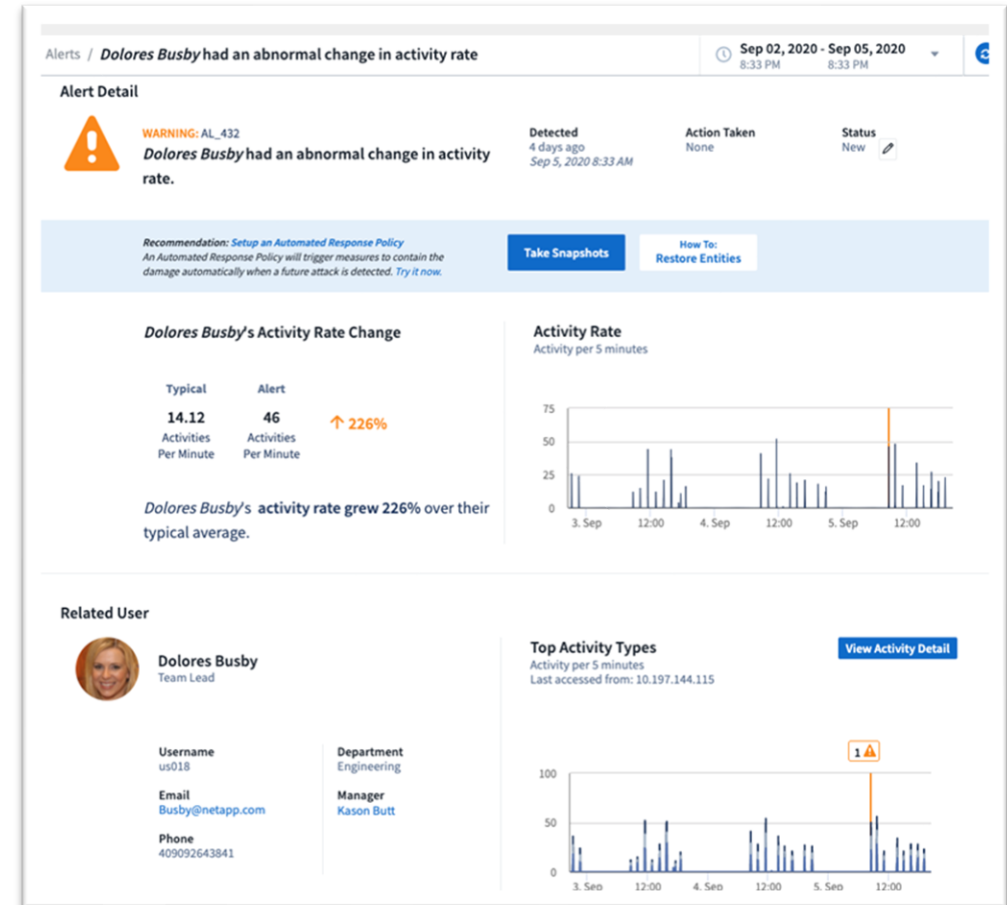
NetApp
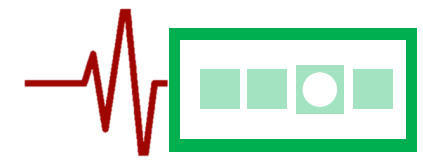
Secure your data – Cloud Insights and Cloud Secure

User anomaly and threat detection

- Detect ransomware attacks before it's too late.

- Minimize the impact of an attack with automatic Snapshot data recovery point.

- Gain visibility into malicious user activity and identify potential policy risks.

- Easily satisfy audit reporting requirements, saving time and money.

- Simple SaaS solution, rapid time to value, no upgrades, scalable from single departments to global enterprises.

"We recently experienced a ransomware event, and when we saw what Cloud Insights' Ransomware Detection provides, we were sold."
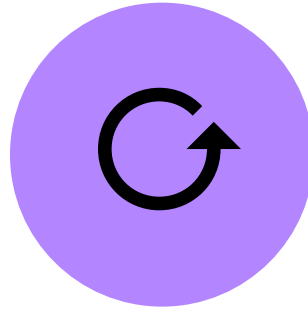
—Director of IT, Transportation Company

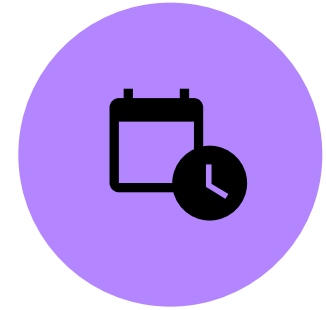# NetApp Data Protection and Security Assessment

Assess your NetApp® ONTAP® environment and prepare for security threats, on premises and in the cloud.
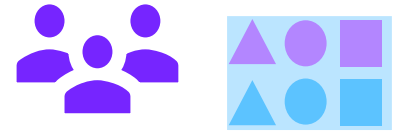
Determine data protection and security readiness before a threat occurs.

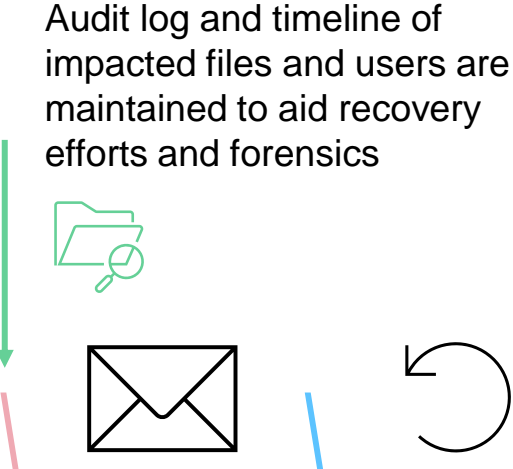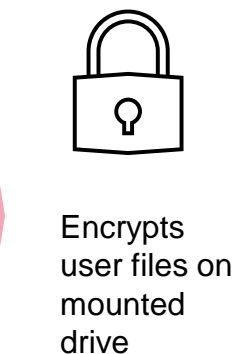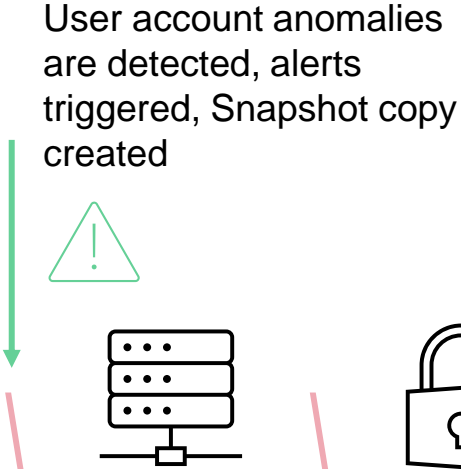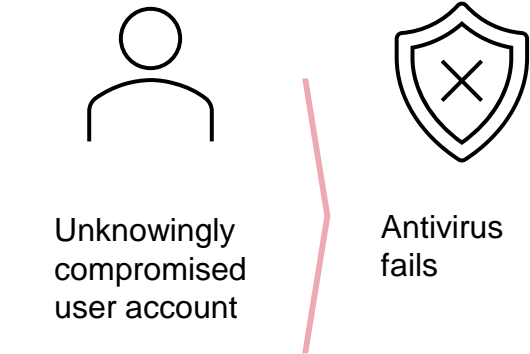**Recover faster** when an attack happens, to reduce data loss and disruption.

Stay up to date with security changes to avoid future risks

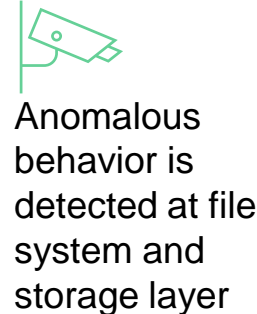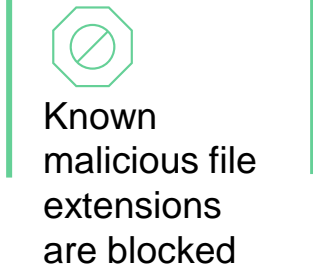**NetApp Professional Services**

Anatomy and prevention of a ransomware attack

Cloud Insights user monitoring

User account anomalies are detected, alerts triggered, Snapshot copy created

Audit log and timeline of impacted files and users are maintained to aid recovery efforts and forensics

ONTAP® data management

Unknowingly compromised user account

Antivirus fails

Malware delivered, launches child processes

Connects with command and control server to deliver information and get instructions

Encrypts user files on mounted drive

Ransom note delivered

Data restored

Ransom avoided

Immutable Snapshot™ copies minimize data loss

Known malicious file extensions are blocked

Anomalous behavior is detected at file system and storage layer

SnapLock® indelible copies prevent file encryption and backup deletion

SnapRestore® enables rapid data recovery from clean Snapshot copies

Leading technology partners integrate with NetApp

Enhance your NetApp Zero Trust architecture with powerful partners

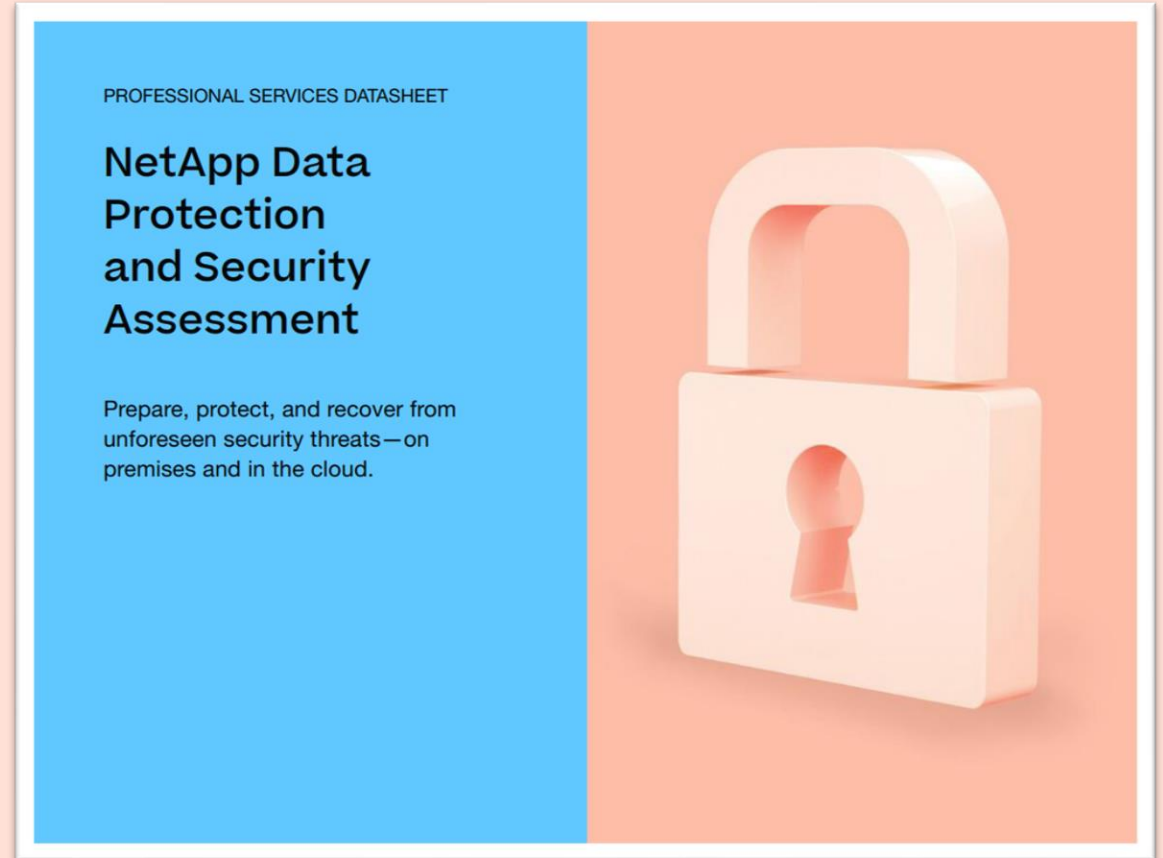| Data protection	User behavior	Auditing and logging
Integration with NetApp® ONTAP® Snapshot™ and efficient replication with SnapMirror®	Integration with FPolicy APIs to deliver intelligent view of file and user behavior	Integration with forensic analytic syslog or SIEM tools

Now is the time to talk to NetApp

ONTAP® customers, schedule your Data Protection and Security Assessment today.

New to NetApp? Take a test drive with a NetApp® Lab on Demand focused on Zero Trust architectures.

https://www.netapp.com/test-drives/#zerotrustontap

PROFESSIONAL SERVICES DATASHEET

NetApp Data Protection and Security Assessment

Prepare, protect, and recover from unforeseen security threats—on premises and in the cloud.

Data Protection and Security Assessment

NetApp unlocks the best of cloud

■ NetApp