Synology®

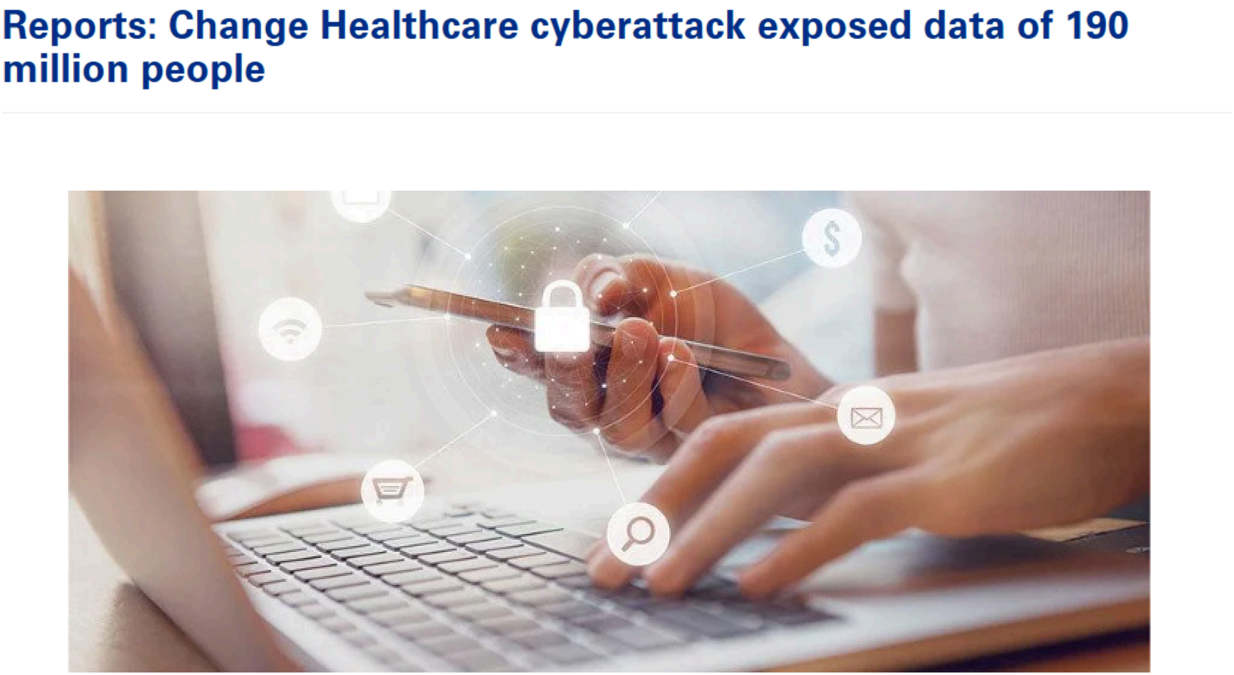
From Disaster Recovery to Cyber Recovery:

6 Key Elements for Enterprise Data Protection Strategy

ANZ Country Manager

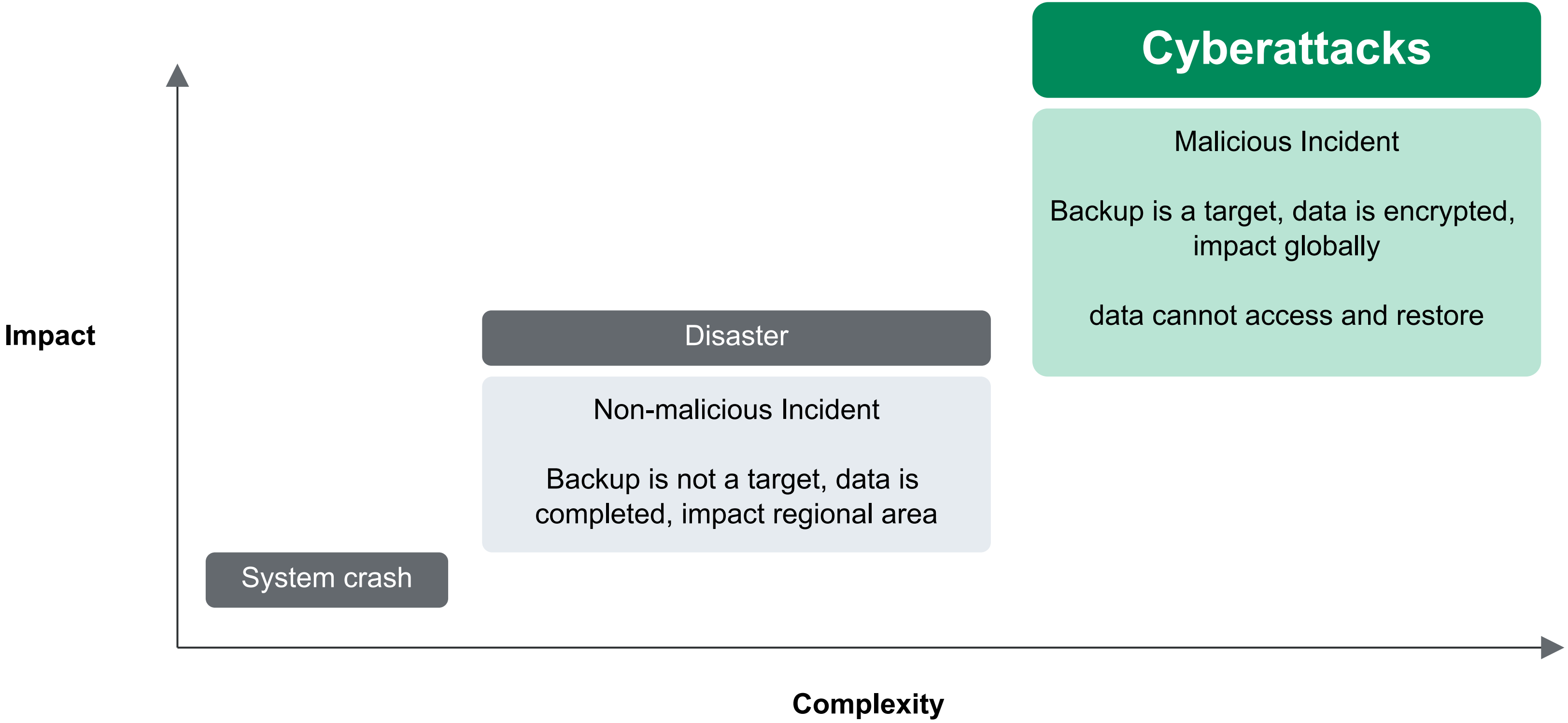
Jasmine Chiu

Increasingly complex and frequent cyberattacks



Reports: Change Healthcare cyberattack exposed data of 190 million people

Trends in Data Protection Positioning



Cyberattacks

Malicious Incident

Backup is a target, data is encrypted, impact globally

data cannot access and restore

Disaster

Non-malicious Incident

Backup is not a target, data is completed, impact regional area

System crash

From Disaster Recovery to Cyber Recovery

	Disaster Recovery	Cyber Recovery
Event	Natural disasters, hardware failures	Ransomware, cyberattacks
Scope	Partial: localized	Comprehensive: entire enterprise or even industry supply chain
Data access	Ability to back up and restore	Unable to back up and restore
Focus	System service availability	Data integrity and confidentiality

Australians Hit With One Cyber Attack Every Second in 2024

Source: Global data breach statistics: a 2024 recap Surfshark

47 million Data Breaches Recorded

Source: Global data breach statistics: a 2024 recap Surfshark

Soaring Data Breach Costs

$4.26m

average cost of a data breach in Australia

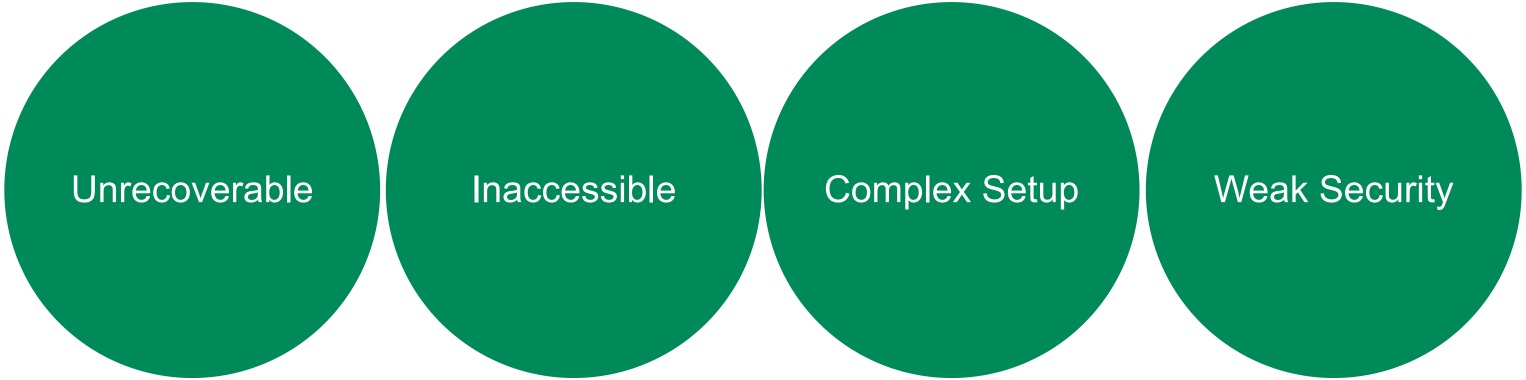
+27%

since 2020

Source: Phishing Emails Targeting Australian Firms Rise by 30% in 2024 (TechRepublic)

What challenges hinder businesses from protecting data?

The Common Blind Spots of Deploying Data Protection



Unrecoverable

Inaccessible

Complex Setup

Weak Security

Before incident

After incident

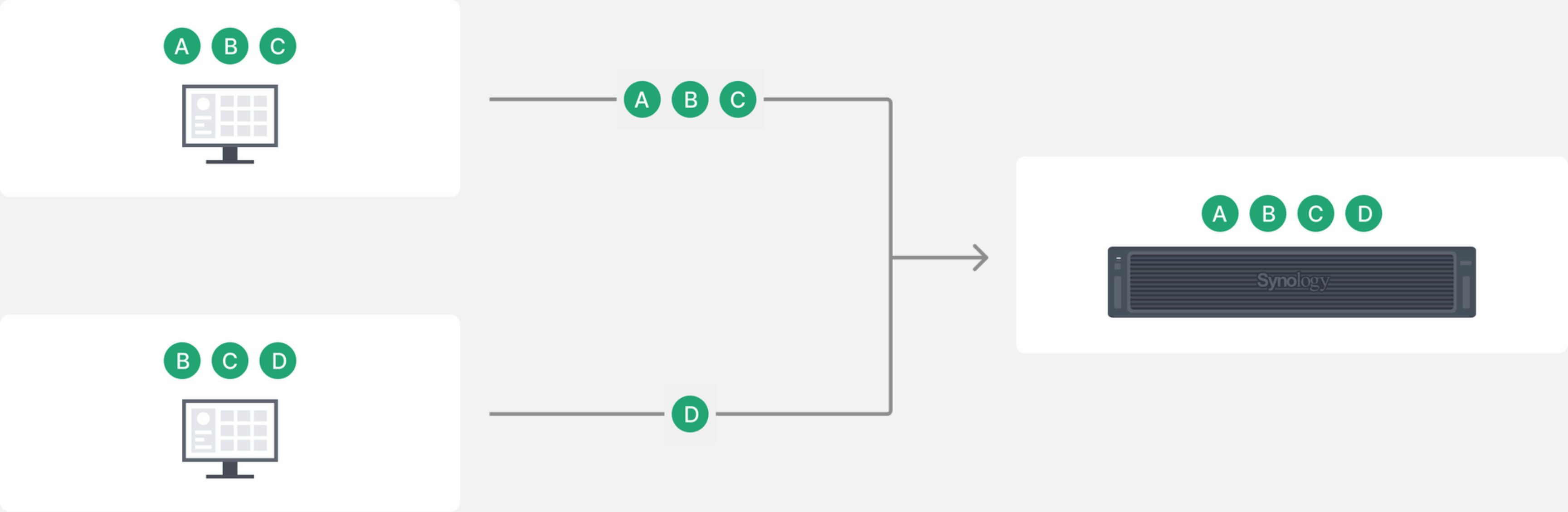
Source

Infra

Fast Backup

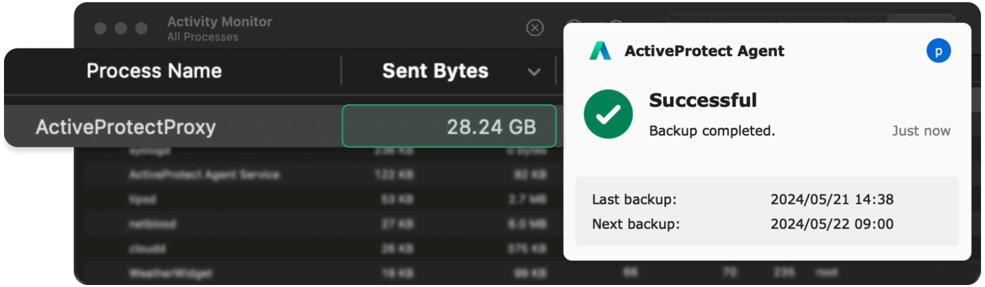
Snapshots with Fast Block Tracking and Time-Consistent Point-in-Time

Source-side Deduplication



Saves 99% of Redundant Data Transmission Traffic

Device A Full Backup



Activity Monitor
All Processes

Process Name	Sent Bytes
ActiveProtectProxy	28.24 GB

ActiveProtect Agent

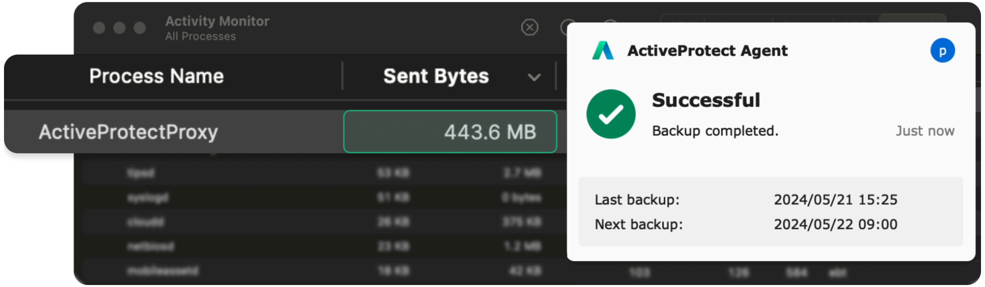
Successful

Backup completed.

Just now

Last backup: 2024/05/21 14:38
Next backup: 2024/05/22 09:00

Device B Full Backup



Activity Monitor
All Processes

Process Name	Sent Bytes
ActiveProtectProxy	443.6 MB

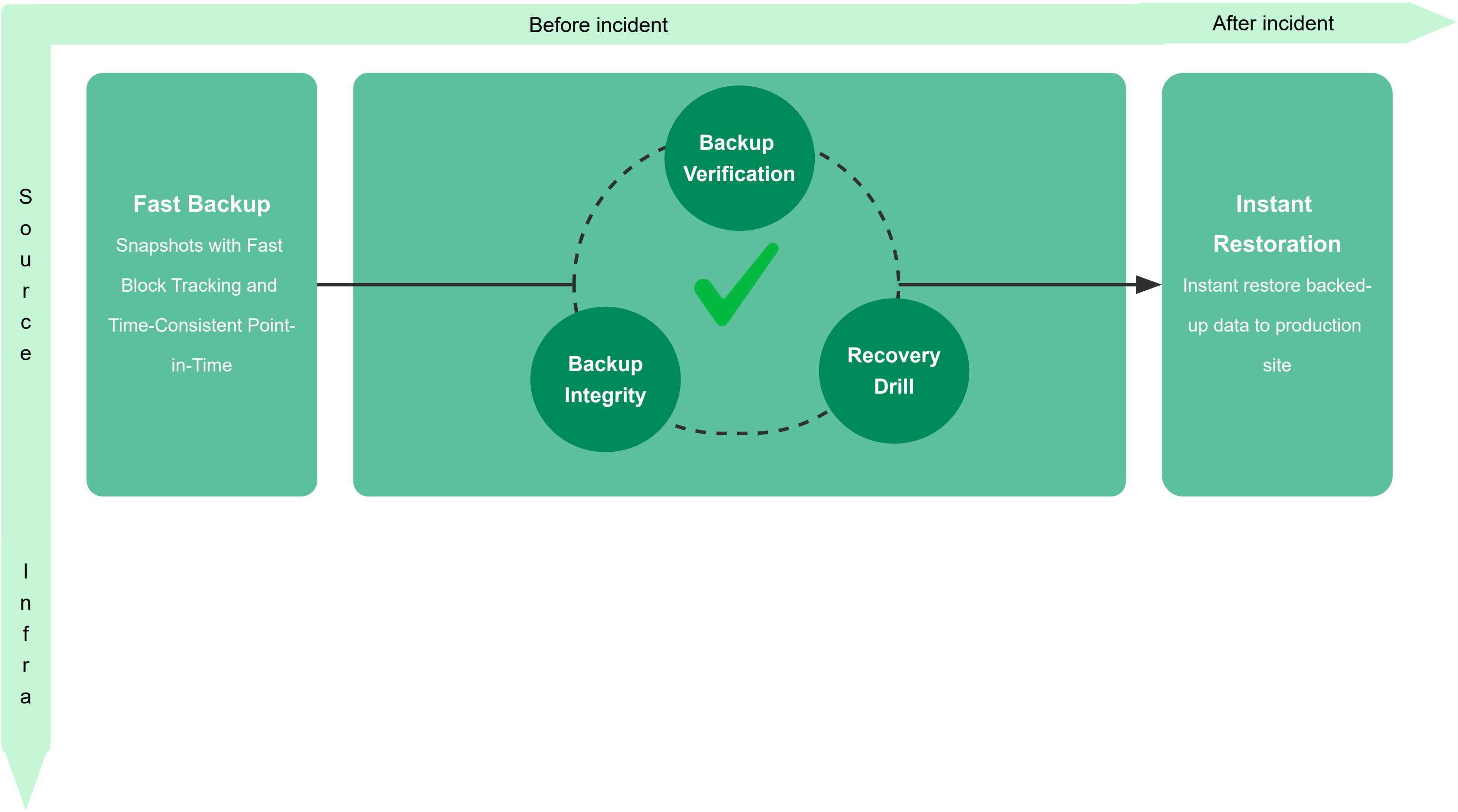
ActiveProtect Agent

Successful

Backup completed.

Just now

Last backup: 2024/05/21 15:25
Next backup: 2024/05/22 09:00

Before incident
After incident
Source
Infra
Fast Backup
Snapshots with Fast Block Tracking and Time-Consistent Point-in-Time
Backup Verification
Backup Integrity
Recovery Drill
Instant Restoration
Instant restore backed-up data to production site

Built-in quality assurance

Self-healing Backup

BTRFS checksum with RAID repairs damaged files automatically

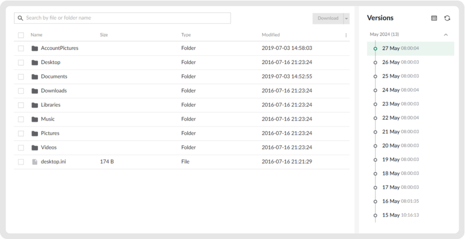
Backup Verification

Takes a video when the backup image is imported

Sandbox environment

Allows for regular restoration drills using the built-in hypervisor

Diverse Restoration Capabilities
Restore key data according to your needs



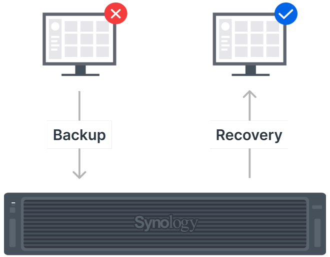
Name	Size	Type	Modified
AccountPictures		Folder	2019-07-03 14:58:03
Desktop		Folder	2016-07-16 21:23:24
Documents		Folder	2019-07-03 14:52:55
Downloads		Folder	2016-07-16 21:23:24
Libraries		Folder	2016-07-16 21:23:24
Music		Folder	2016-07-16 21:23:24
Pictures		Folder	2016-07-16 21:23:24
Videos		Folder	2016-07-16 21:23:24
desktop.ini	174 B	File	2016-07-16 21:21:29

Versions

May 2024 (13)

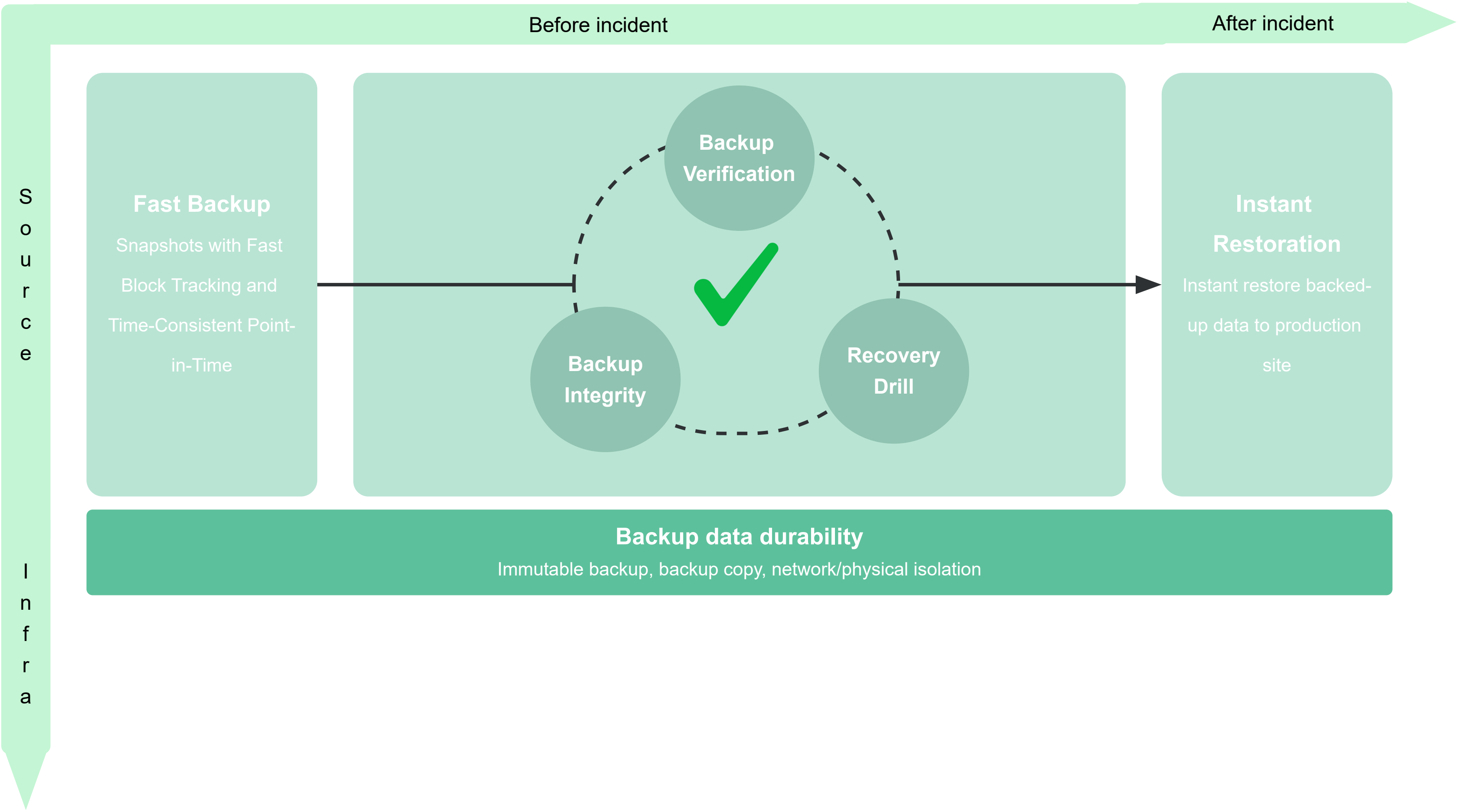
27 May 08:00:04
26 May 08:00:03
25 May 08:00:03
24 May 08:00:04
23 May 08:00:03
22 May 08:00:04
21 May 08:00:03
20 May 08:00:03
19 May 08:00:03
18 May 08:00:03
17 May 08:00:03
16 May 08:01:35
15 May 10:16:13

File-level Restoration



System Bare-metal Restore

Instant Restore to Hypervisor



Before incident

After incident

Source

Infra

Fast Backup

Snapshots with Fast Block Tracking and Time-Consistent Point-in-Time

Backup Verification

Backup Integrity

Recovery Drill

Instant Restoration

Instant restore backed-up data to production site

Backup data durability

Immutable backup, backup copy, network/physical isolation

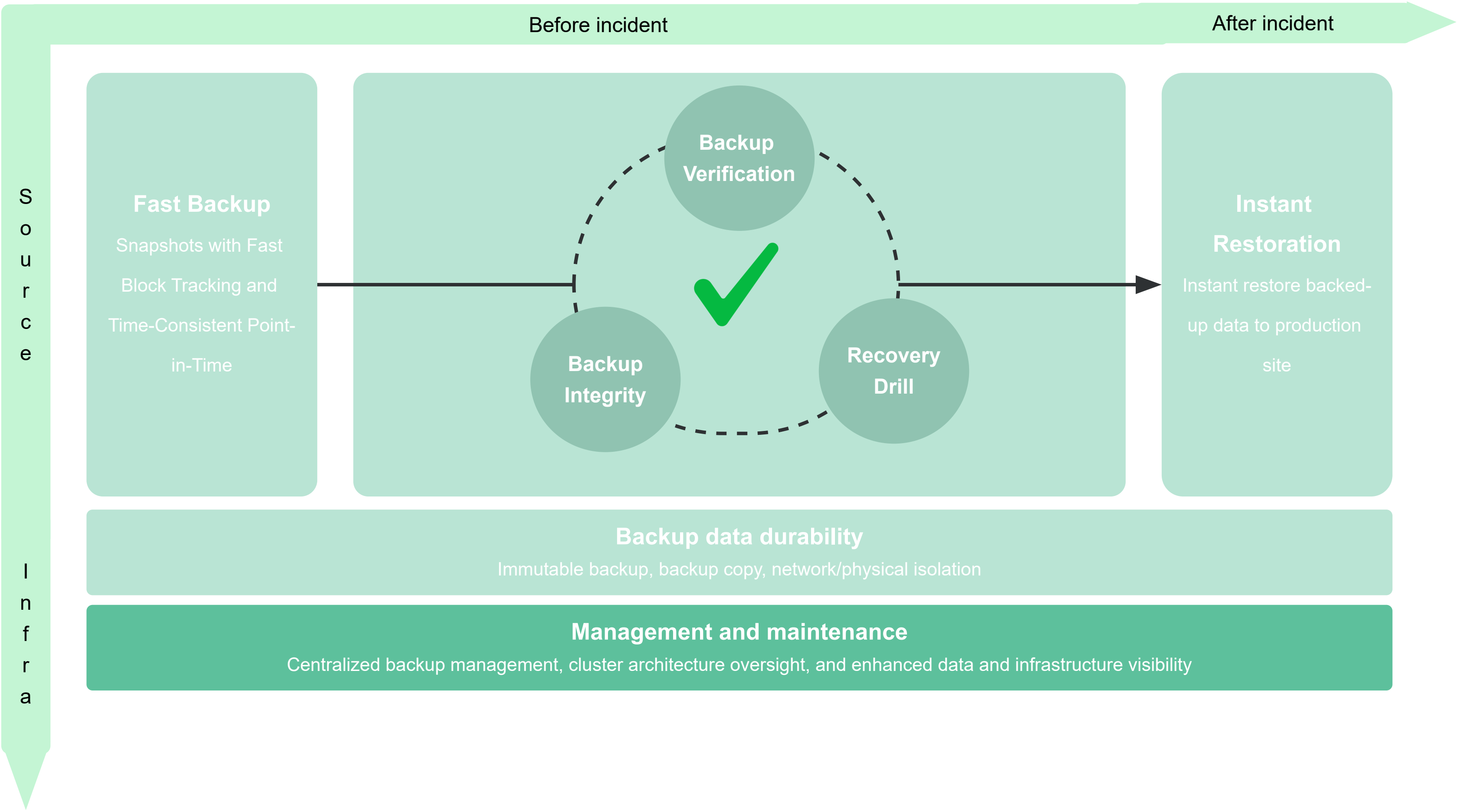
Enhance Integration of Remote Storage Security

Client-side Encryption

Protect backup copies through client-side encryption mechanisms to ensure that all backup copies are encrypted before they are stored, preventing unauthorized access to the data.

WORM Storage

Store backup copies in remote storage, with retention periods bound to prevent deletion or modification during the data retention period. This safeguards against any malicious attacks on backup copies.



Before incident

After incident

Source

Infra

Fast Backup

Snapshots with Fast Block Tracking and Time-Consistent Point-in-Time

Backup Verification

Backup Integrity

Recovery Drill

Instant Restoration

Instant restore backed-up data to production site

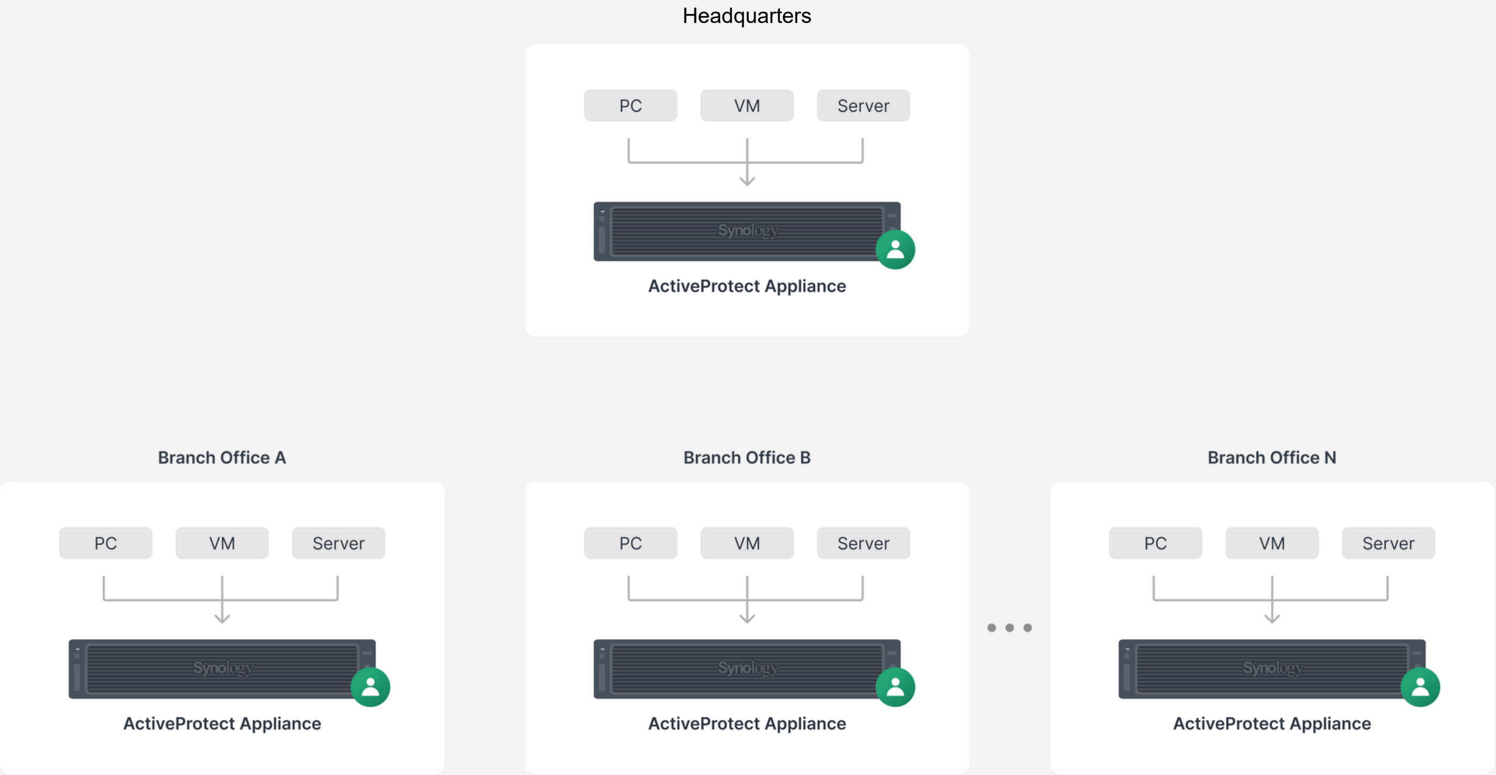
Backup data durability

Immutable backup, backup copy, network/physical isolation

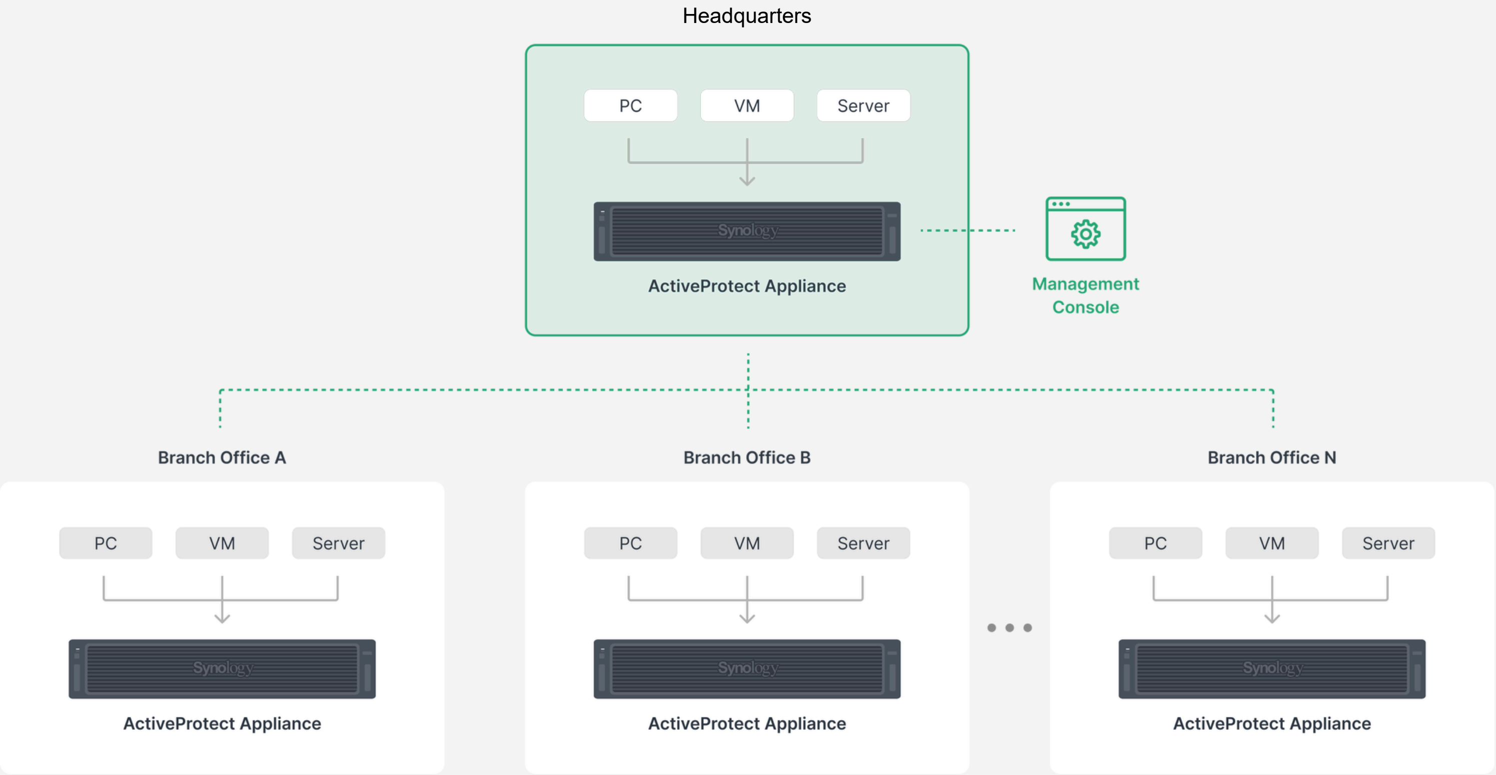
Management and maintenance

Centralized backup management, cluster architecture oversight, and enhanced data and infrastructure visibility

Multiple Servers Deployment



Single Interface for Multiple Servers



High Scalability to Protect the Entire Organization's Data

2.5K

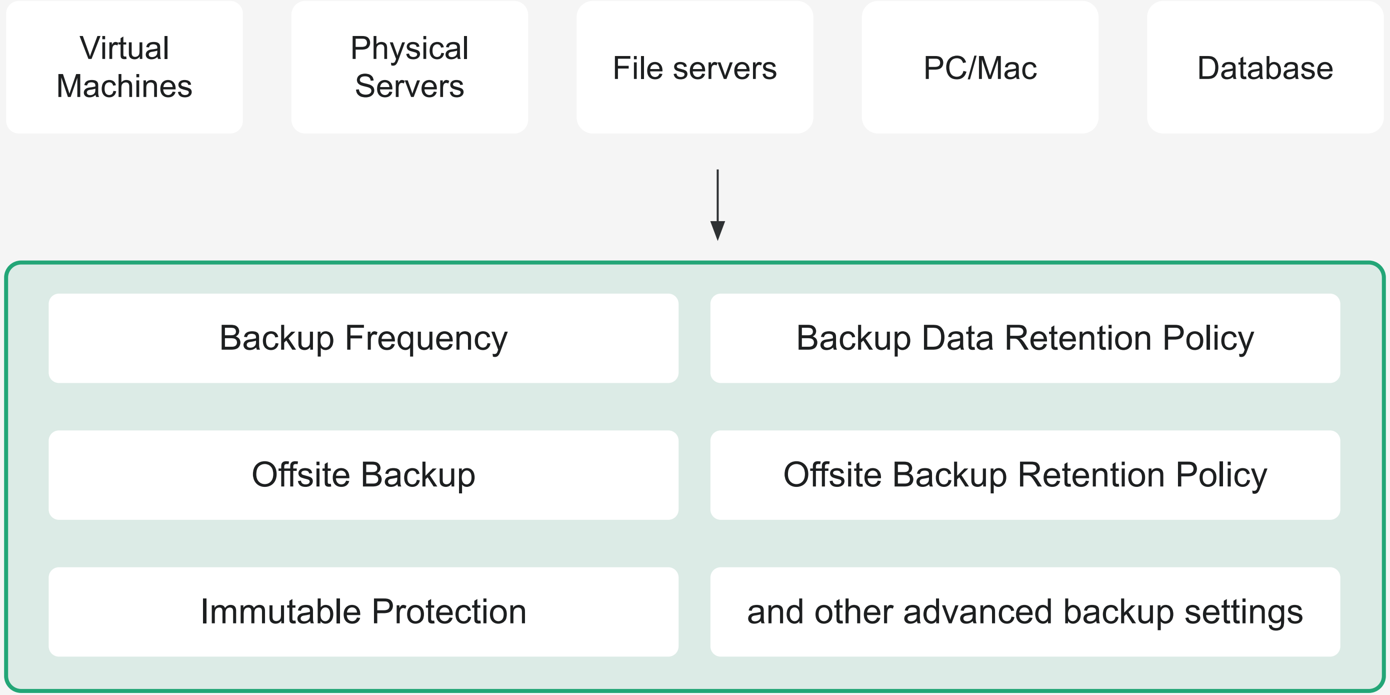
Site / Backup Server

150K

Backup Sources

(Devices and SaaS accounts)

Single Protection Plan
Covering All Backup Configurations



Virtual Machines

Physical Servers

File servers

PC/Mac

Database

Backup Frequency

Backup Data Retention Policy

Offsite Backup

Offsite Backup Retention Policy

Immutable Protection

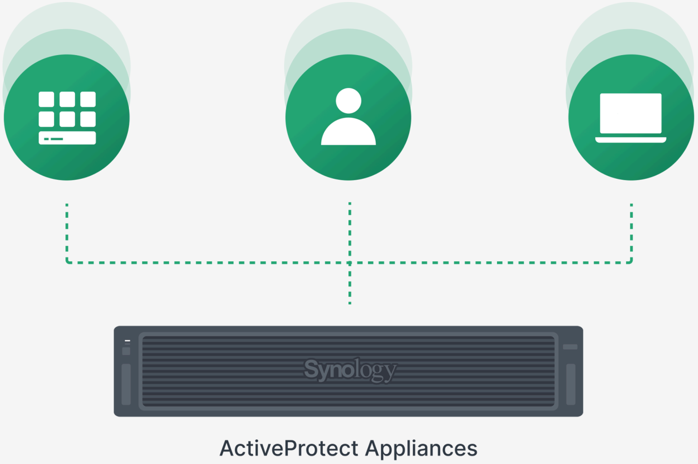
and other advanced backup settings

Auto Protection

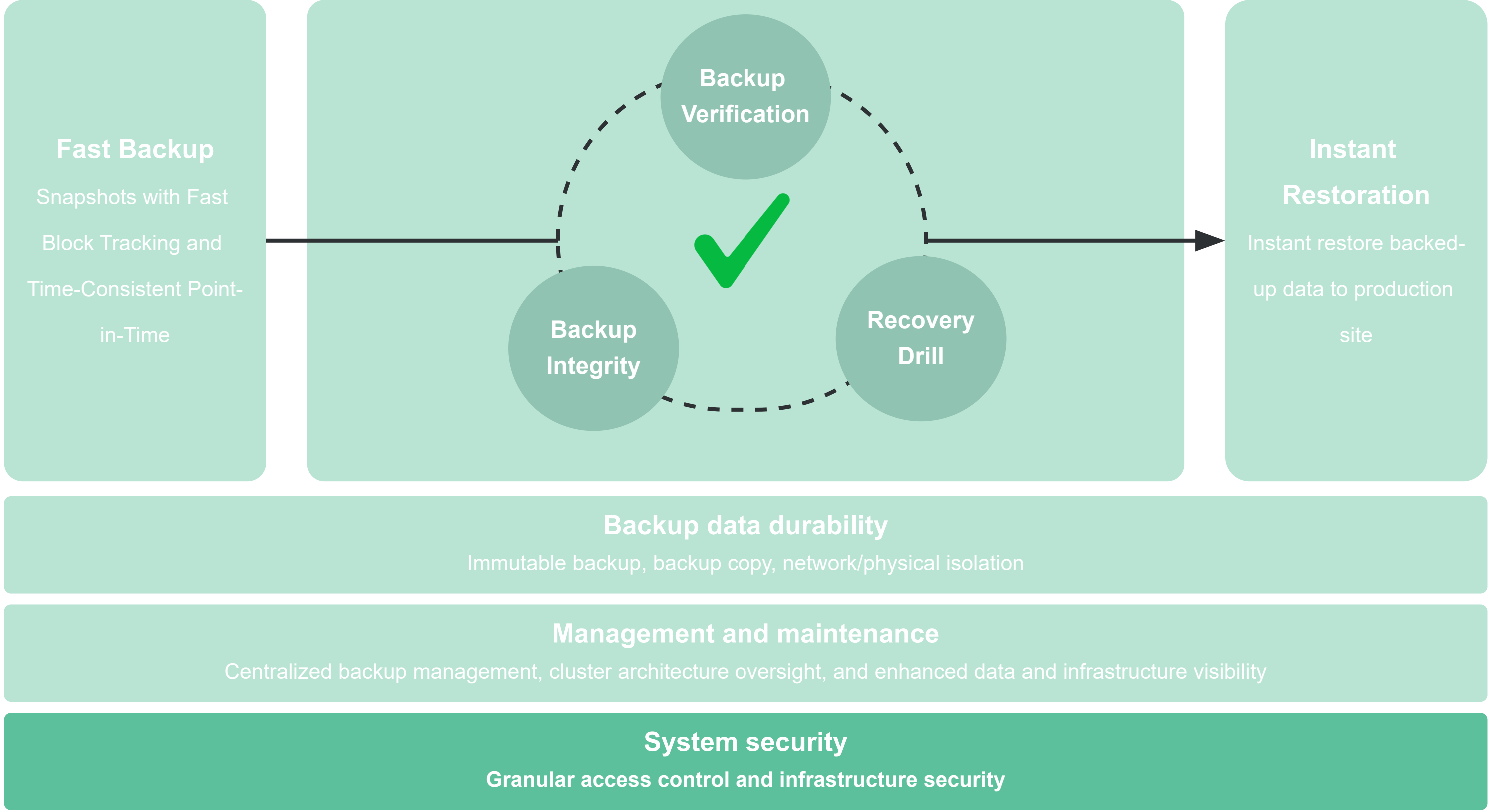
- **Virtual Machine:** Apply protection policies automatically **based on the host/cluster/folder** where the virtual machines reside

- **Cloud Service:** Apply protection policies automatically **based on the group** to which the account belongs

- **Physical Device:** During deployment, input the **Connect Key** to establish a connection and apply protection policies automatically



Trusted Backup System



Fast Backup

Snapshots with Fast Block Tracking and Time-Consistent Point-in-Time

Backup Verification

Backup Integrity

Recovery Drill

Instant Restoration

Instant restore backed-up data to production site

Backup data durability

Immutable backup, backup copy, network/physical isolation

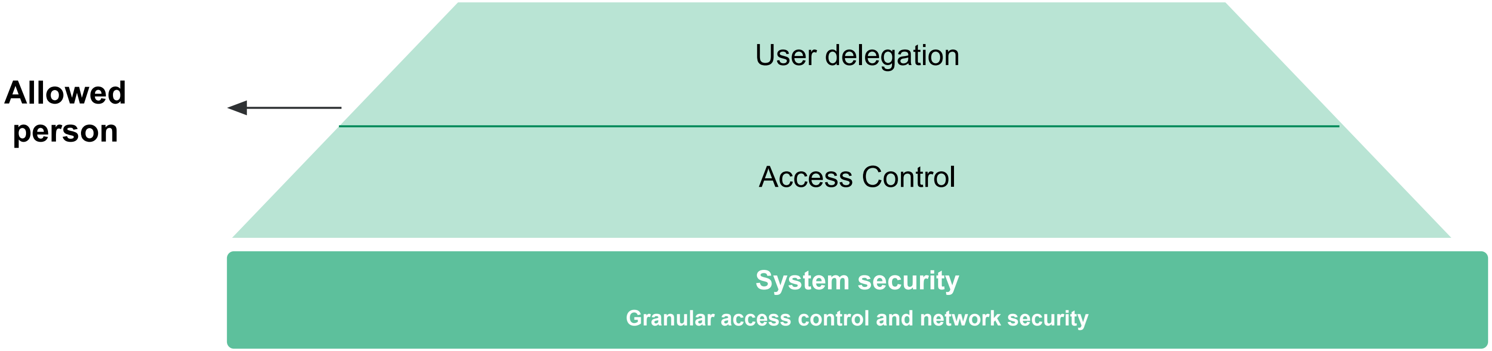
Management and maintenance

Centralized backup management, cluster architecture oversight, and enhanced data and infrastructure visibility

System security

Granular access control and infrastructure security

Designed with Data Security at its Core



Allowed person

User delegation

Access Control

System security

Granular access control and network security

Access Control

- Basic: Account & password

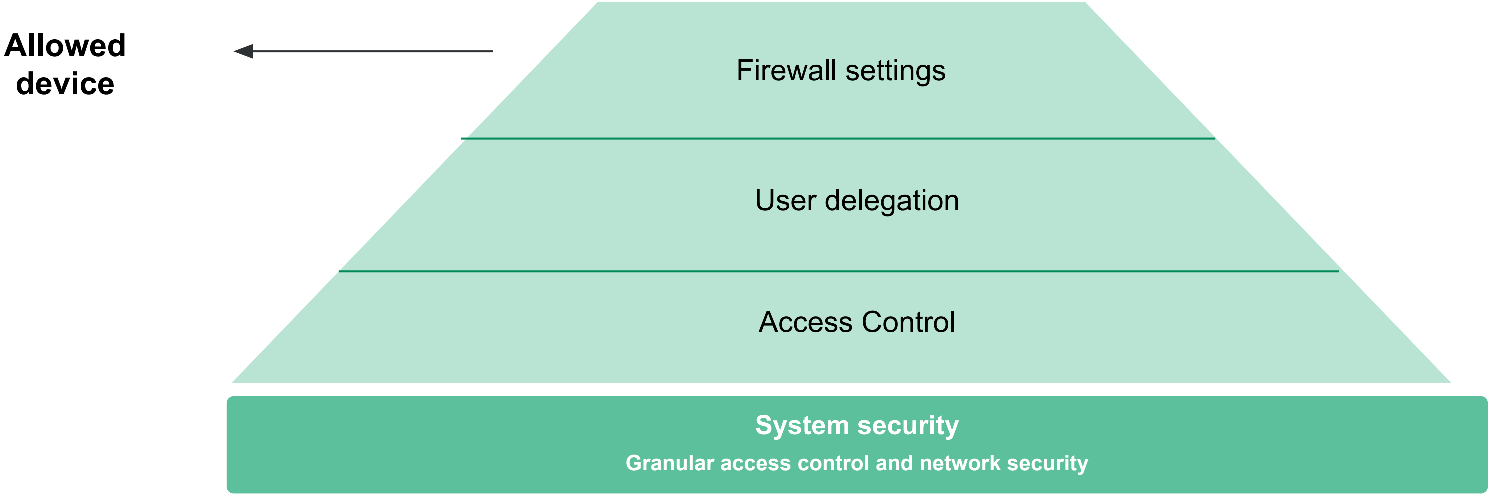
- Multi-factor (MFA): Integrating with directory services and supports SSO (SAML 2.0 and OIDC)

- Two-factor (2FA): Admin account

Granular User Permission

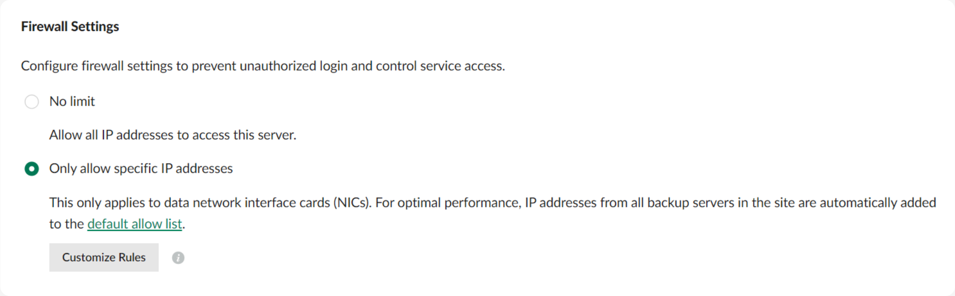
		Infra IT Team	Backup IT Team	Employee	Auditor
System Management	Storage	V	X	X	X
	Hardware config	V	X	X	X
	Networking	V	X	X	X
	System security	V	X	X	X
Backup	Protection Plan	X	V	X	X
	Backup config	X	V	X	X
	Backup server	X	V	X	X
Restore	Restore all data	X	V	X	X
	by service restore	X	V	V	X
	by backup server	X	V	X	X
Monitoring	Backup status	X	V	X	V

Designed with Data Security at its Core



Accessible Only to Authorized Devices

Through firewall settings, only devices on a specified IP whitelist are allowed to access the backup server



Firewall Settings

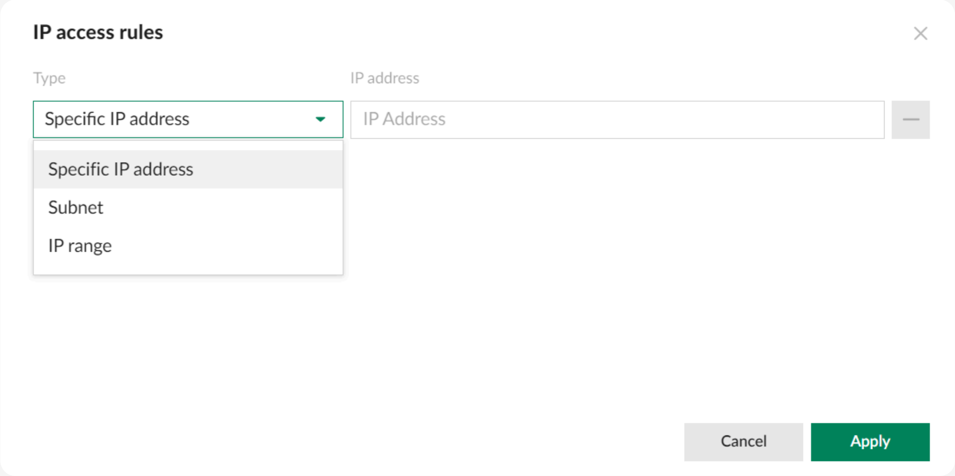
Configure firewall settings to prevent unauthorized login and control service access.

○ No limit

Allow all IP addresses to access this server.

● Only allow specific IP addresses

This only applies to data network interface cards (NICs). For optimal performance, IP addresses from all backup servers in the site are automatically added to the default allow list.

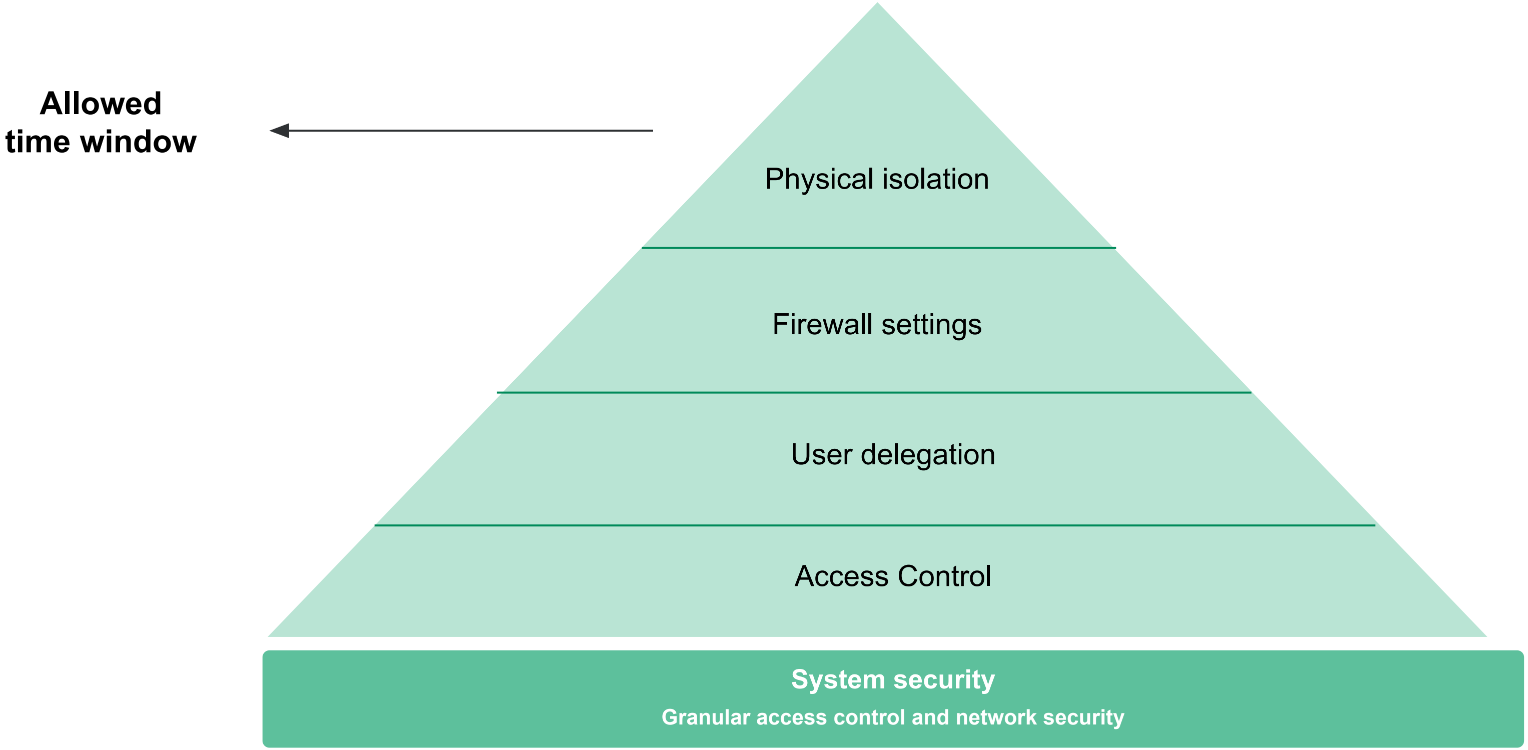


IP access rules

Type: Specific IP address

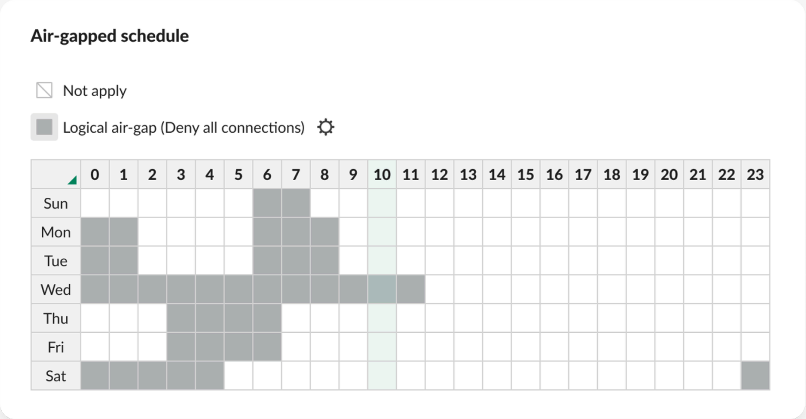
IP address: IP Address

Designed with Data Security at its Core



Accessible only when allowed time

Through physical isolation mechanisms and scheduled on/off of devices or network ports, ensure that access to equipment is only possible at designated times.

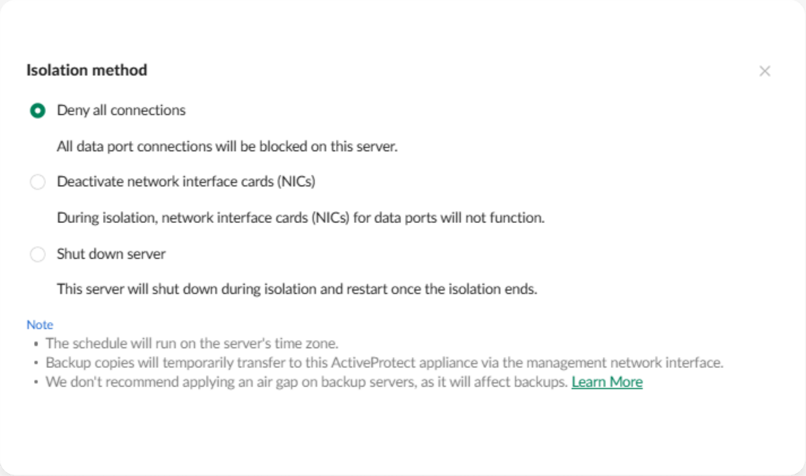


Air-gapped schedule

⧄ Not apply

■ Logical air-gap (Deny all connections)

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Sun							■	■																
Mon	■	■					■	■	■															
Tue	■	■					■	■	■															
Wed	■	■	■	■	■	■	■	■	■	■	■	■												
Thu				■	■	■	■																	
Fri				■	■	■	■																	
Sat	■	■	■	■	■																			■



Isolation method

● Deny all connections

All data port connections will be blocked on this server.

○ Deactivate network interface cards (NICs)

During isolation, network interface cards (NICs) for data ports will not function.

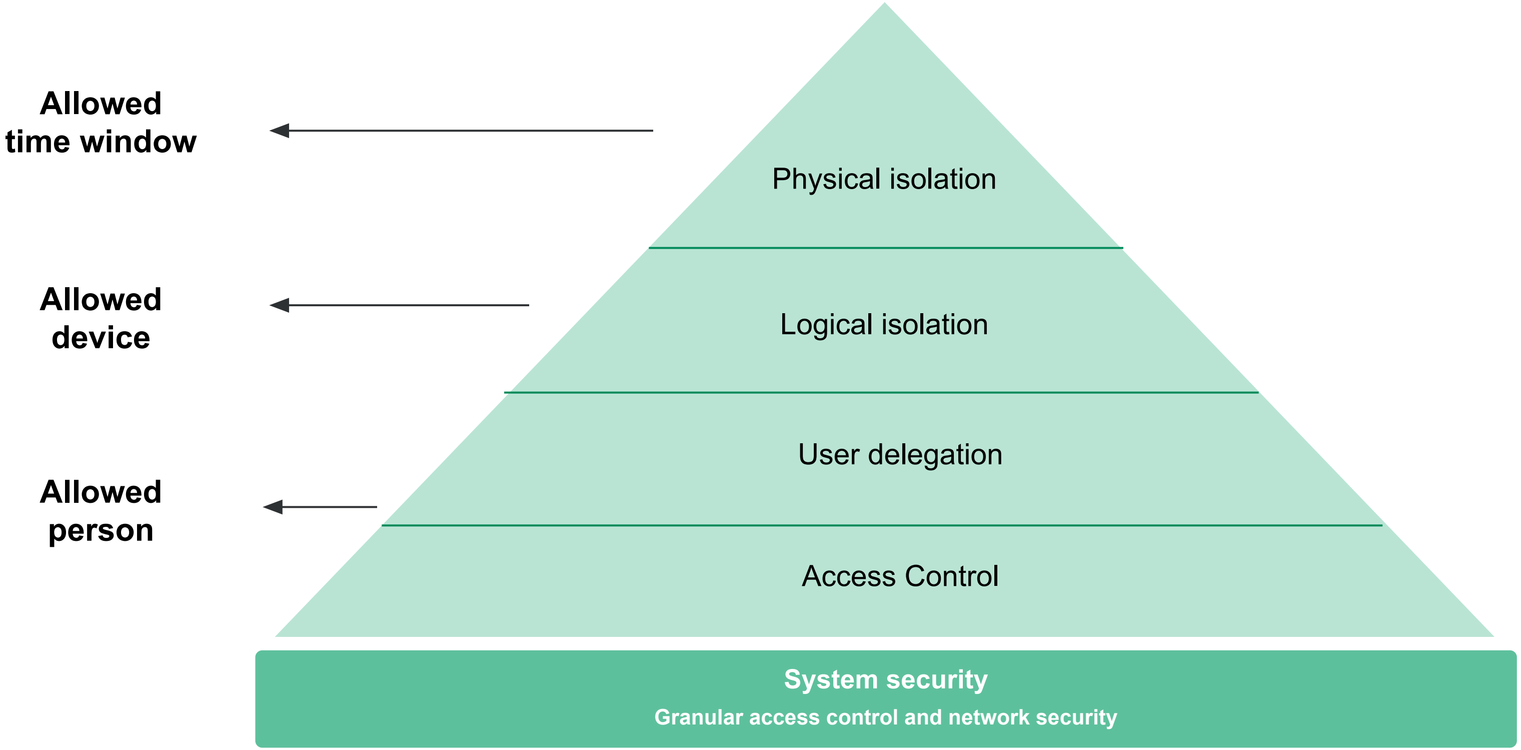
○ Shut down server

This server will shut down during isolation and restart once the isolation ends.

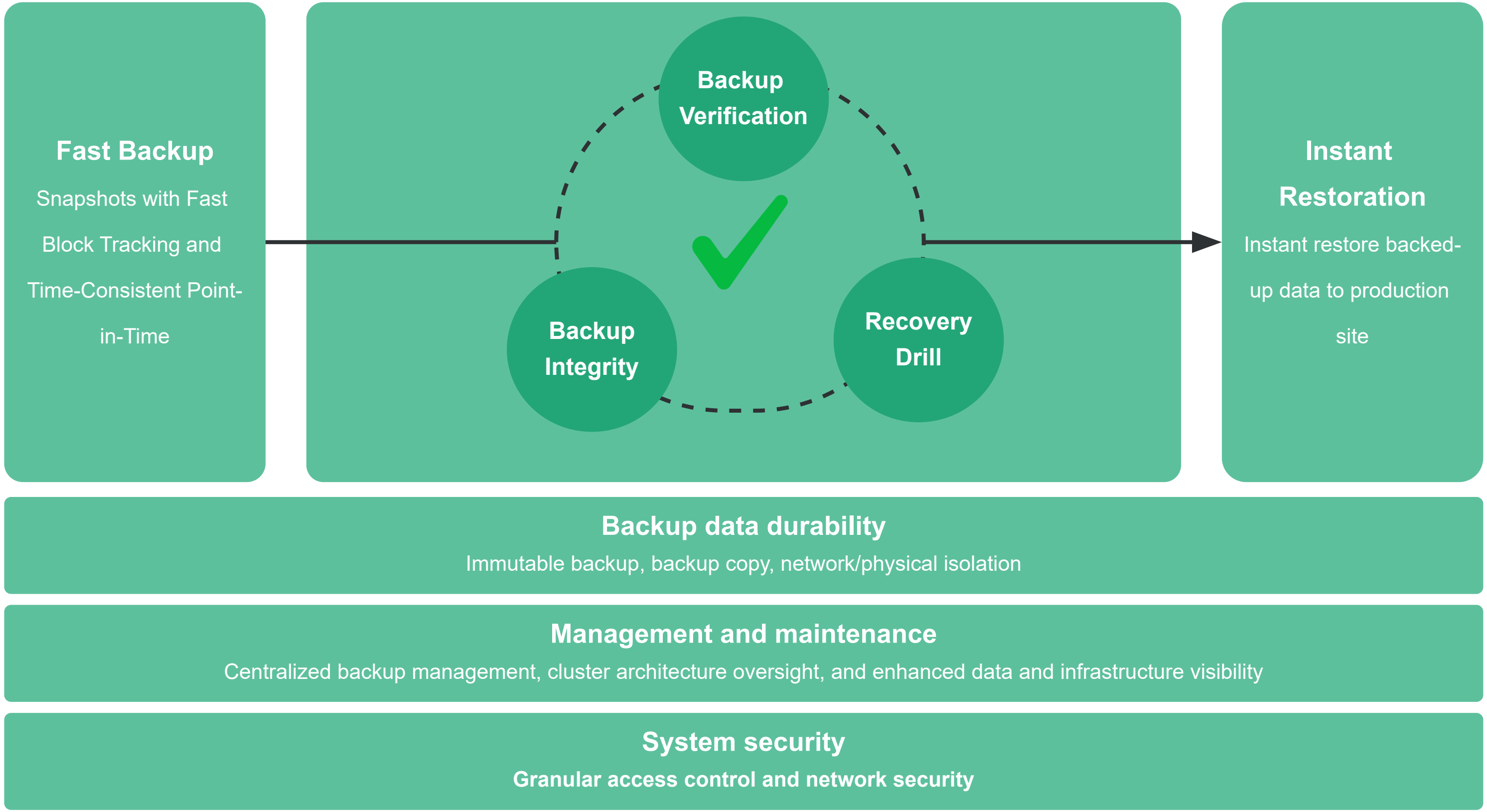
Note

- The schedule will run on the server's time zone.
- Backup copies will temporarily transfer to this ActiveProtect appliance via the management network interface.
- We don't recommend applying an air gap on backup servers, as it will affect backups. Learn More

Designed with Data Security at its Core



Synology cyber-resiliency data protection



Fast Backup

Snapshots with Fast Block Tracking and Time-Consistent Point-in-Time

Backup Verification

Backup Integrity

Recovery Drill

Instant Restoration

Instant restore backed-up data to production site

Backup data durability

Immutable backup, backup copy, network/physical isolation

Management and maintenance

Centralized backup management, cluster architecture oversight, and enhanced data and infrastructure visibility

System security

Granular access control and network security

Synology® | DP SERIES

Synology ActiveProtect

ActiveProtect Appliance

DP320
Suggested
backup: 5TB

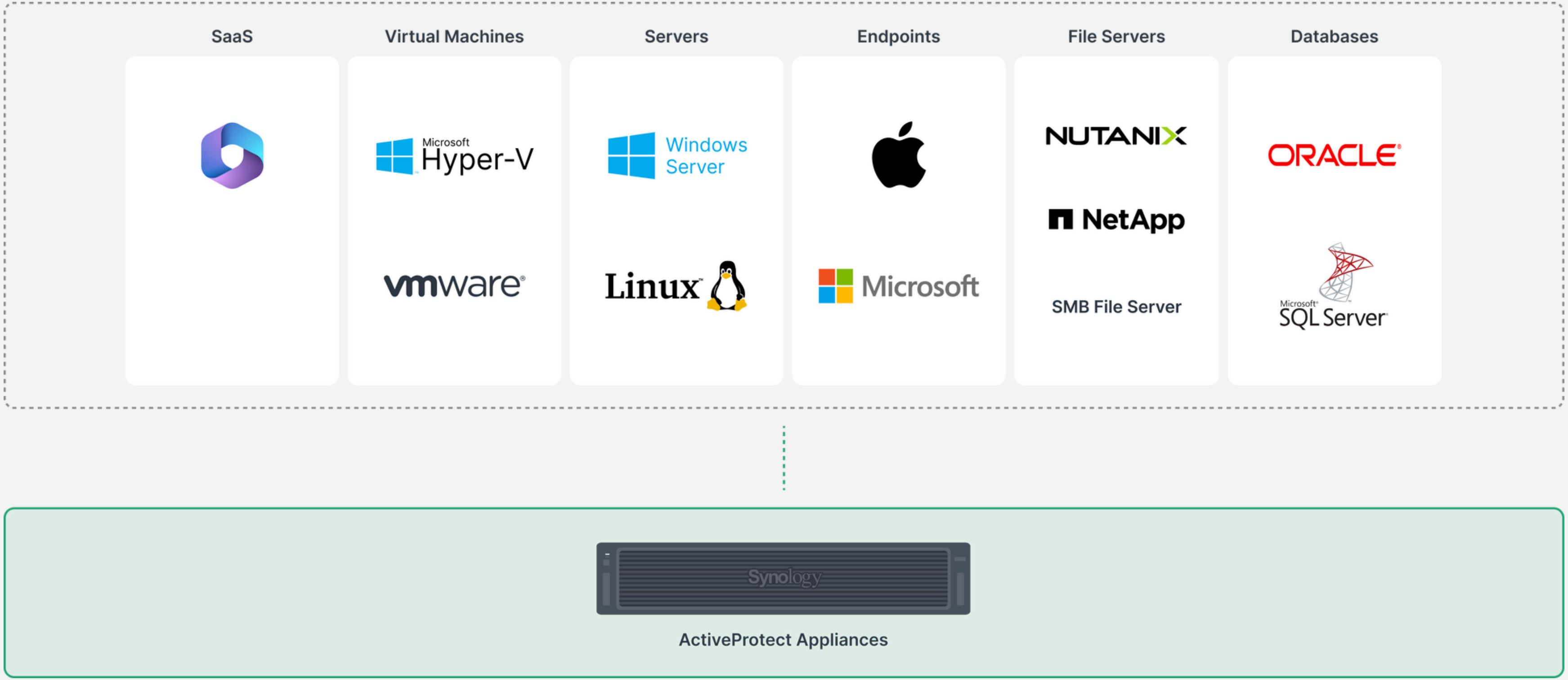
DP7400
Suggested
backup: 83.5TB

DP340
Suggested
backup: 14.5TB

ActiveProtect Manager

Modern, secure, and simple. A next-generation backup OS designed to protect emerging workloads for businesses.

Cross-Platform Centralized Protection



SaaS

Virtual Machines

Servers

Endpoints

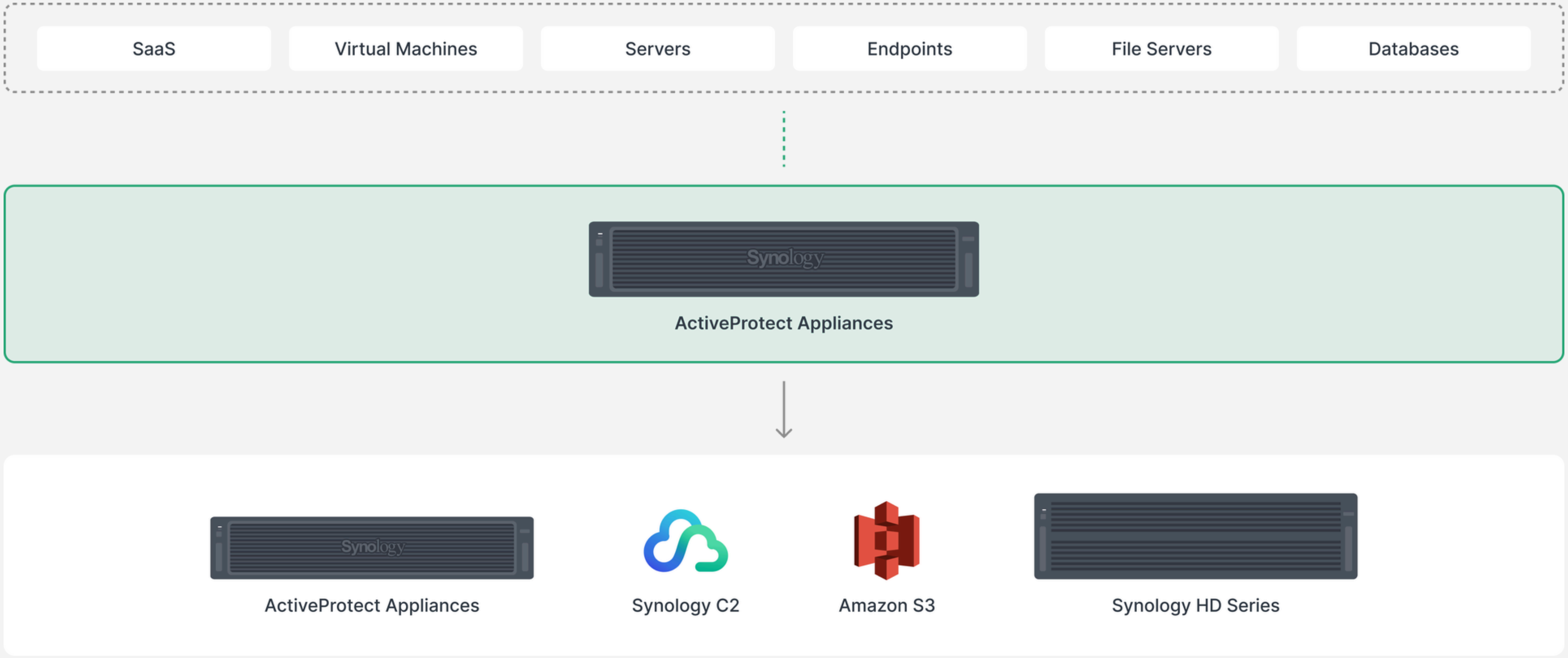
File Servers

Databases

SMB File Server

ActiveProtect Appliances

Native Offsite Backup Capability



SaaS

Virtual Machines

Servers

Endpoints

File Servers

Databases

ActiveProtect Appliances

ActiveProtect Appliances

Synology C2

Amazon S3

Synology HD Series

Synology ActiveProtect Appliance

Simple Management

Reliable Restoration

Optimal Performance

Synology ActiveProtect Appliance

Simple Management

Reliable Restoration

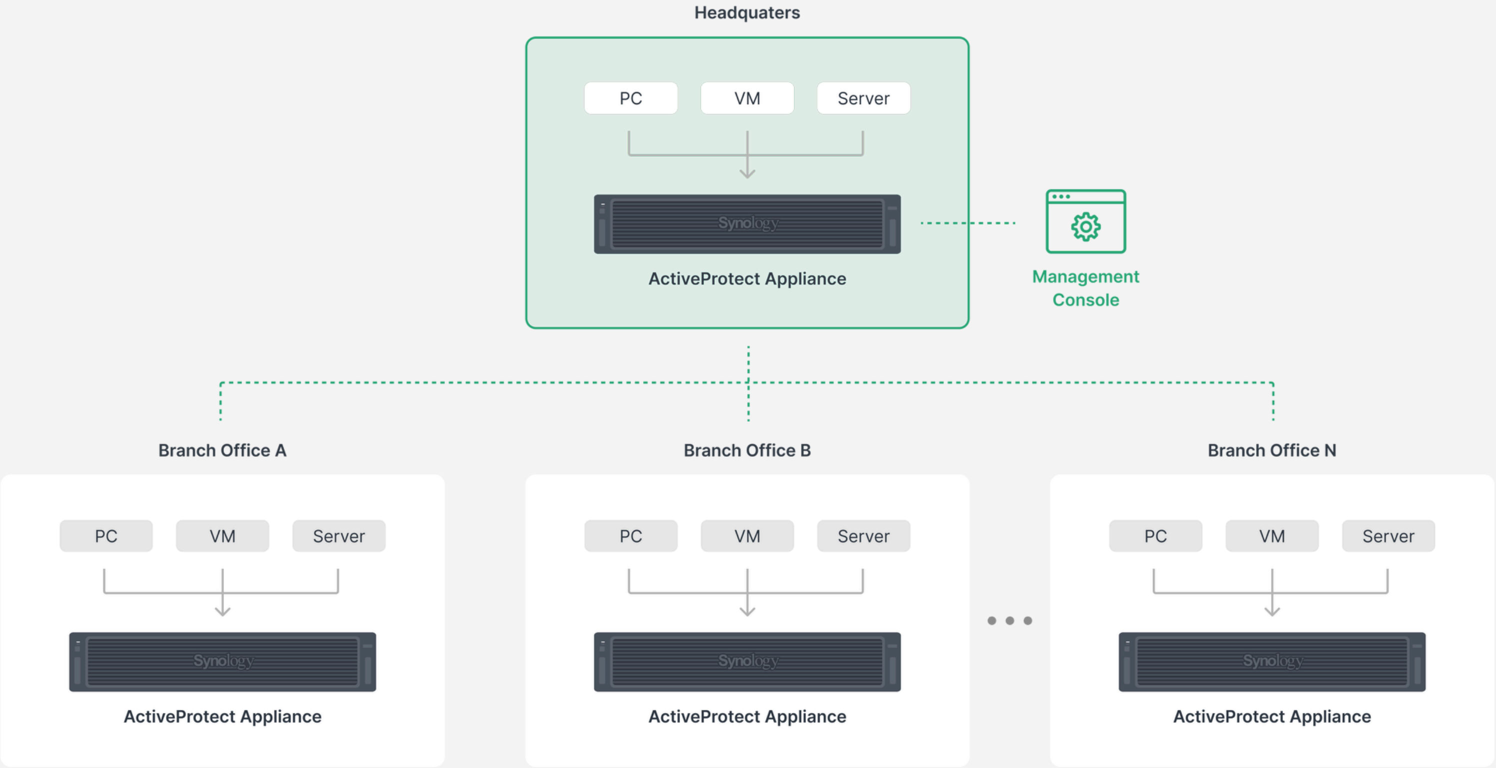
Optimal Performance

Easy Deployment with Software & Hardware Integration

10 min

Complete Initial Setup

Single Interface for Multi-site Deployments



High Scalability to protect the entire organization’s data

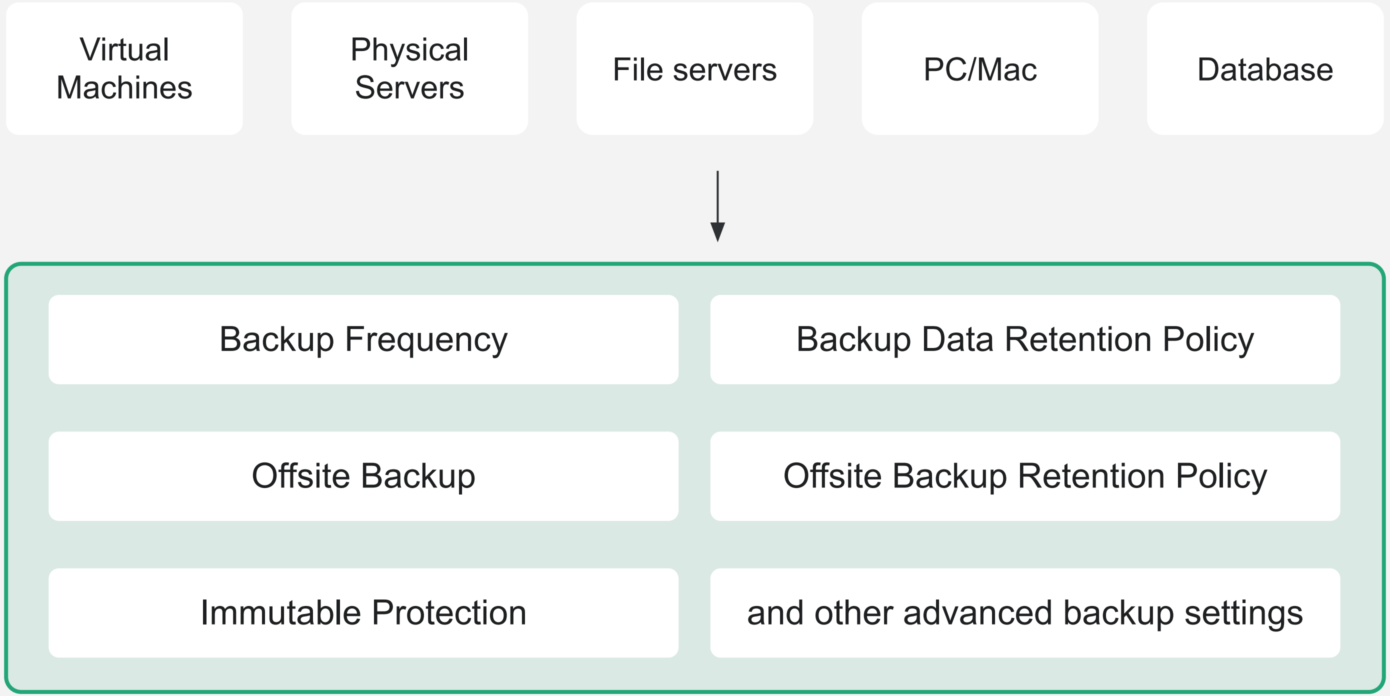
2.5K

Site / Backup Server

150K

Endpoint Devices /
Cloud Accounts

Single Protection Plan
Covering All Backup Configurations



Virtual Machines

Physical Servers

File servers

PC/Mac

Database

Backup Frequency

Backup Data Retention Policy

Offsite Backup

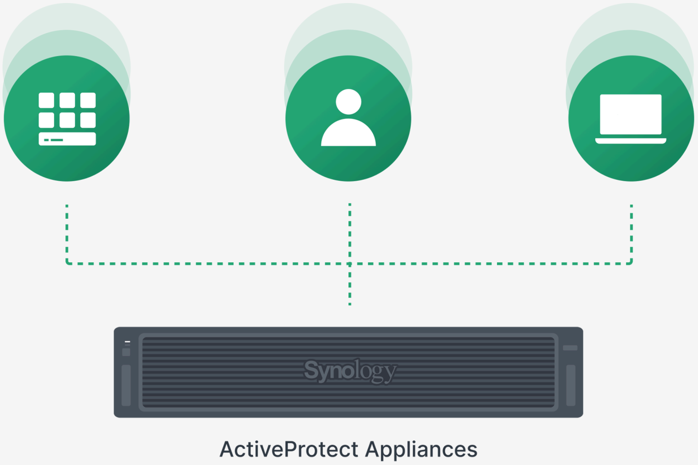
Offsite Backup Retention Policy

Immutable Protection

and other advanced backup settings

Set & Forgot

- **Virtual Machine:** Apply protection policies automatically **based on the host/cluster/folder** where the virtual machines reside
- **Cloud Service:** Apply protection policies automatically **based on the group** to which the account belongs
- **Physical Device:** During deployment, input the **Connect Key** to establish a connection and apply protection policies automatically



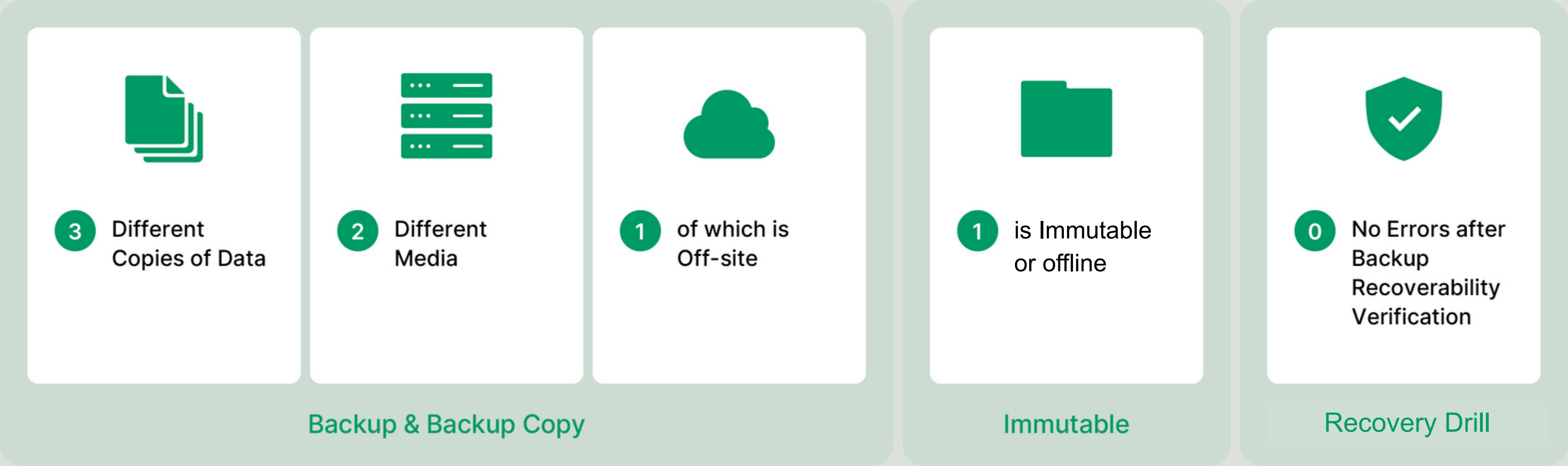
Synology ActiveProtect Appliance

Simple Management

Reliable Restoration

Optimal Performance

3-2-1-1-0 Backup Rule



3 Different Copies of Data

2 Different Media

1 of which is Off-site

Backup & Backup Copy

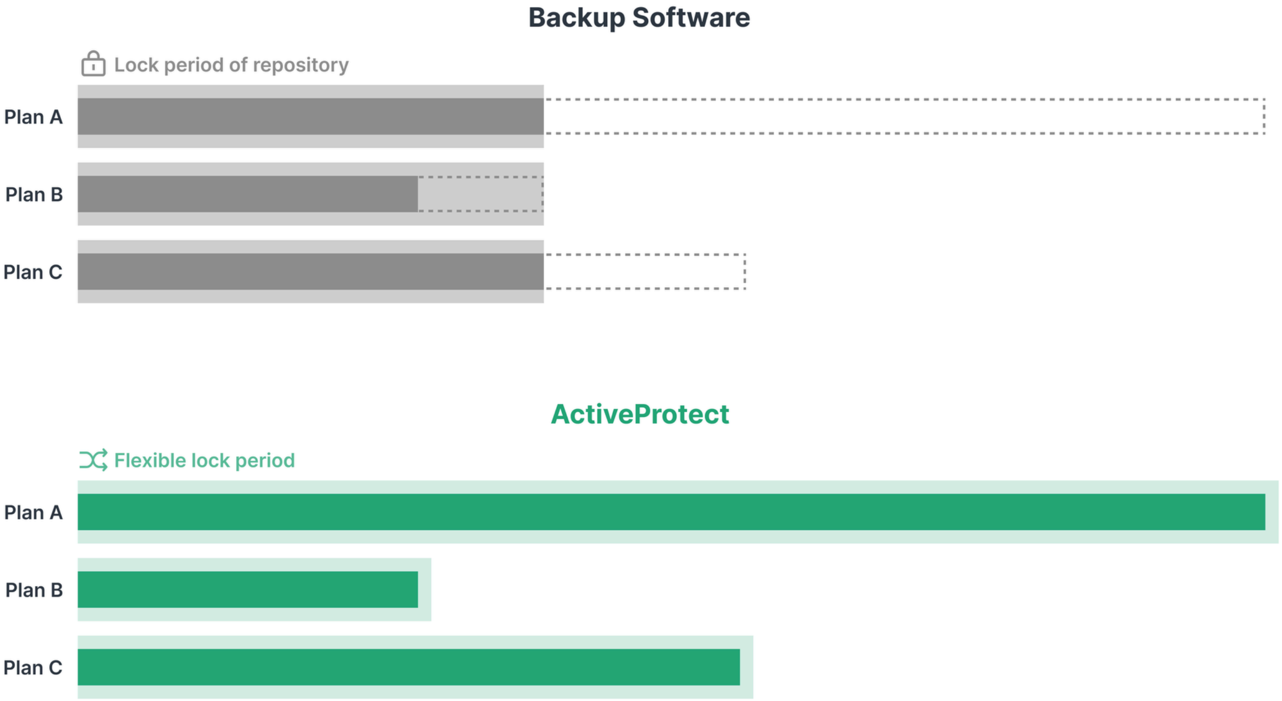
1 is Immutable or offline

Immutable

0 No Errors after Backup Recoverability Verification

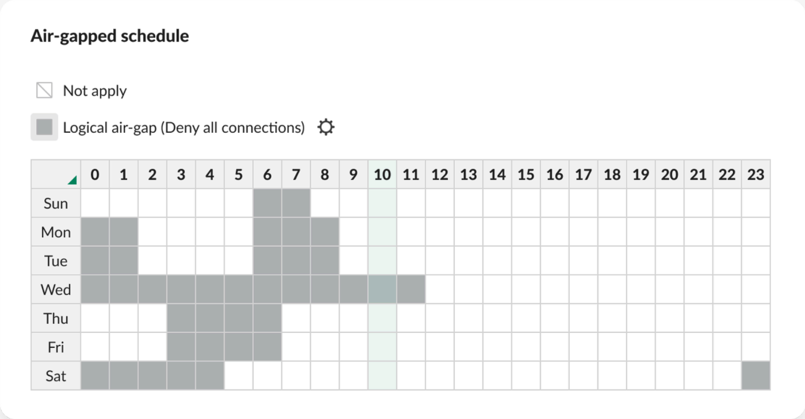
Recovery Drill

Native Immutability



Offline Backup

Through physical isolation mechanisms and scheduled on/off of devices or network ports, ensure that access to equipment is only possible at designated times.

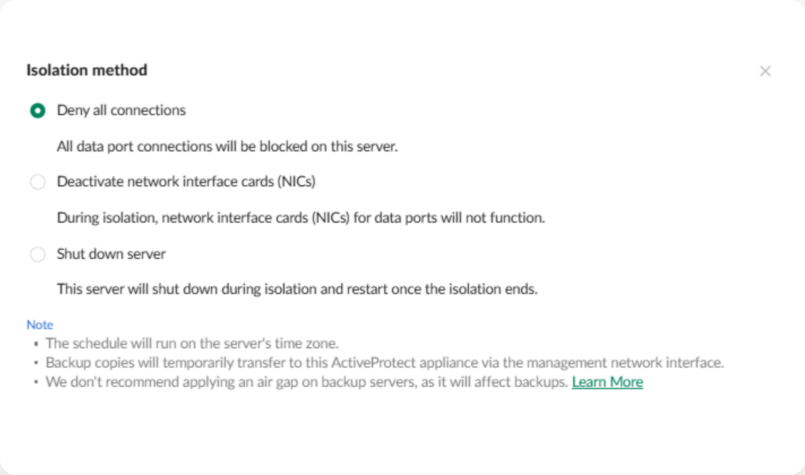


Air-gapped schedule

□ Not apply

▨ Logical air-gap (Deny all connections)

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Sun							▨	▨																
Mon	▨	▨					▨	▨	▨															
Tue	▨	▨					▨	▨	▨															
Wed	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨												
Thu				▨	▨	▨	▨																	
Fri				▨	▨	▨	▨																	
Sat	▨	▨	▨	▨	▨																			▨



Isolation method

● Deny all connections

All data port connections will be blocked on this server.

○ Deactivate network interface cards (NICs)

During isolation, network interface cards (NICs) for data ports will not function.

○ Shut down server

This server will shut down during isolation and restart once the isolation ends.

Note

- The schedule will run on the server's time zone.
- Backup copies will temporarily transfer to this ActiveProtect appliance via the management network interface.
- We don't recommend applying an air gap on backup servers, as it will affect backups. Learn More

Built-in quality assurance

Self-healing Backup

BTRFS checksum with RAID repairs damaged files automatically

Backup Verification

Takes a video when the backup image is imported

Sandbox environment

Allows for regular restoration drills using the built-in hypervisor

Designed with Data Security at its Core

Prevention of ransomware

- Native integrated off-site backup
- Immutable protection
- Scheduled offline (Air gap)
- Backup verification
- Built-in hypervisor for recovery drills

Security authentication

- Support for Windows AD/LDAP authentication
- Support for SAML 2.0 SSO server to meet multi-factor authentication requirements
- Access control permissions

System security

- Product Security Incident Response Team
- Rapid response to security incidents
- Static code analysis
- Penetration testing
- Membership in FIRST organization

Data and network security

- Automated repair of static data corruption
- Automatic repair of disk corruption
- Built-in firewall
- Transmission encryption
- Out-of-band management mechanism

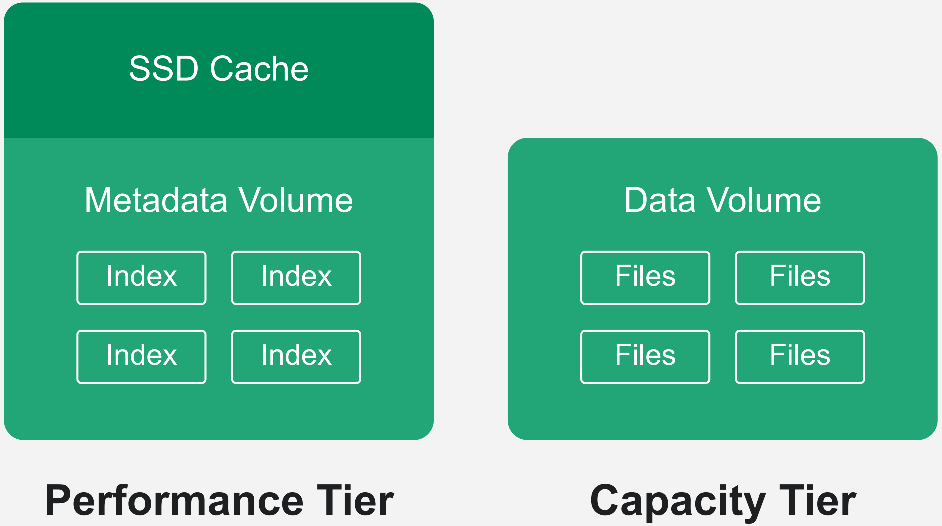
Synology ActiveProtect Appliance

Simple Management

Reliable Restoration

Optimal Performance

Storage Space Redistribution


SSD Cache

Metadata Volume

Index

Index

Index

Index

Performance Tier

Data Volume

Files

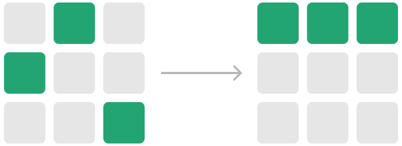
Files

Files

Files

Capacity Tier

Exclusive Backup Engine for Optimized Performance



Data Reordering

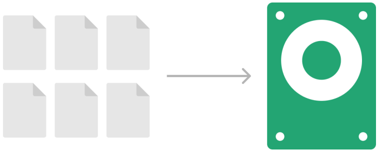
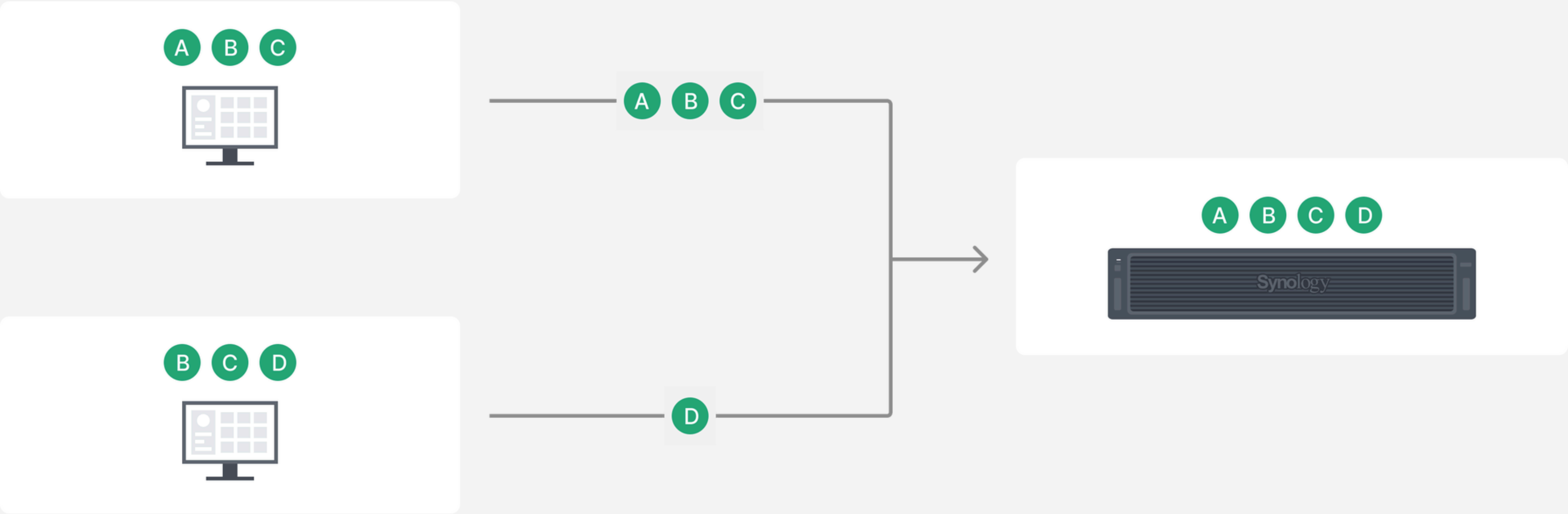


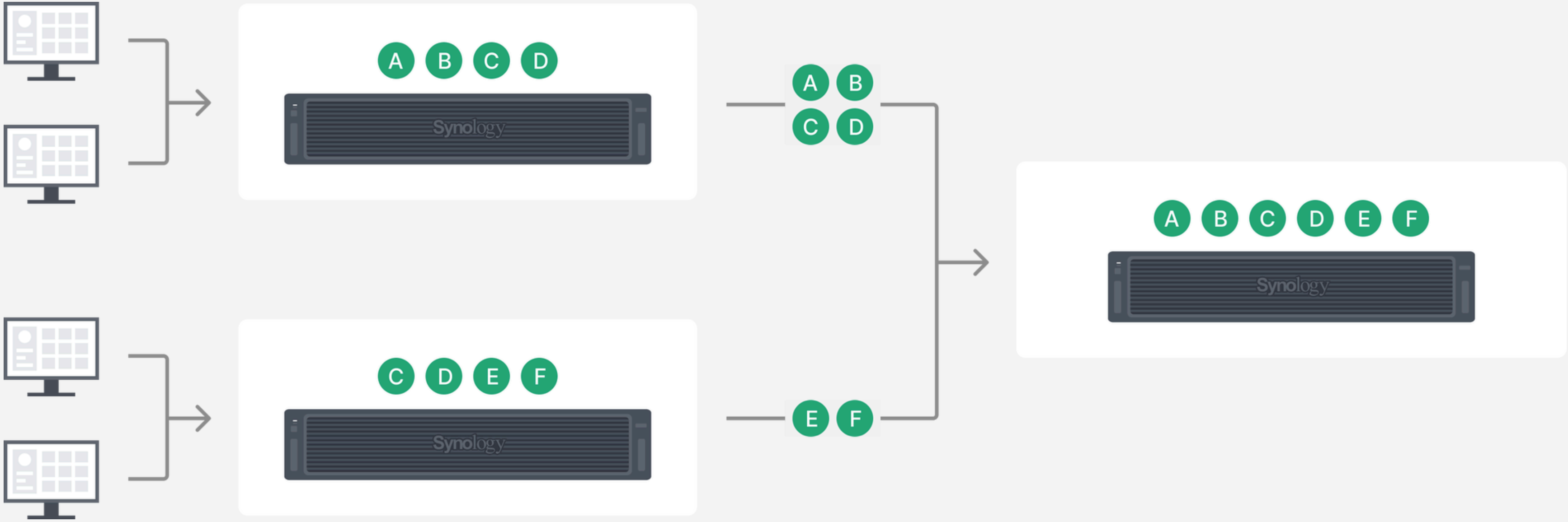
Image-file Level Data Processing

Block-level Data Copying

Global Source-side Deduplication



Cross-site Remote Backup also Applicable



Synology ActiveProtect Appliance

Simple Management

Single-platform management for up to 150,000 devices

Reliable Restoration

Integration of immutable storage and offline backup against ransomware

Outstanding Performance

Integrate source side-deduplication and optimized storage configuration

Synology®

DP SERIES

Thank you!

Synology ANZ Country Manager

Jasmine Chiu