Lenovo NetApp

NetApp INSIGHT 2023

AIways On

数据存储与管理前沿技术系列课程

第五讲：Fight ransomware with zero trust and NetApp advanced security technologies

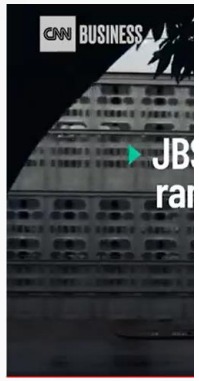
2023年12月5日

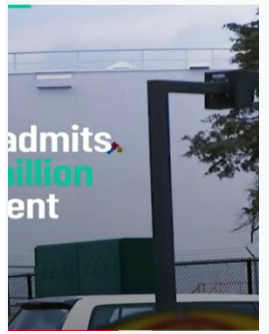
Lenovo NetApp

目录

Contents

不要因为被勒索而成为头条新闻！





每日经济新闻 I

+关注

23-11-17 11:19 来自 微博网页版

#工行在美全资子公司遭勒索病毒攻击#【揭秘"攻击"工行在美全资子公司的"勒索病毒"！业内：就像自己的抽屉被别人上了锁！】美东时间11月8日，"宇宙第一大行"中国工商银行股份有限公司在美全资子公司——工银金融服务有限责任公司（以下简称"ICBCFS"）被"网络狂徒"盯上了。

日前，ICBCFS在官网发布声明称，由于遭勒索软件攻击，导致部分系统中断。ICBCFS表示，发现攻击后立即切断并隔离了受影响系统，已展开彻底调查并向执法部门报告，正在专业信息安全专家团队的支持下推进恢复工作。

至于业务受影响程度，ICBCFS在声明中提到，已成功结算周三执行的美国国债交易和周四完成的回购融资交易。中国工商银行及其他国内外附属机构的系统未受此次事件影响，中国工商银行纽约分行也未受影响。

这起事件的主角之一，所谓的"勒索病毒"是什么？有业内人士比喻称，"如果自己存放重要资料的抽屉被他人上了锁，锁上贴着字条——'交赎金拿钥匙'，这就是'勒索病毒'。"

勒索软件每年使企业损失数百万美元

$1.4M

Average cost
to remediate a ransomware attack in 2021

$3B

Insurance premiums
92% annual growth

1.7X

The downtime and recovery time
cost to remediate is 1.7 times the average ransomware payment

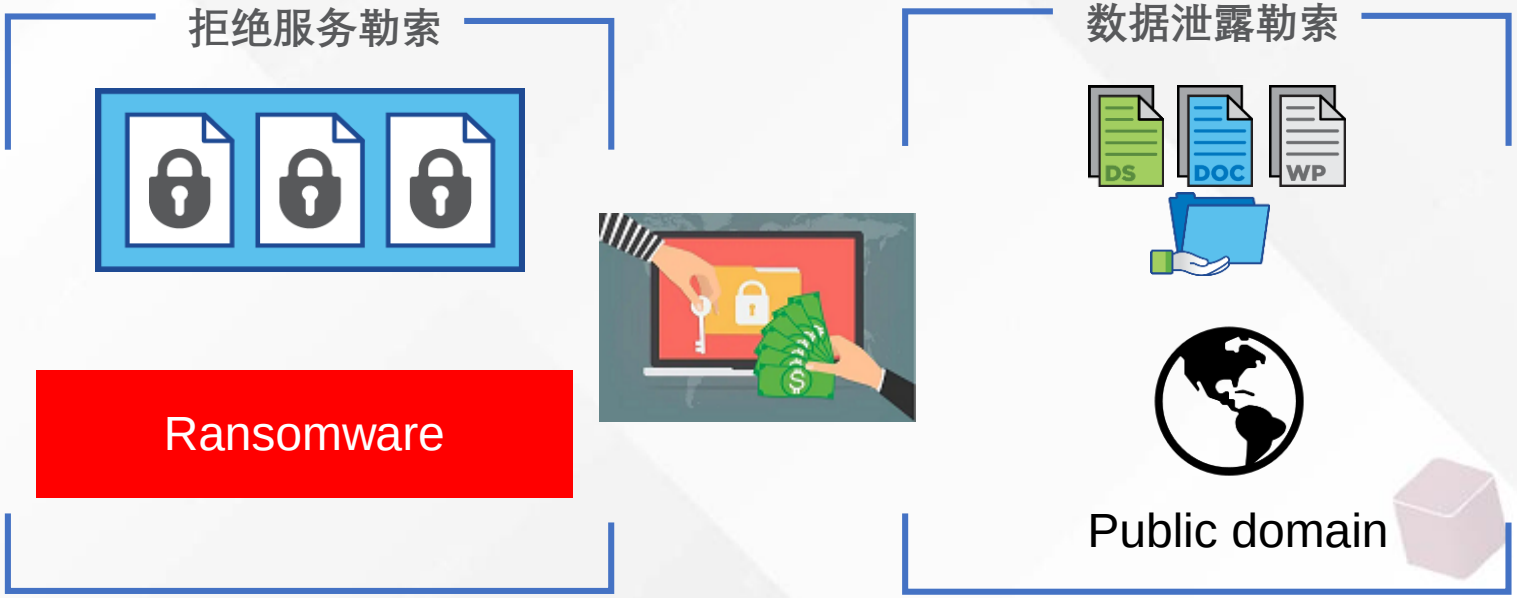
勒索病毒及其主要类型

勒索病毒是一种极具破坏性、传播性的恶意软件，主要通过钓鱼邮件、网页挂马等形式传播，或利用漏洞、远程桌面入侵等发起攻击而被植入，利用多种密码算法加密用户数据，恐吓、胁迫、勒索用户支付赎金。

表现形式分类：

1. **文件加密类** – 加密文件
2. **数据窃取类** – 公开数据
3. **系统加密类** – 不能启动
4. **屏幕锁定类** – 不能登录

最终结果：



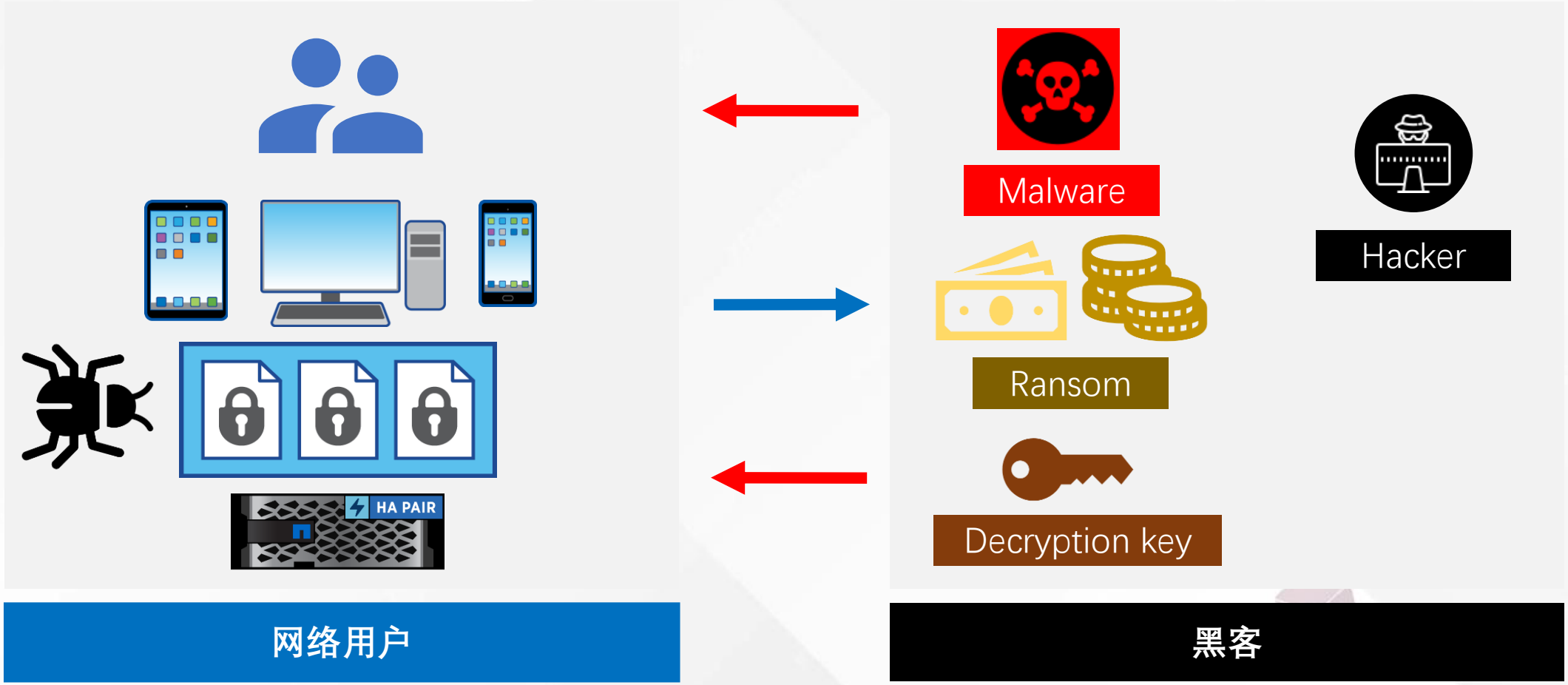
勒索病毒典型攻击流程

1. 探测侦察阶段
收集基础信息
发现攻击入口

2. 攻击入侵阶段
部署攻击资源
获取访问权限

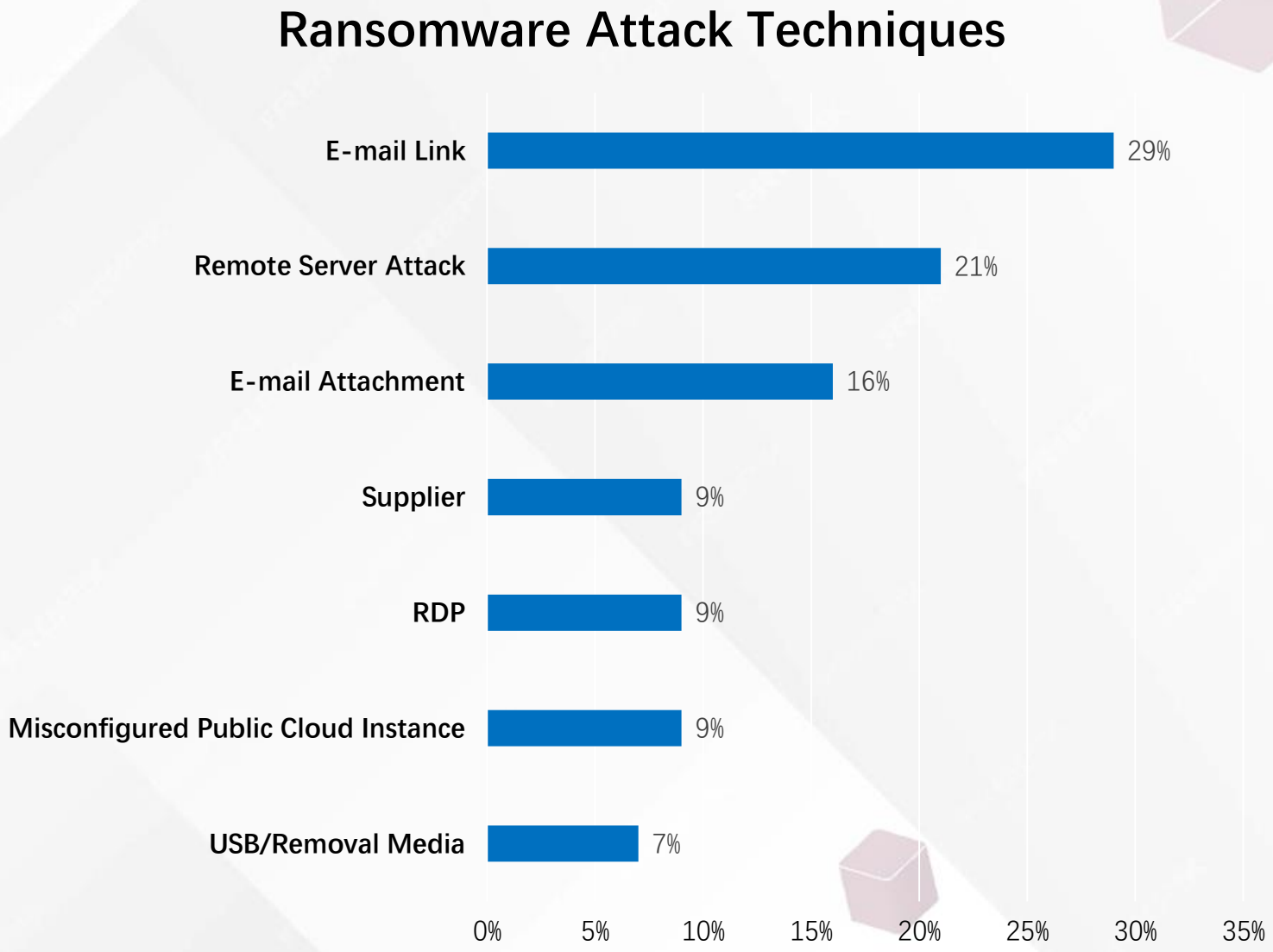
3. 病毒植入阶段
植入勒索病毒
扩大感染范围

4. 实施勒索阶段
加密窃取数据
加载勒索信息



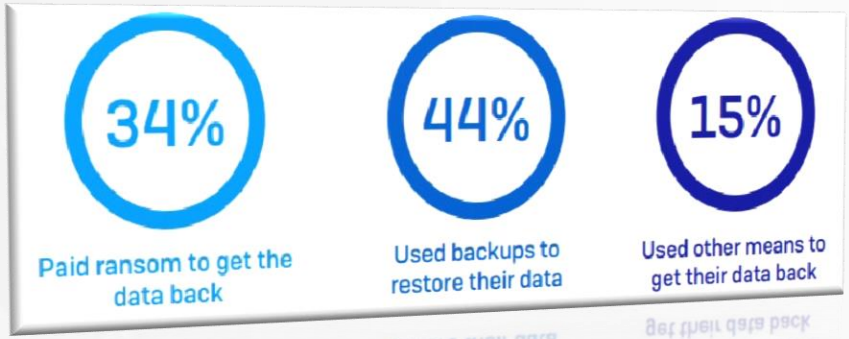
勒索病毒传播形式

Ransomware Attack Techniques As Spreading Mode



构建勒索病毒攻击安全防护框架

探测侦察 → 攻击入侵 → 病毒植入 → 实施勒索



1 事前积极预防

- 制定应急预案
- 加强安全管理
- 部署安全产品
- 加强安全意识
- 做好数据备份

2 事中应急响应

- 隔离感染设备
- 排查感染范围
- 攻击事件研判
- 尝试病毒破解

3 事后加固补漏

- 利用备份数据恢复
- 更新安全管理措施
- 加强安全隐患修补
- 恢复感染设备使用

Lenovo NetApp

目录

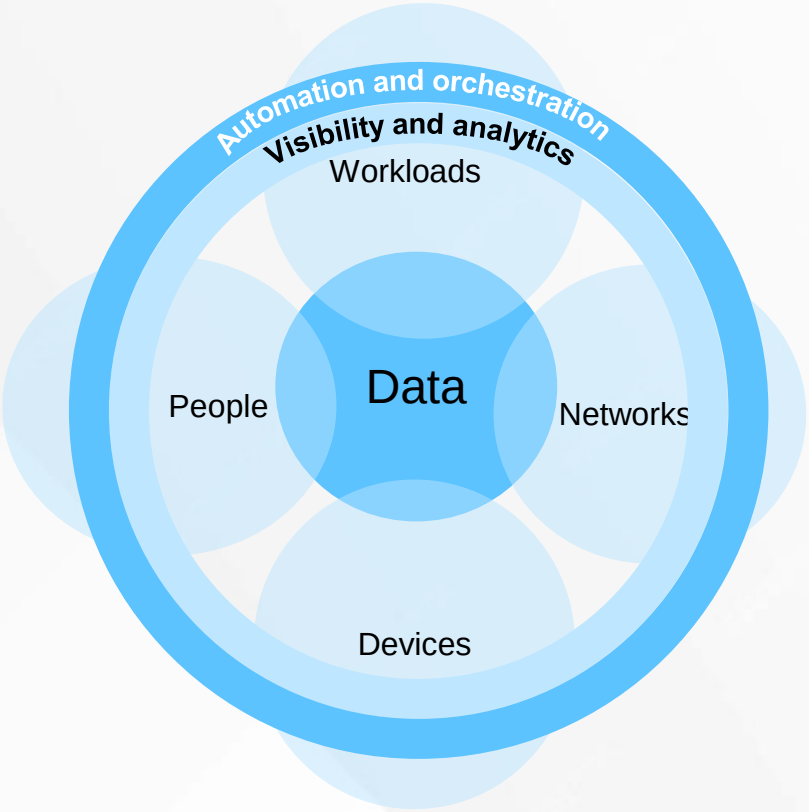
Contents

零信任原则

- Zero Trust - 由内而外设计，核实并从不信任
  - Old model: Trust but verify and outside-in approach
- A Zero Trust architecture - 使用微内核从内部确定威胁
  - Micro-core 是由一套全面的控制措施保护的数据、服务、应用程序或资产的内部定义

基本原则:

- 显式验证
- 使用最低权限访问
- 假设违背



零信任体系结构 – 简化版

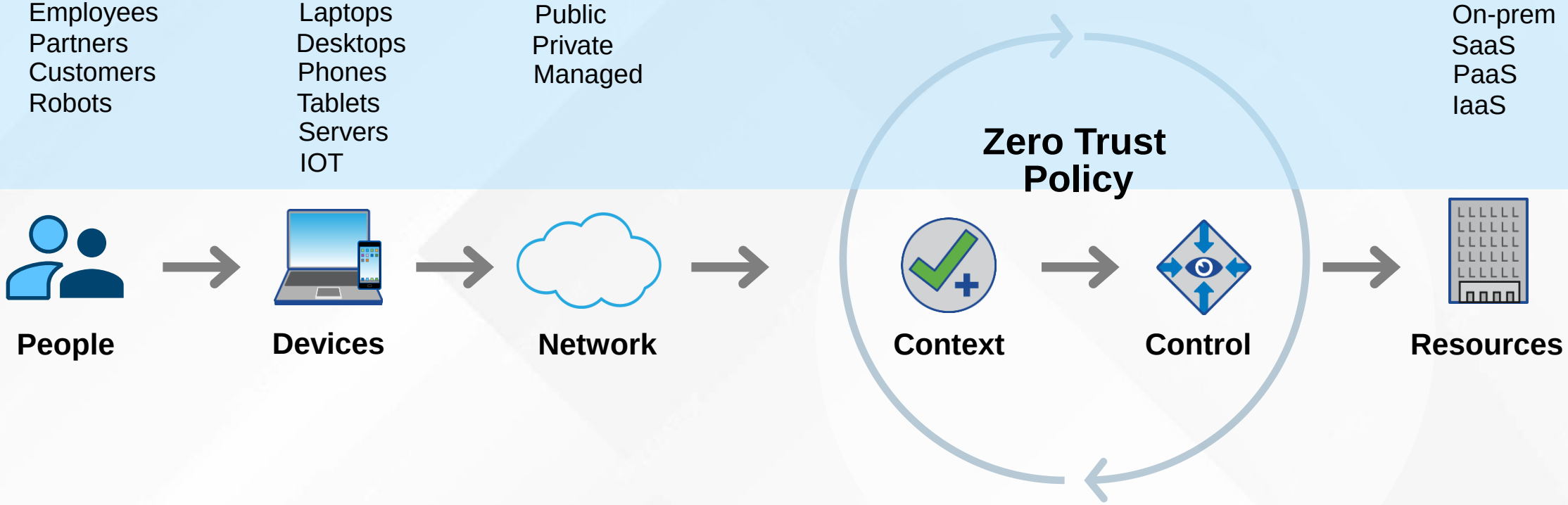
Scope

Employees
Partners
Customers
Robots

Laptops
Desktops
Phones
Tablets
Servers
IOT

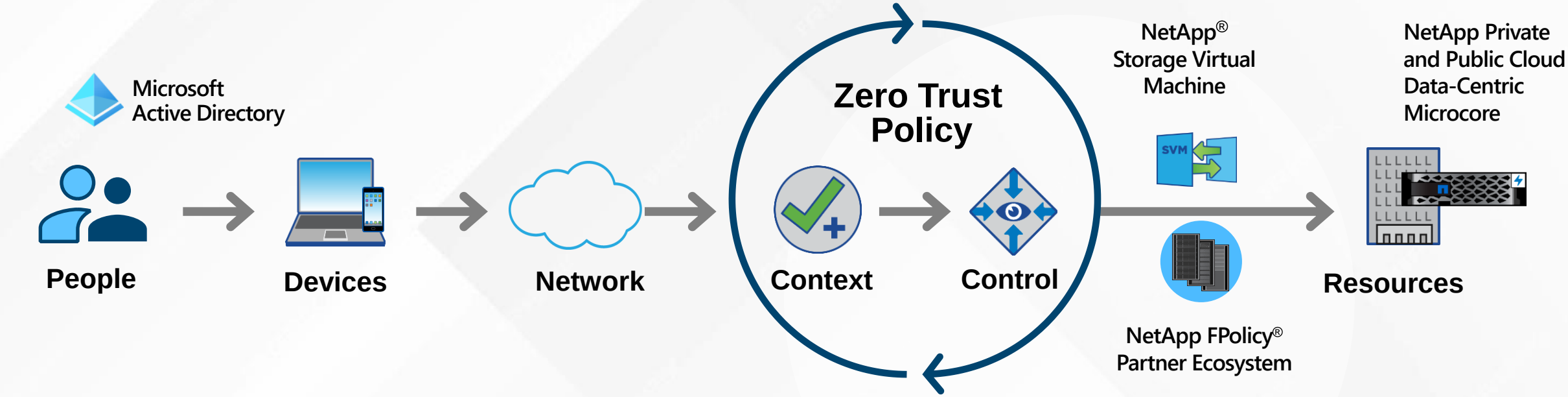
Public
Private
Managed

On-prem
SaaS
PaaS
IaaS



智能化、自动化

零信任体系结构 – 结合功能和特性



智能化、自动化

NetApp Zero Trust FPolicy Engine for User Behavioral Analytics

NetApp Encryption In Flight & At Rest

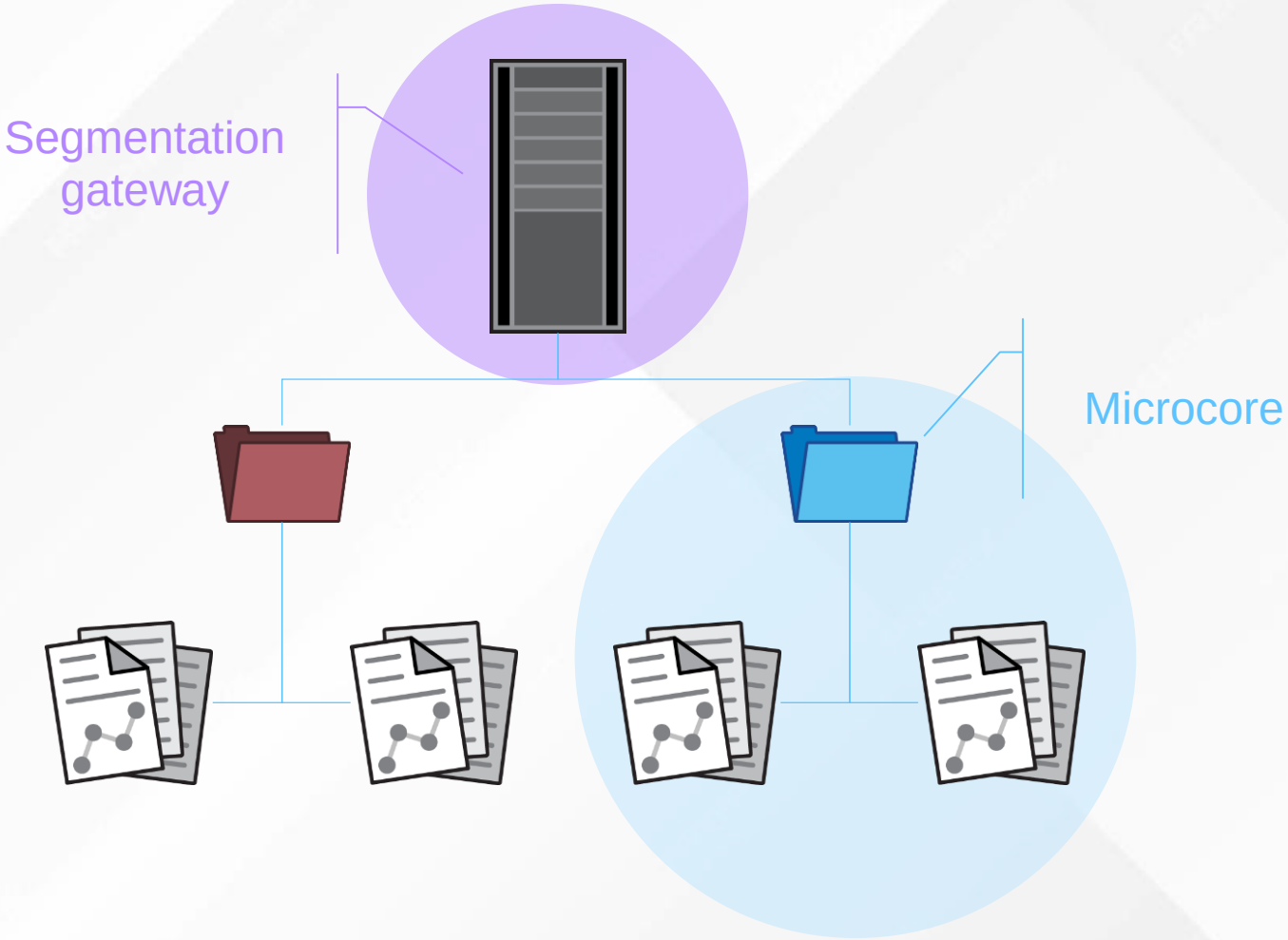
NetApp Multifactor Authentication

Hardening Guide & Solution for Ransomware

NetApp SnapShots™ and Immutable WORM Storage

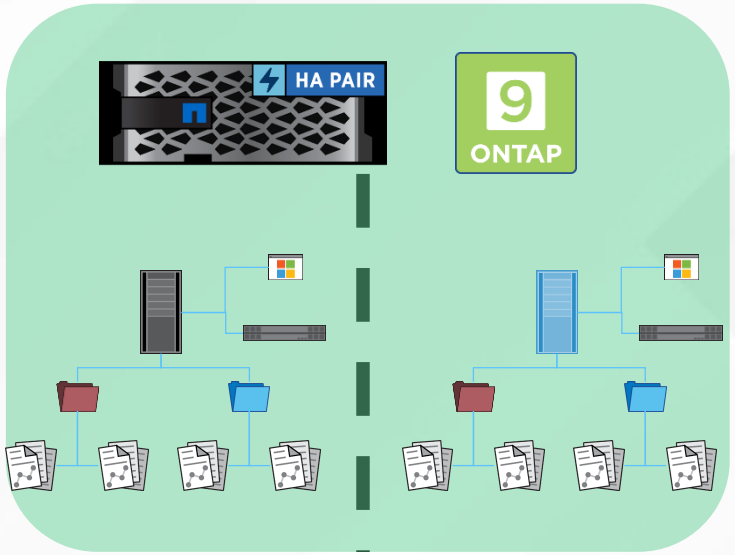
Network Virtualization and Storage Segmentation

由内而外构建：以数据为中心的微核心



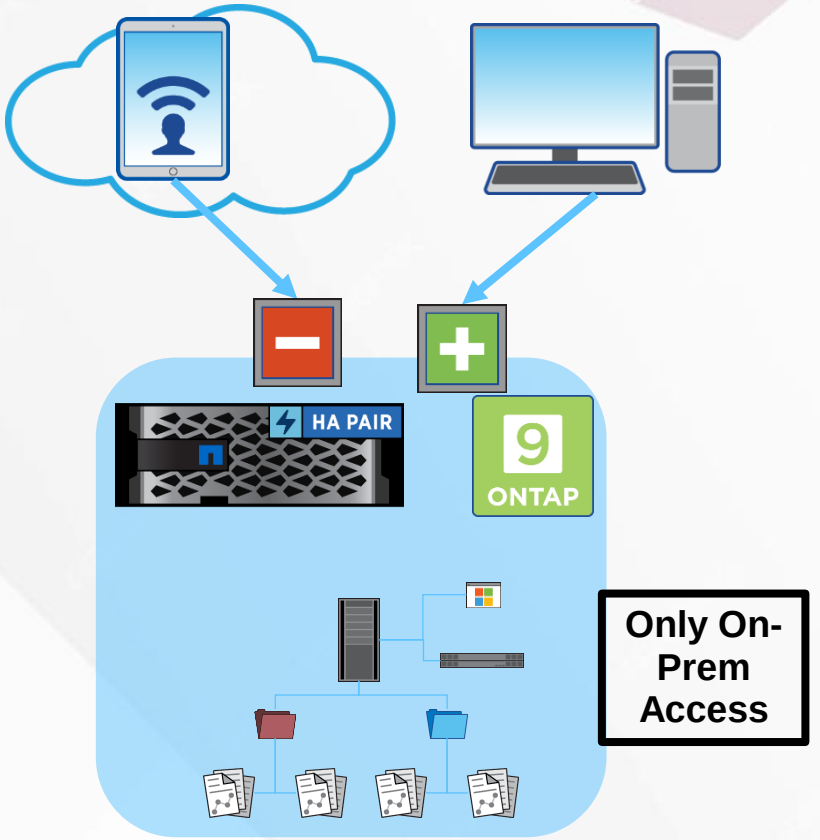
- **Microcore** defines the smallest unit that you are trying to protect – which is **data**
- **Segmentation gateway** determines what is accessible – which is the **storage virtual machine (SVM)**
- SVM allows access to data through permissions and control lists

防止数据微核心的攻击



Storage segmentation

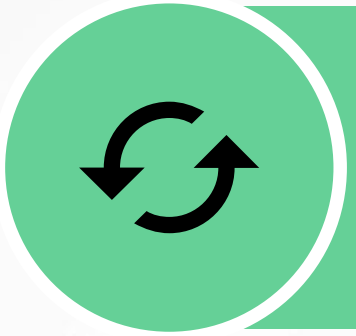
Network virtualization



Attribute-based access controls

NetApp如何帮助抵御勒索软件

Detection and prevention



Remediation and restoration

检测和预防 – 事前事中分层防御

Detection and prevention

NetApp FPolicy

- Common ransomware file extension blocking in native mode
- File and user behavioral analytics in external mode

NetApp® ONTAP® autonomous ransomware protection (ARP)

- Automatic detection of ransomware in 9.10.1 and later

监控异常并直观展示

- NetApp Active IQ® Unified Manager alerting
  - NetApp Snapshot™ copy rate of change and decrease in storage efficiency loss alert
- NetApp Active IQ® and System Manager insights
  - ”Ransomware defense” best practices

FPolicy – 零信任引擎

Detection and prevention

Benefits:

- Granular file-based event notification
- Storage-based intrusion detection system (IDS)

Modes:

- External
- Native

Integration with security information and event management (SIEM) partners supports:

- Log management and compliance reporting
- Real-time monitoring and event management

CIFS/NFS requests

NetApp® FPolicy partner ecosystem

CLEONDRIS

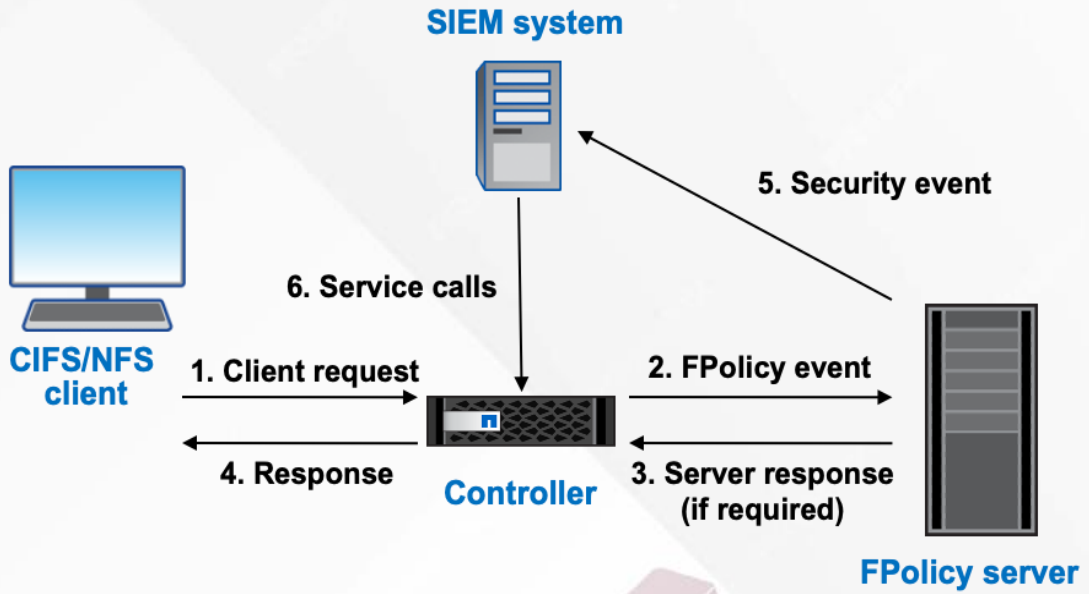
NetApp Cloud Insights

ProLion

STEALTHbits TECHNOLOGIES

symantec.

VARONIS



FPolicy – 文件扩展名黑名单

Detection and prevention

- FPolicy is included with every NetApp® ONTAP® system, and offers defense against basic ransomware attacks
- Commonly used encryption extensions can be blocked from ONTAP NAS exports
- System Manager and NetApp® BlueXP™ now offer simple enablement of this feature with a predefined list of common ransomware file extensions

Blue XP

System Manager

ONTAP自主勒索软件防护 – 1

Detection and prevention

Available in NetApp® ONTAP® 9.10.1+ for NAS, not for S3 and SAN

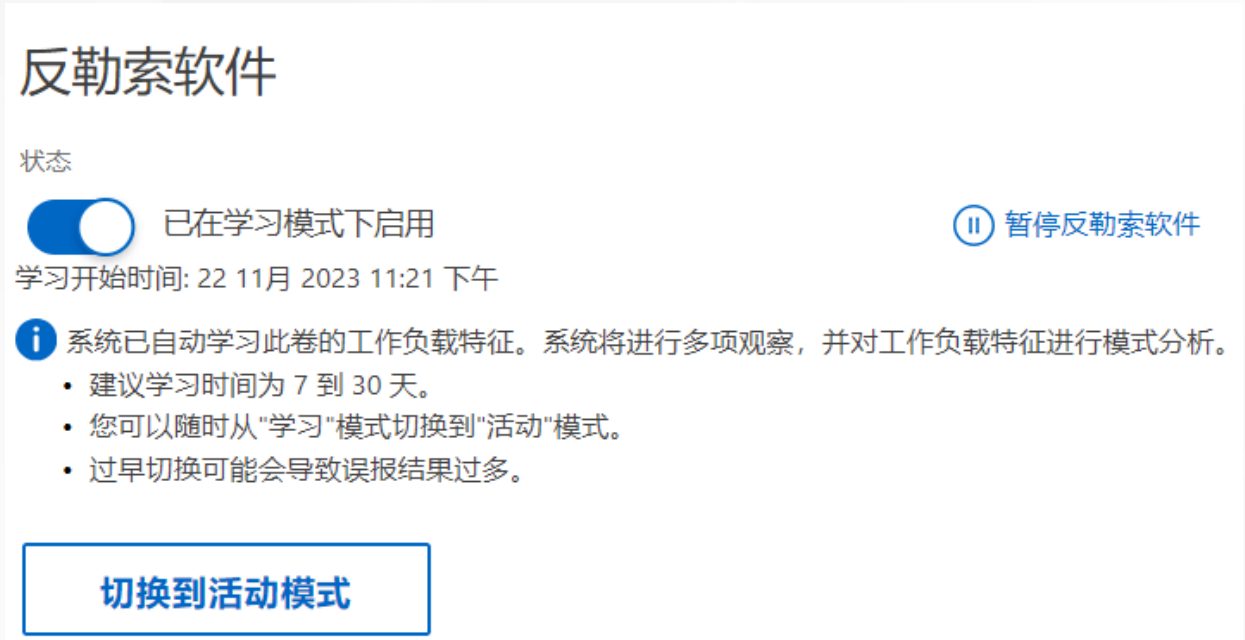
Licensed feature

NetApp Onbox ML analytics engine leverages volume file **entropy**, file **extension** types, and file **IOPS**

Learning mode (min. 7 days, recommended 30 days).

Beginning with ONTAP 9.13.1, ARP automatically determines the optimal learning period interval and automates the switch, which may occur before 30 days.

ONTAP releases	License
ONTAP 9.11.1 and later	Anti_ransomware
ONTAP 9.10.1	MT_EK_MGMT (Multi-Tenant Key Management)，自动升级



ONTAP自主勒索软件防护 – 2

Detection and prevention

Alerts admin via EMS, SysMgr, NetApp Active IQ® Unified Manager

- Does not disrupt I/O-only alerts on suspect activity
- ONTAP does not send alerts about low threats, can modify alerts settings beginning in ONTAP 9.14.1.

Automatically takes NetApp Snapshot™ copy

- The ARP Snapshot uses the anti-ransomware-backup tag
- Snapshot is identifiable by its name, for example Anti_ransomware_backup.2022-12-20_1248
- ARP Snapshots are retained for a minimum of **two** days.
- Beginning with ONTAP 9.11.1, you can modify the Snapshot options.
  - `arw.snap.max.count (6)`
  - `arw.snap.create.interval.hours (4)`
  - `arw.snap.normal.retain.interval.hours (48)`
  - `arw.snap.max.retain.interval.days (5)`
  - `arw.snap.create.interval.hours.post.max.count (8)`
  - `arw.surge.snap.interval.days (5)`
- Admin can determine if it's a false positive
- in addition to existing protection from **scheduled** Snapshot copies.

Additional layer of detection and ransomware protection

- Better together with FPolicy

ONTAP自主勒索软件防护 – 3

Detection and prevention

ARP 适合场景

- Databases on NFS storage
- Windows or Linux home directories
- Images and video

ARP 不适合场景

- Workloads with a high frequency of file create or delete
- unusual surge in file create, rename, or delete
- Workloads where the application or the host encrypts data

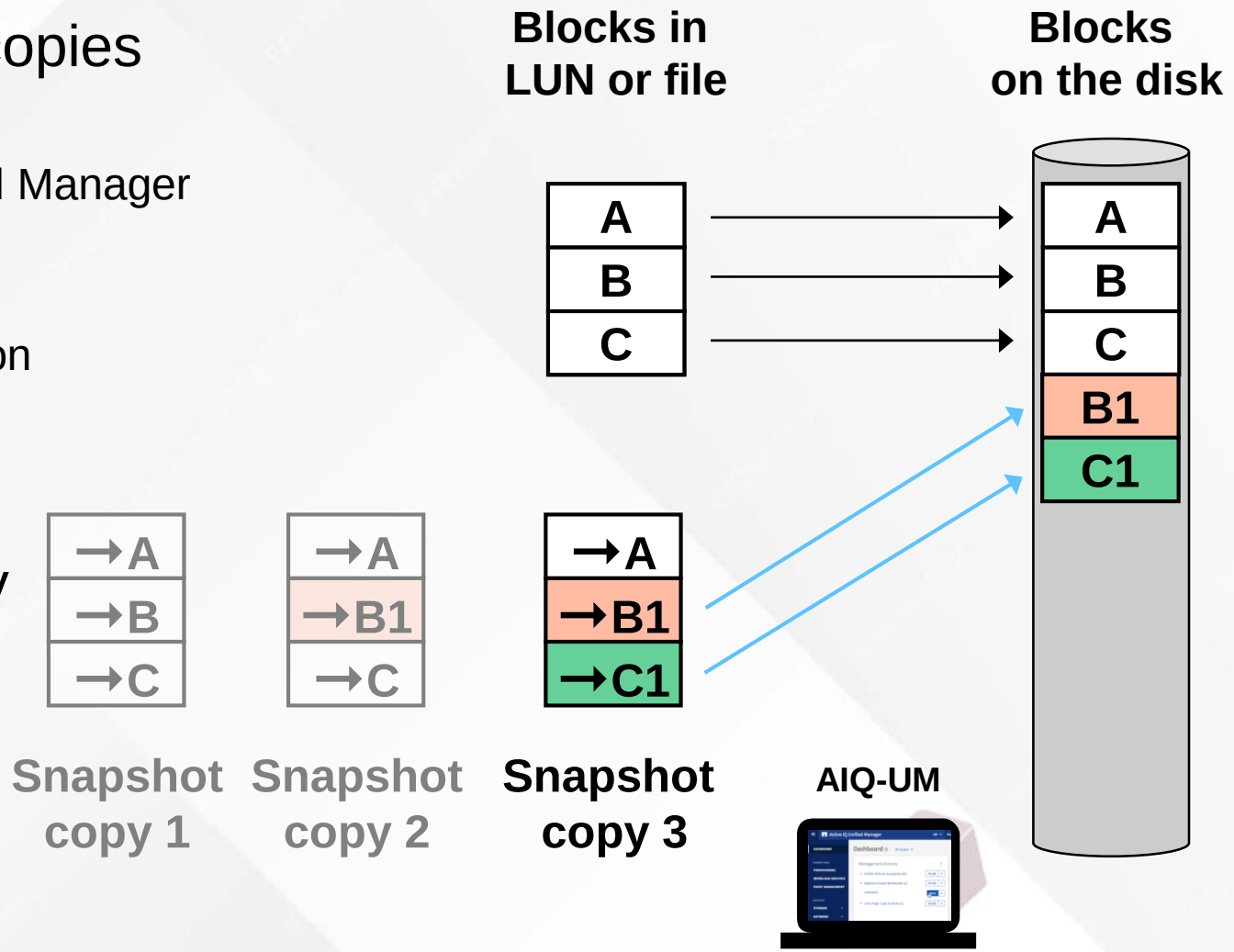
	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1
Volumes protected with Asynchronous SnapMirror	✓	✓	✓		
SVMs protected with Asynchronous SnapMirror	✓	✓	✓		
SVMs enabled for data migration	✓	✓	✓		
FlexGroup volumes	✓	✓			
Multi-admin verification	✓	✓			

负载特性	每节点推荐卷	超限性能下降
Read-intensive or the data can be compressed.	150	4% of maximum IOPS
Write-intensive and the data cannot be compressed.	60	10% of maximum IOPS

使用快照拷贝战胜勒索软件

Remediation and restoration

- Monitor NetApp® Snapshot™ copies
  - Abnormal growth?
  - Monitor with NetApp Active IQ® Unified Manager
- Rapid recovery!
  - Restore Snapshot copy prior to infection
  - Restore hundreds of TBs in seconds
  - Can leverage FlexClone
- Snapshot copies are read only
  - Can't be infected by ransomware
  - Can be deleted though

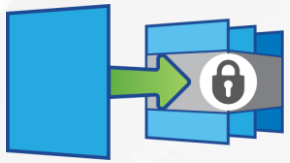


防止恶意删除快照

Remediation and restoration

NetApp® SnapLock® compliance (SLC)

- Licensed feature of NetApp ONTAP®



Ransomware recovery use case

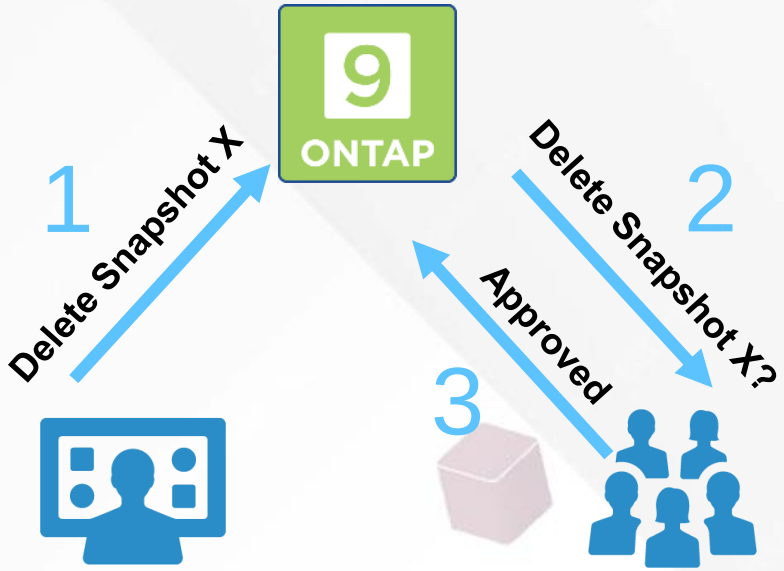
- Don’t lock primary data
- Combine with SnapVault to lock backups
- SLC provides immutable NetApp Snapshot™ copies for NAS and SAN on SLC volumes
- Prevents rogue admins from deleting vaulted Snapshot copies to recover from ransomware

Tamper-proof Snapshot locking on primary storage

- **New In ONTAP 9.12.1, leveraging SLC**
- Works on any volume (not SLC volumes only)
- Manual Snapshot locking or automatic via schedule
- Create FlexClone from Tamper-proof snap for rapid restore

Multi-admin verification (MAV)

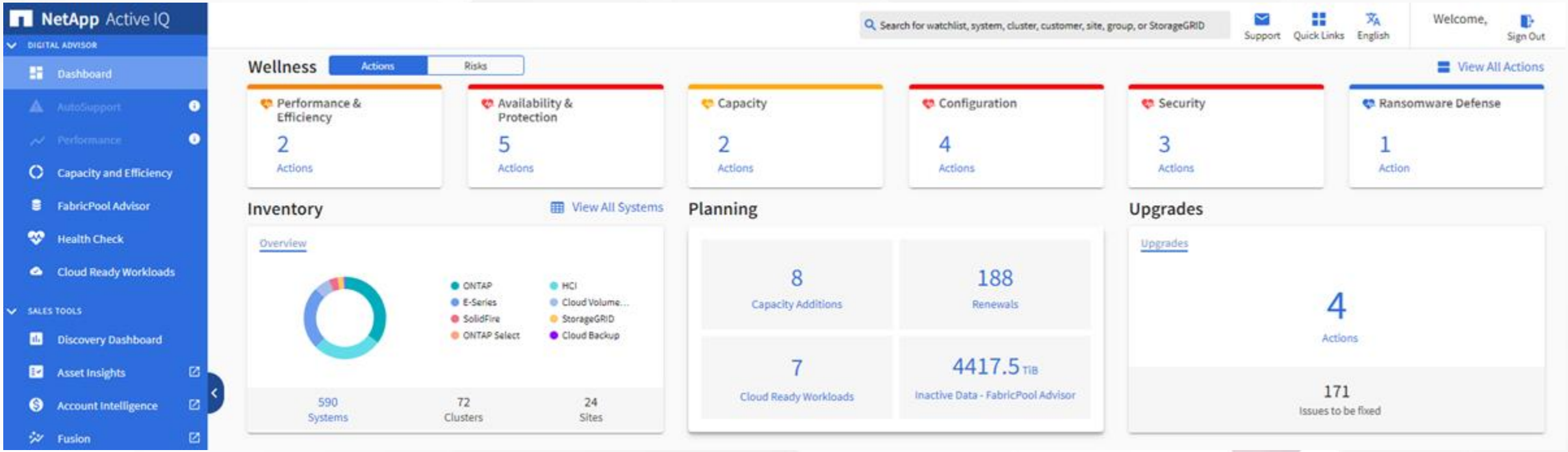
- Built-in feature of NetApp ONTAP® (no license required)
- Administrator accounts have the ability to run destructive commands like deleting Snapshot copies
- Requires N-number of approvals for all or a set of commands before allowing the command to take
- Snapshot deletion for unlocked Snapshot copies will require multiple admin approval



Active IQ Digital Advisor

Ransomware defense

- A set of prescriptive wellness checks to help protect customers against ransomware and recover quickly if they are impacted.
- Checks cover NetApp® Snapshot™ count/retention/auto-delete settings, Fpolicy, and encryption.



NetApp Cyber Resilience

Advanced data protection and data security

Protect		Detect	Respond	Recover
Identify	Protect	Detect	Respond	Recover
				
• Automatically discover and classify data • Easily inventory infrastructure and system resources • Identify and optimize volume permissions • Automatically apply system health recommendations	• Protect data with efficient, immutable, and indelible copies • Automatically block malicious files • Encrypt data in flight and at rest • Protect against unwanted access with multi-factor authentication and role-based access • Block rogue actors with multi-admin verification	• Monitor storage behavior to identify anomalies • Detect slow-moving encryption in your file system • Identify compromised user accounts in real time • Protect against virus / malware attacks • Detect possible bulk data deletion	• Automatically respond to detected threats by creating NetApp® Snapshot™ recovery points • Instantly block user storage access when detecting user behavior anomalies	• Recover terabytes of data in seconds to support rapid operational recovery • Identify what data was impacted and by whom, to support detailed forensic analysis • Support auditing requirements with detailed syslogs exported to SIEM tools

勒索软件保护和恢复服务

NetApp Professional Services

Assess

Assesses current environment

- Determines remediation for potential:
  - ✓ Need for ONTAP Upgrades (9.10.1 or later required)
  - ✓ Gaps in NetApp Native software solutions
  - ✓ Data protection risks
  - ✓ Ability to recover
  - ✓ Discover policies/retention periods

Configure & Manage

Implements and configures NetApp Ransomware tools/ARS

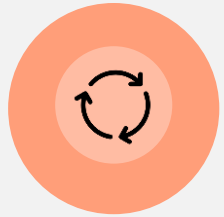
- Cloud Insights/Cloud Secure
- Cloud Data Sense
- SnapMirror/Snap Vault
- SnapLock Compliance/Worm
- SnapCenter
- Advanced Data Encryption
- AIQ/AIQUM
- ONTAP FPolicy
  - White/blacklisting
  - External mode

Delivers high-touch managed services

- 24x7x365 monitoring/triage/remediation of ransomware alerts
- Software tool administration/upgrades
- Create/manage replication policies
- Modify FPolicy configurations
- Perform ONTAP Upgrades as required
- Service level objectives for response

Assists with scoring for cyber security insurance

Recover



Speeds ransomware data recovery

Maintains business continuity and speeds recovery times:

- Data recovery via SnapCenter platform
- Assist in ensuring data is in place to meet customer recovery needs
- Assist in containing ransomware spread
- SnapShot roll back where necessary
- Isolate/Patch/Restore (customer responsibility)

Lenovo
NetApp

目录
Contents

总结

Help with detection, reme
and clean-up from a rans

io can help you secure your
at many layer

- Segmentation / Encryption
- es
- Multi-Factor Authentication
- Autonomous Anti-Ransomware

Microsoft Active Directory

Zero Trust

NetApp Storage Virtual Machine

NetApp Private and Public Cloud Data-Centric Microcore

1

2

3

事前积极预防

事中应急响应

事后加固补漏

- Data Protection & Security Assessment package to provide guidelines to achieve your SLA / SLO

谢 谢!

联想凌拓官方联络方式

官方网站：www.lenovonetapp.com

服务热线：400-828-3001 (呼叫中心)

400-116-0099（销售热线）

官方社交平台账号：

联想凌拓
官方微信

Bilibili联想凌拓
空中沙龙

联想凌拓
渠道微信