Data Center   **Infraestrutura**   **Segurança**   **Cloud**   **Mídia Indoor**

A MDF Technology tem a solução que sua empresa necessita, com um vasto portfolio de soluções em TI e publicidade online.

Agregue valor ao seu negócio, crie uma estratégia e renove seu parque tecnológico em conjunto conosco. A MDF Technology tem as melhores soluções para atender a necessidade de seu negócio e trazer retorno para seu investimento.

⟡ **ameaças**   Buscar no blog 🔍

Brasil é líder em empresas atacadas por ransomware na epidemia

Cibercrime aproveitou a transferência de funcionários para regime de home office para intensificar ataques
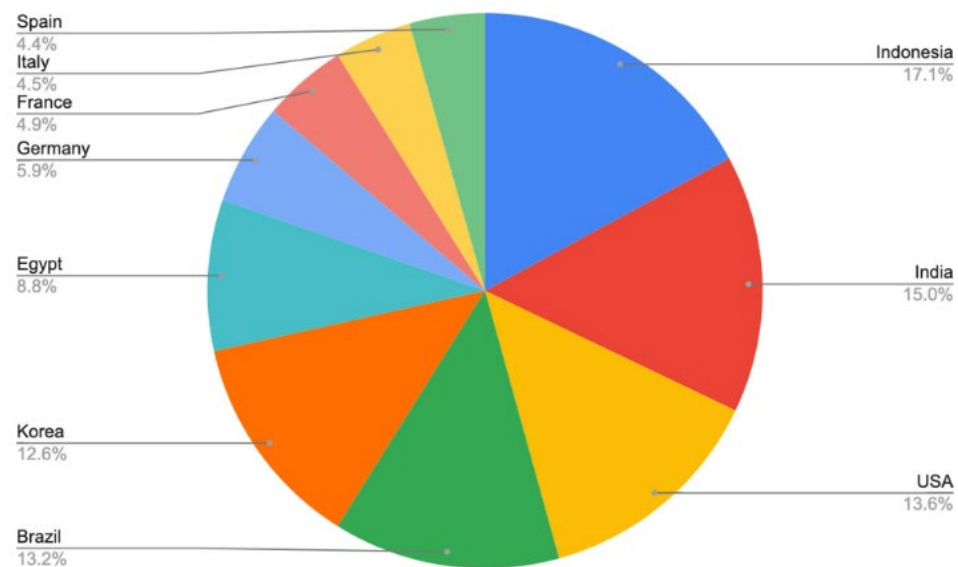
Renato Rodrigues   4 jun 2020

Brazil leads in ransomware attacks

The country ranks second after the United States on a list of the world's five most targeted markets
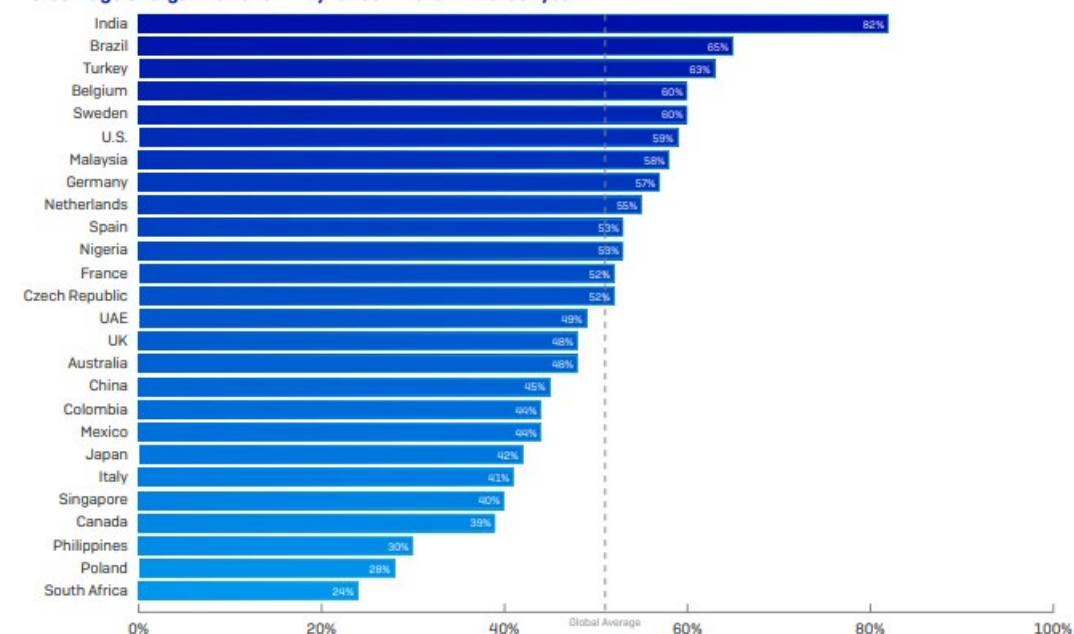
Brazil is the world's second most threatened country by ransomware attacks, according to a new study by security firm Trend Micro.

Top countries with endpoints encountering - or being crypto-locked by - strains of ransomware over the past six months (Source: Emsisoft)

Percentage of organizations hit by ransomware in the last year

Country	%
India	82%
Brazil	65%
Turkey	63%
Belgium	60%
Sweden	60%
U.S.	59%
Malaysia	58%
Germany	57%
Netherlands	55%
Spain	53%
Nigeria	53%
France	52%
Czech Republic	52%
UAE	49%
UK	48%
Australia	48%
China	45%
Colombia	44%
Mexico	44%
Japan	42%
Italy	41%
Singapore	40%
Canada	39%
Philippines	30%
Poland	28%
South Africa	24%

In the last year, has your organization been hit by ransomware? Base: 5,000 respondents.

THE STATE OF RANSOMWARE 2020

A Sophos white paper May 2020
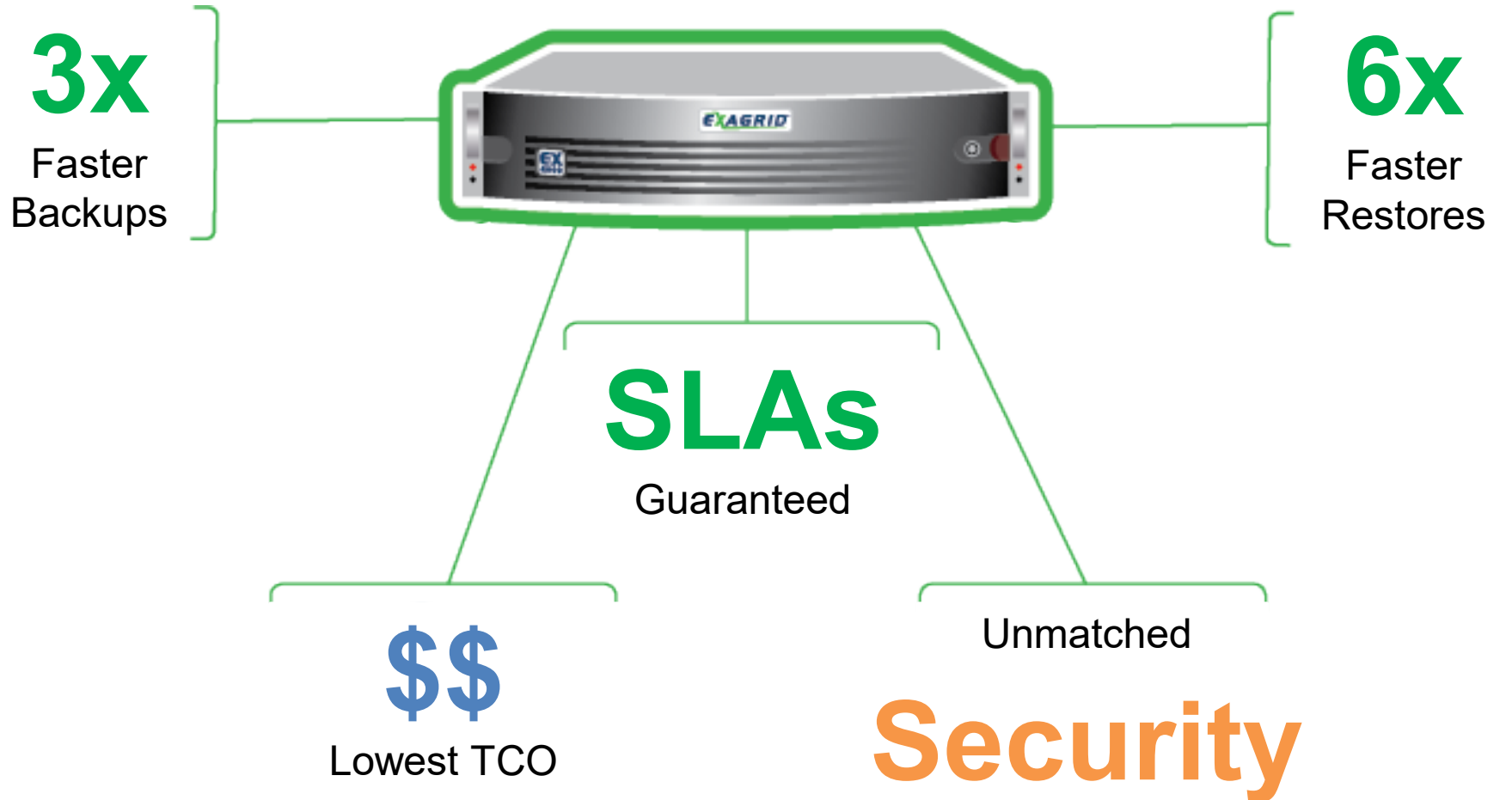
Results of an independent study of 5,000 IT managers across 26 countries

Ataques de ransomware no Brasil cresceram 3,5 vezes desde janeiro, diz pesquisa

Rafael Rigues 26/03/2020 12h30

What to Expect

3x
Faster Backups

6x
Faster Restores

SLAs
Guaranteed

$$
Lowest TCO

Unmatched
Security

Available disk targets for backups

Performance | Cost/Benefit

Conventional Storage

Fast Backup (write speed)

Fast Restore (read speed)

High Retention Cost

InLine Dedupe Backup Appliance

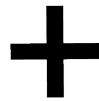Backup (Dedupe first, write later)

Restore (Rehydrate first, restore later)

Low retention cost

ExaGrid Tiered Backup Storage

ExaGrid Disk-cache Landing Zone
Performance Tier
For High Speed Backups and Restores

+

ExaGrid Long-term Retention Repository
Retention Tier
For Cost Efficiency

EXAGRID®

ExaGrid Disk-cache Landing Zone
Performance Tier

ExaGrid Long-term Retention Repository
Retention Tier

Pros
Fast for backups
Fast for restores

Pros
Lower disk usage
Least expensive option

# ExaGrid Scalability – Scale-out & Hyper-converged

ExaGrid Disk-cache Landing Zone
Performance Tier

ExaGrid Long-term Retention Repository
Retention Tier

ExaGrid Disk-cache Landing Zone
Performance Tier

ExaGrid Long-term Retention Repository
Retention Tier

ExaGrid Disk-cache Landing Zone
Performance Tier

ExaGrid Long-term Retention Repository
Retention Tier
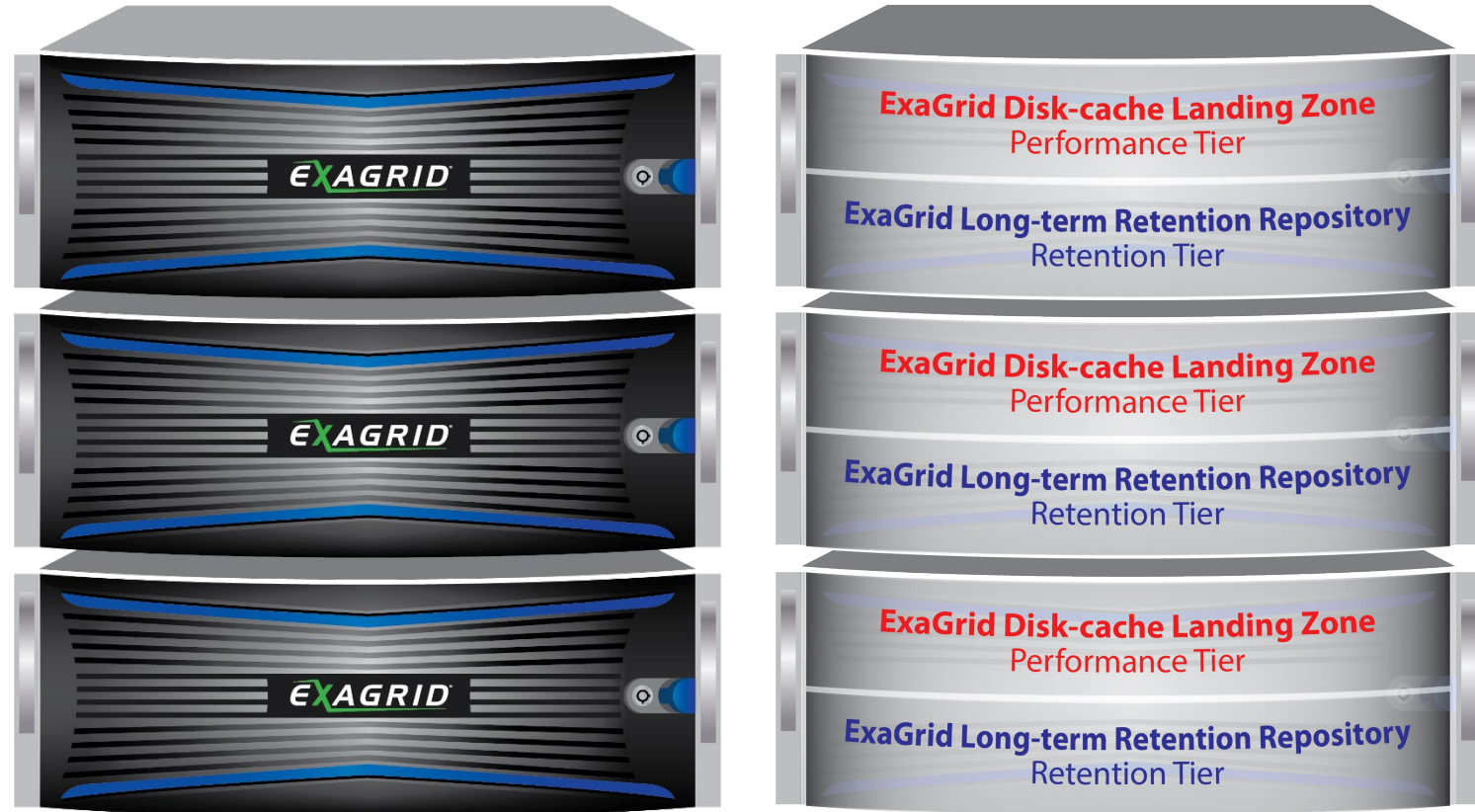
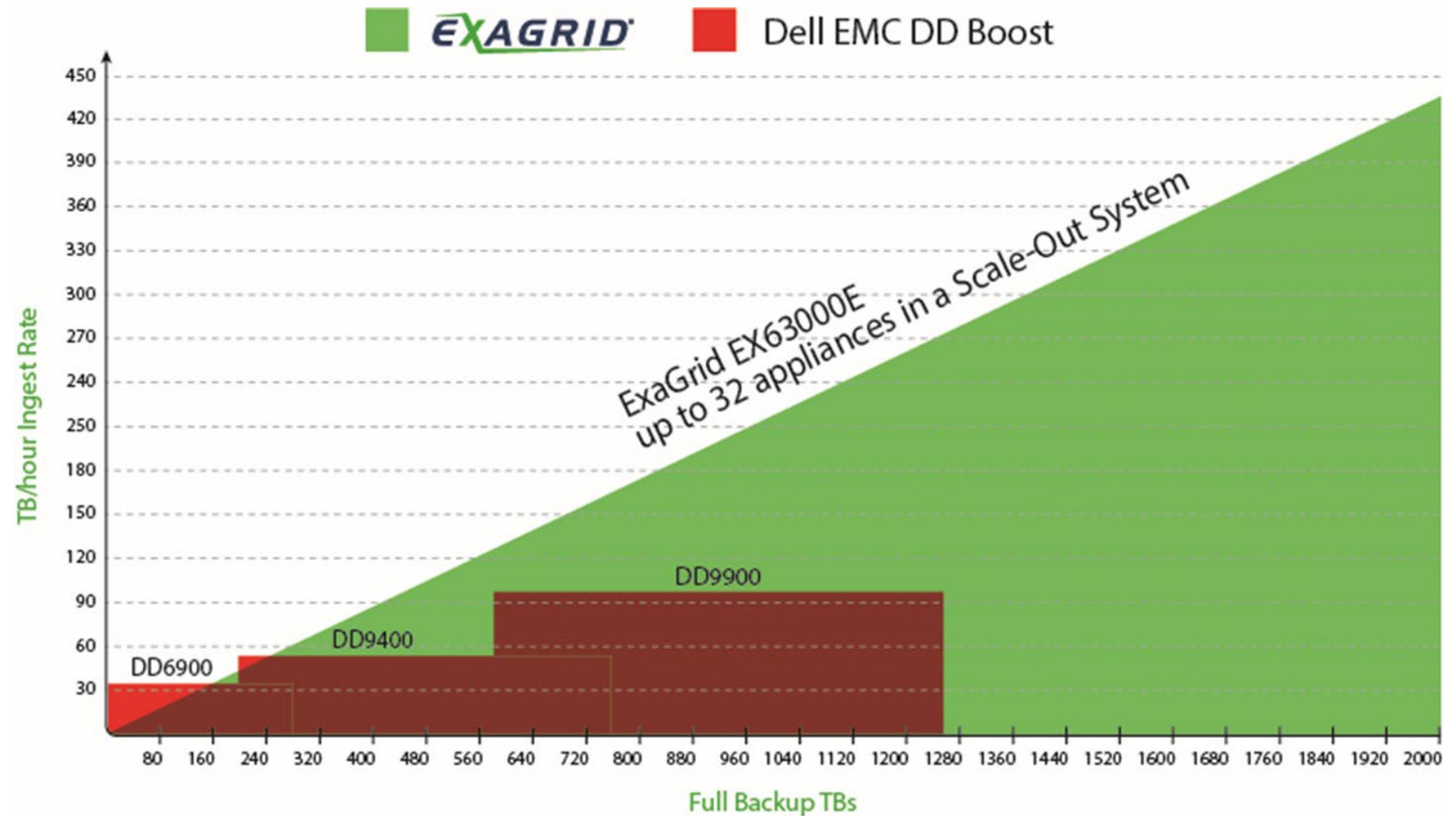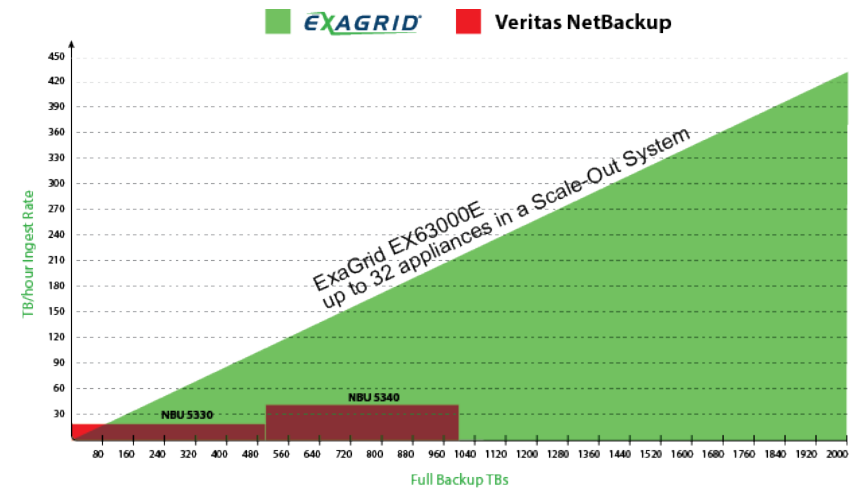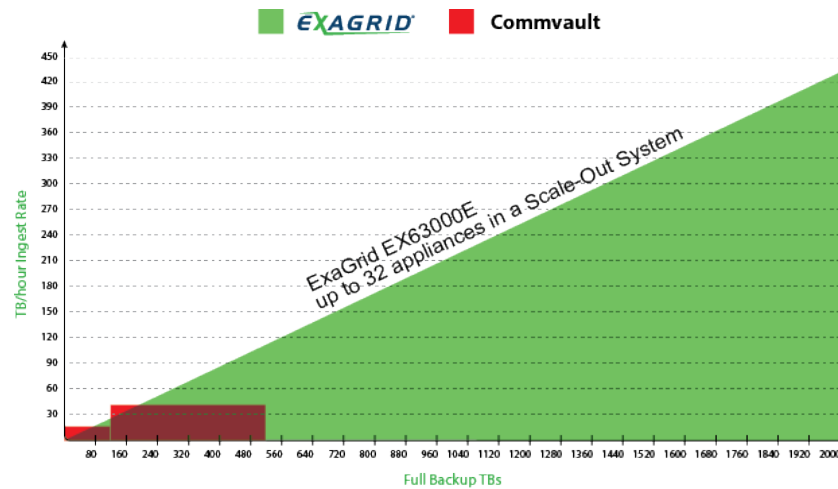# ExaGrid vs In-Line/Scale-up technology

Backup
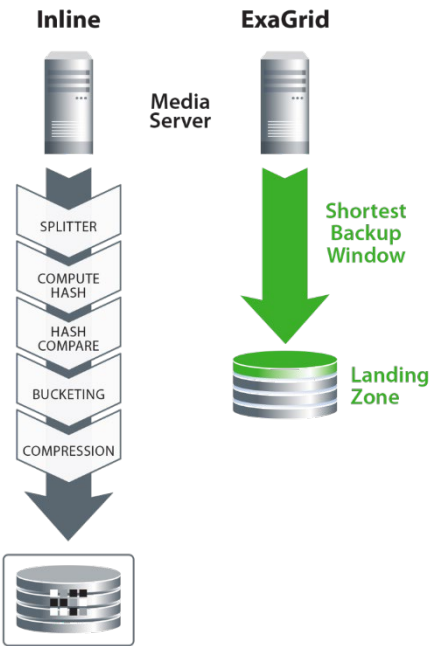
Restore
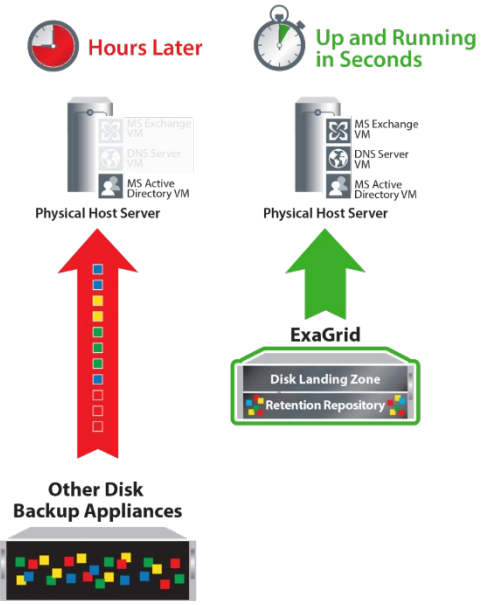
Ingest Performance of Scale-Out vs. Scale-Up

Ingest Performance of Scale-Out vs. Scale-Up

Works with Industry Leading Backup Applications
Heterogeneous Environments

UNIQUE Integrated Data mover

VMs & Infrastructure

VM VM VM VM | VM VM VM VM
VMware | **Hyper-V**

Veeam Backup Server

Backup Proxy

Data Mover

EX-V

Incremental | Synthetic Full | Backup Repository

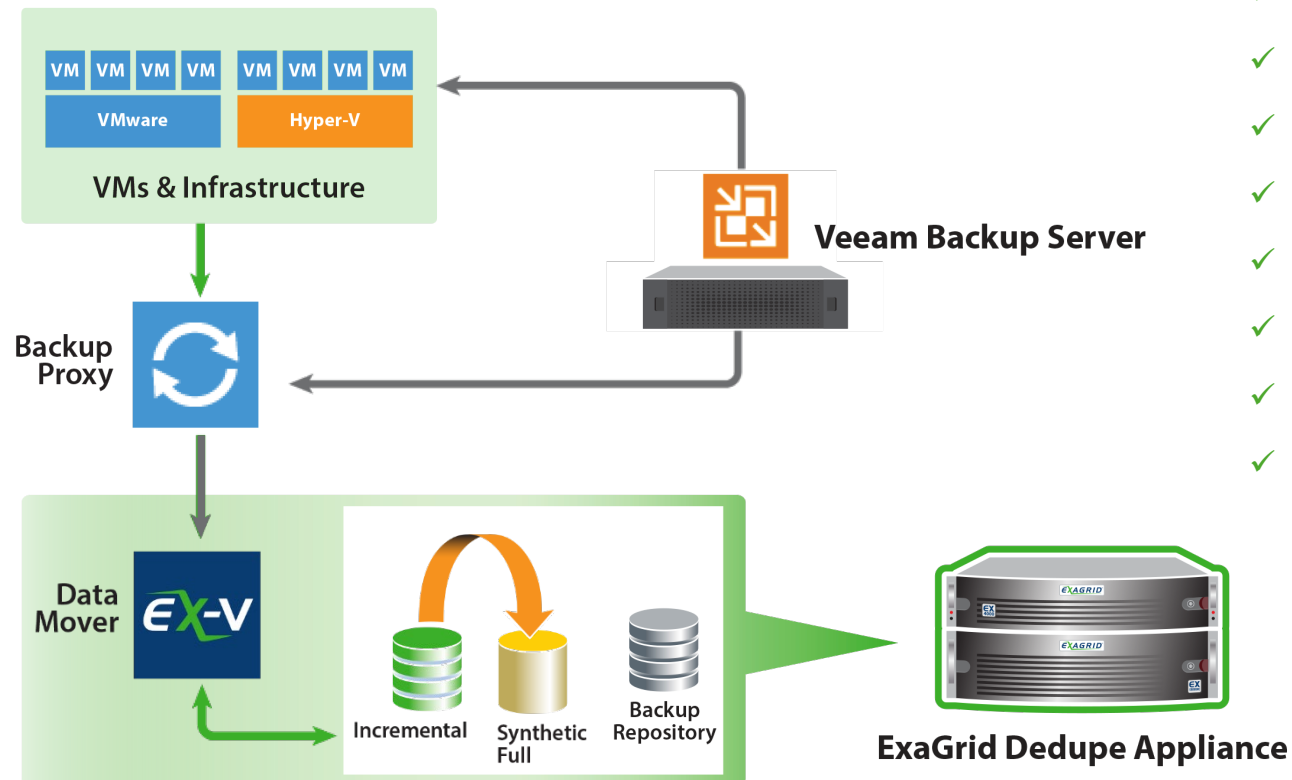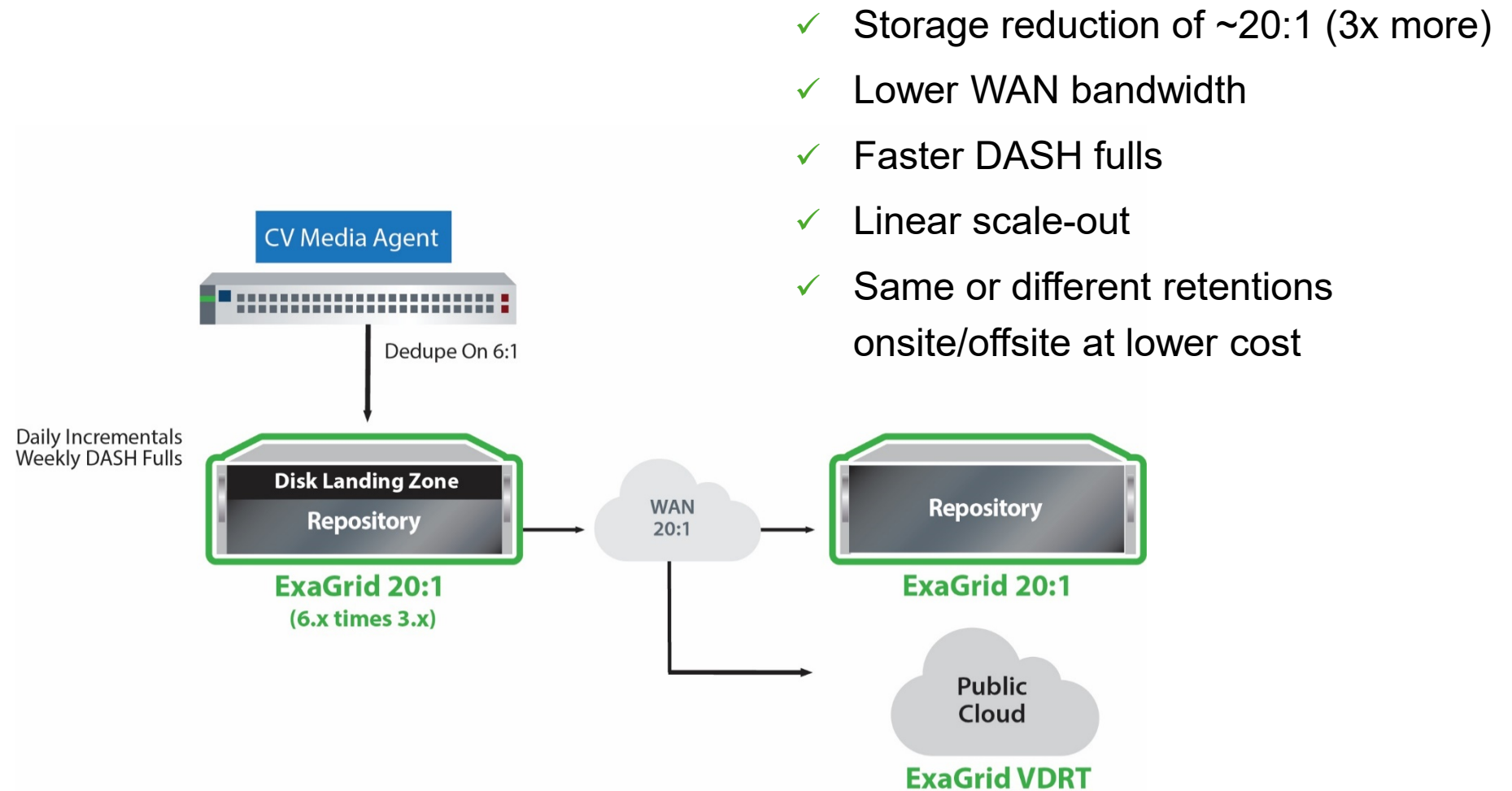**ExaGrid Dedupe Appliance**

- ✓ Storage reduction of ~20:1 (3x more)
- ✓ Lower WAN bandwidth
- ✓ 30% Faster Backups
- ✓ 20x Faster VM Boot
- ✓ Ransomware Proof
- ✓ 6x Faster Synthetic fulls
- ✓ Reduced Veeam Infra
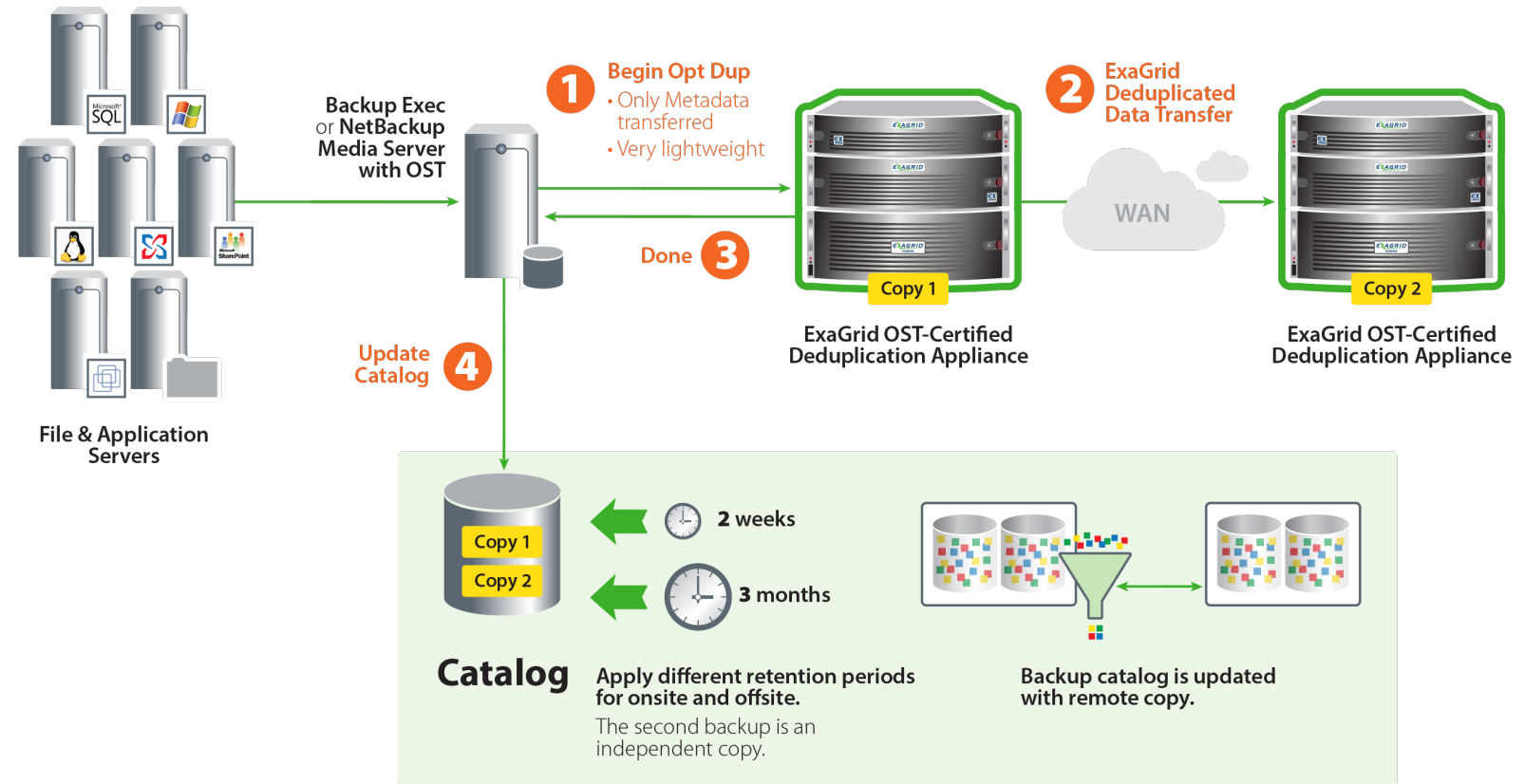- ✓ Support for Veeam SOBR
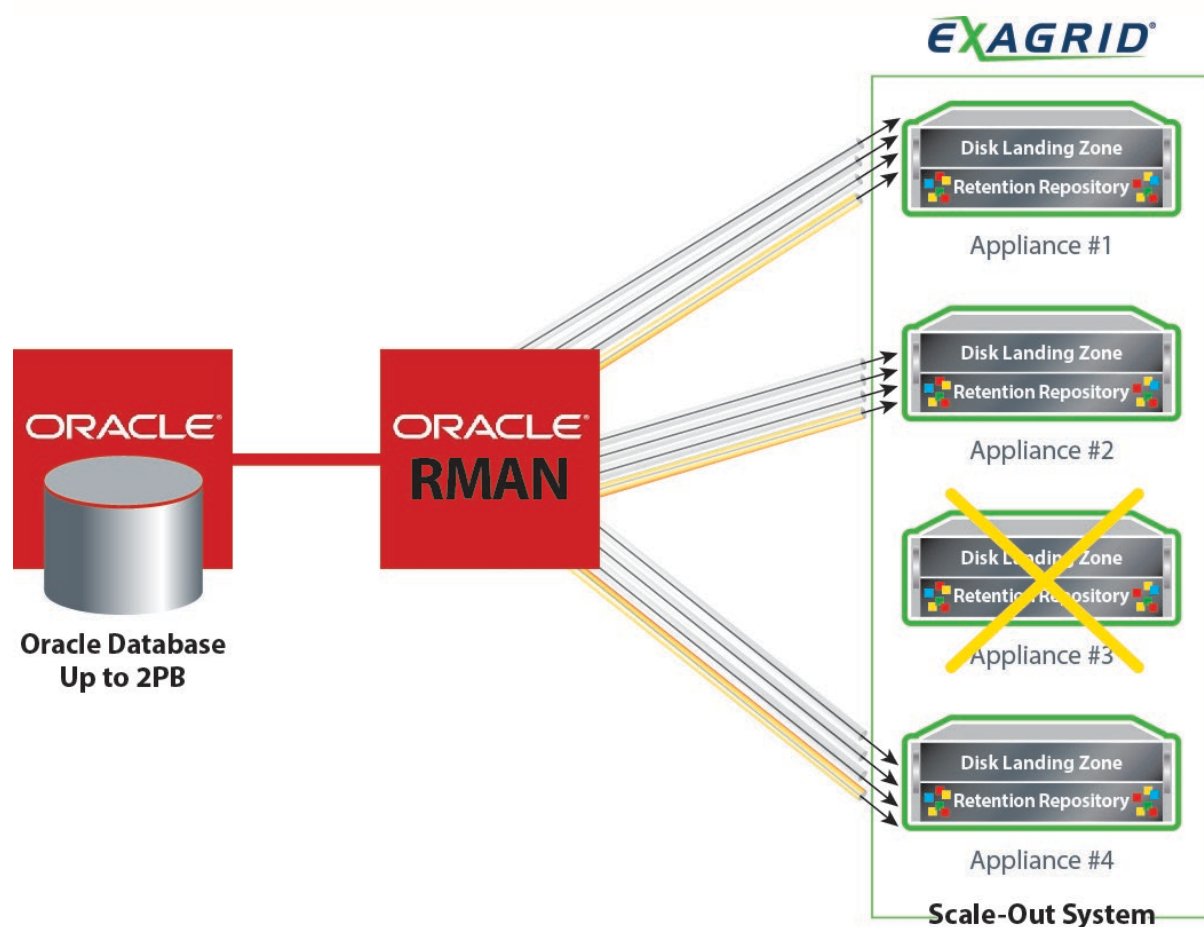
COMMVAULT®

Only Dedupe ON in the Market!!

✓ Storage reduction of ~20:1 (3x more)

✓ Lower WAN bandwidth

✓ Faster DASH fulls

✓ Linear scale-out

✓ Same or different retentions onsite/offsite at lower cost

CV Media Agent

Dedupe On 6:1

Daily Incrementals
Weekly DASH Fulls

Disk Landing Zone
Repository

ExaGrid 20:1
(6.x times 3.x)

WAN
20:1

Repository

ExaGrid 20:1

Public
Cloud

ExaGrid VDRT

Integrated with Veritas OST

VERITAS™

Begin Opt Dup
1. Only Metadata transferred
   - Very lightweight

2 ExaGrid Deduplicated Data Transfer

Done 3

Update Catalog 4

Backup Exec or **NetBackup** Media Server with OST

File & Application Servers

Copy 1

ExaGrid OST-Certified Deduplication Appliance

WAN

Copy 2

ExaGrid OST-Certified Deduplication Appliance

Catalog

Copy 1
Copy 2

2 weeks

3 months

Apply different retention periods for onsite and offsite.

The second backup is an independent copy.

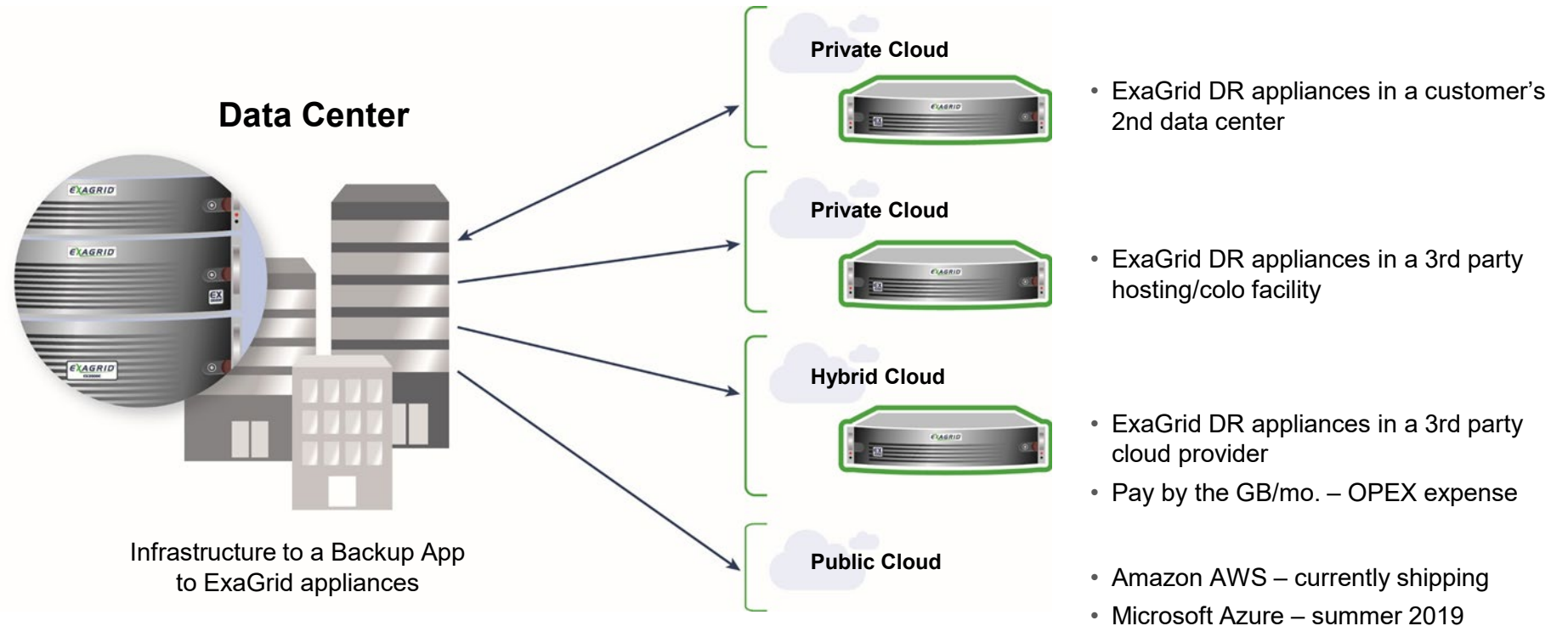**Backup catalog is updated with remote copy.**

ORACLE®

Fastest RMAN Backups with Failover and RMAN Channels

- ✓ Fastest backups
- ✓ Restore in Seconds
- ✓ 2PB full database backup in a single system
- ✓ Performance load balancing
- ✓ RMAN failover if any appliance fails

DR Scenarios

Data Center

Private Cloud

• ExaGrid DR appliances in a customer's 2nd data center

Private Cloud

• ExaGrid DR appliances in a 3rd party hosting/colo facility

Hybrid Cloud

• ExaGrid DR appliances in a 3rd party cloud provider
• Pay by the GB/mo. – OPEX expense

Public Cloud

• Amazon AWS – currently shipping
• Microsoft Azure – summer 2019

Infrastructure to a Backup App
to ExaGrid appliances

• Adaptive deduplication deduplicates and replicates in parallel

• 50:1 WAN bandwidth efficiency

• Bandwidth throttle and WAN encryption for data replication

• Configure the disaster recovery site to all repository to save cost

Multi-site Data Center Disk Backup Topology
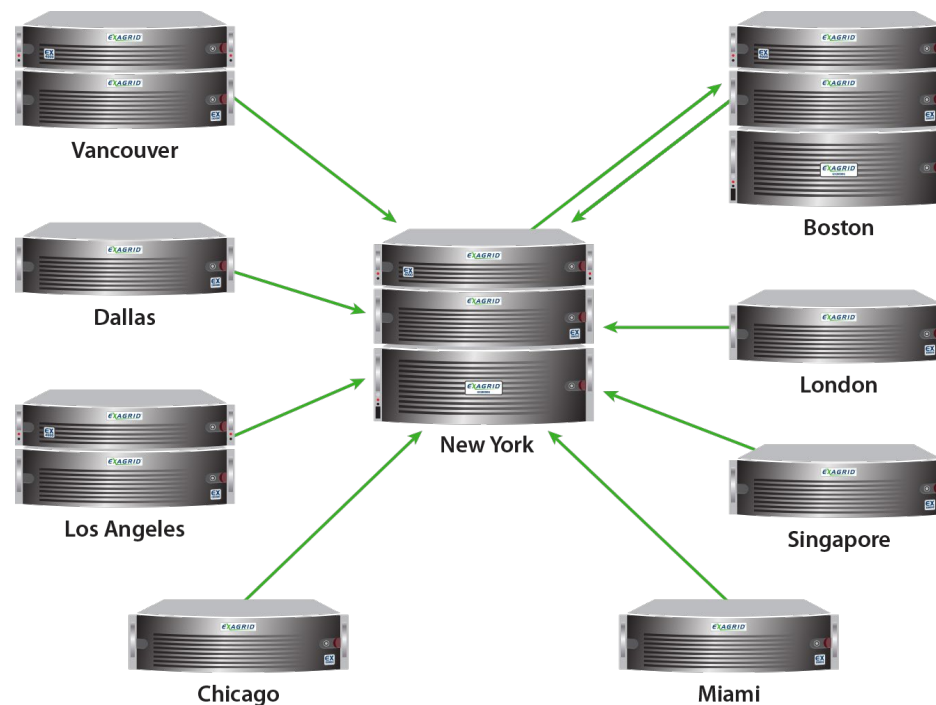
Multi-site Architecture

- 16 locations in a single group – spoke and hub
- 50:1 WAN efficiency across all sites
- Management from single UI
- Cross-site protection between sites
- Consolidated DR copies of backup reduces costs

94% of organizations get their data back

While 73% of ransomware attacks succeed in encrypting data, the good news is that 94% of organizations affected managed to get their data back.

As we've seen, 26% got their data back by paying the ransom. However, more than double that (56%) restored their data using backups. The remaining 12% said that they got their data back through other means.


73%
Of attacks result in data being encrypted

94%
Of victims get their data back

56%
Used backups to get the data back

Here's the well-worn MO: Attackers infect one or more systems with crypto-locking malware, then demand a ransom, typically payable in bitcoins, for the promise of a decryption tool. Law enforcement and security experts continue to recommend that organizations maintain offsite backups and fast-restore capabilities, so they never need to consider paying (see: *Baltimore Ransomware Carnage Compounded by Local Storage*).

4. **Make regular backups and store offsite and offline.** 56% of organizations whose data was encrypted restored their data using backups last year. Using backups to restore your data considerably lowers the costs of dealing with the attack compared with paying the ransom.
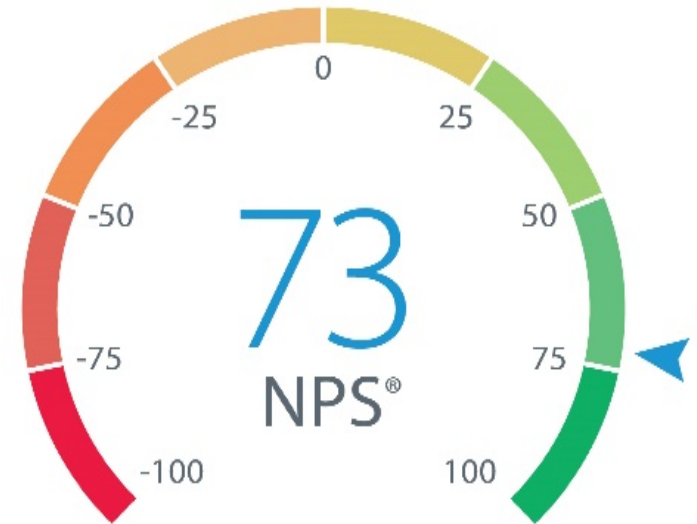
Never pay a Ransom (again)
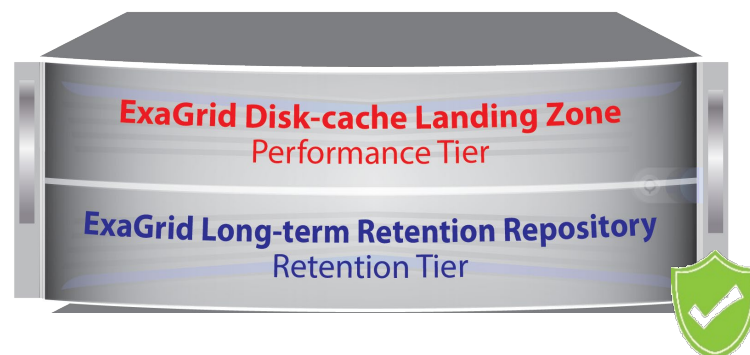
Tiered Storage
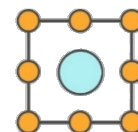
Data Isolation

Intelligent Retention-Lock

Personal Touch - Maintenance and Support

World-Class Support

73 NPS®

Customers give ExaGrid
NPS score of +73

ExaGrid Appliances in a Scale-out System
32 Appliances in a Single System – 4PB Usable Capacity
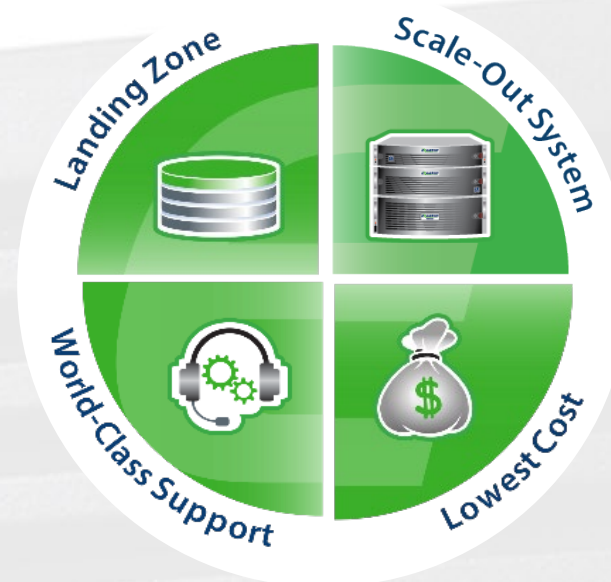
ExaGrid Model	Usable Capacity (TB)	Max Backup Thruput (TB/hr)
EX3000	6	0.72
EX5000	10	1.08
EX7000	14	2.40
EX10000E	20	2.40
EX13000E	28	2.40
EX21000E	42	4.32
EX32000E	66	7.56
EX40000E	78	8.00
EX63000E	126	13.50

Stress-free backup storage

Obrigado por sua Atenção