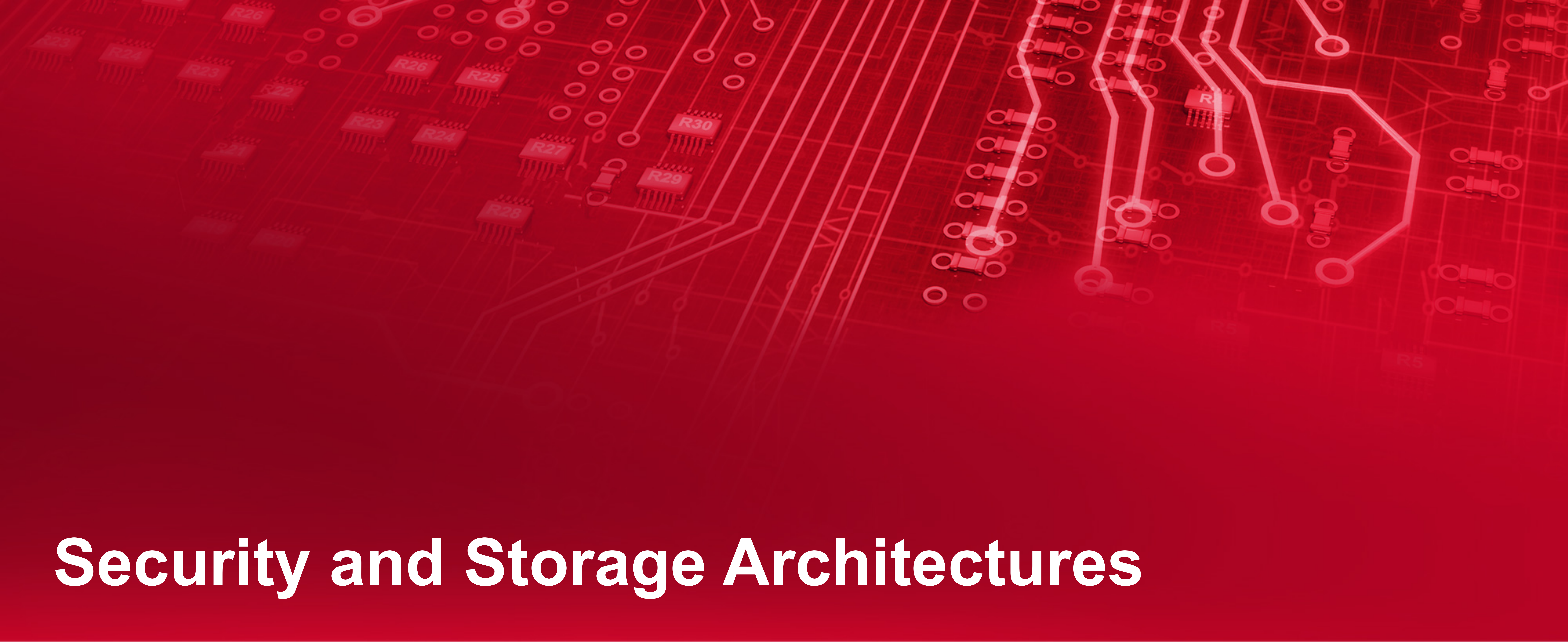
BROADCOM®

your trusted partner

Security and Storage Architectures



Security and Storage Architectures

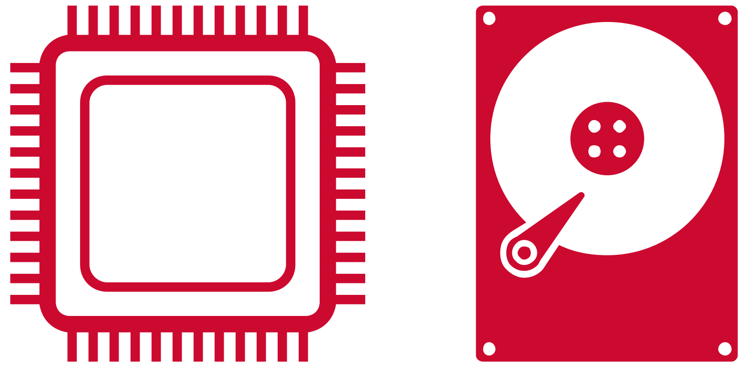
Dr. Chip Copper, R&D

April 25th, 2019

BROADCOM®

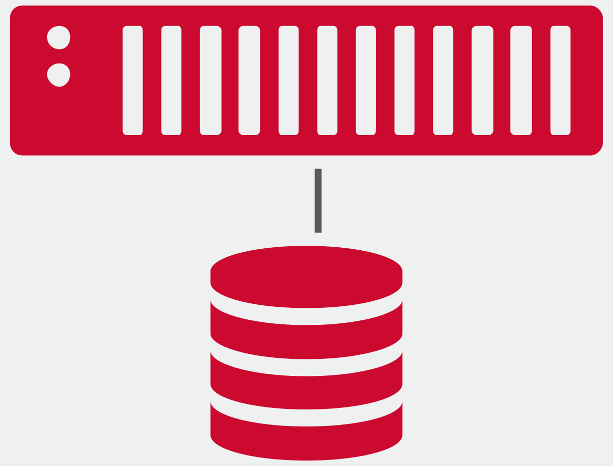
SAN Architecture is Fundamentally Different

- The abstraction of a typical application environment is simple
  - Processing (CPU)
  - Data (Storage)



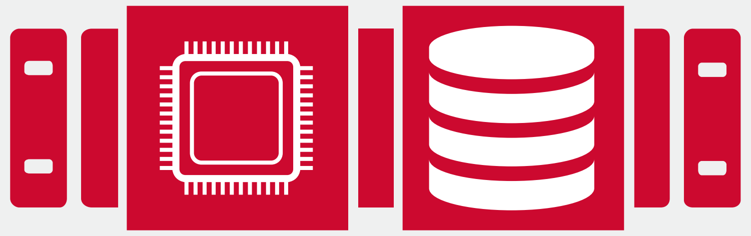
- This abstraction ignores the physical implementation of the connection between the two

1



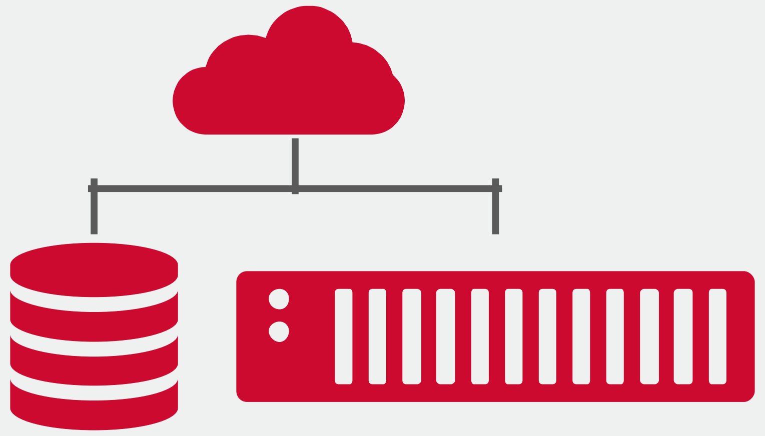
Direct attach to a raw volume (PCI/M.2/SATA)

2



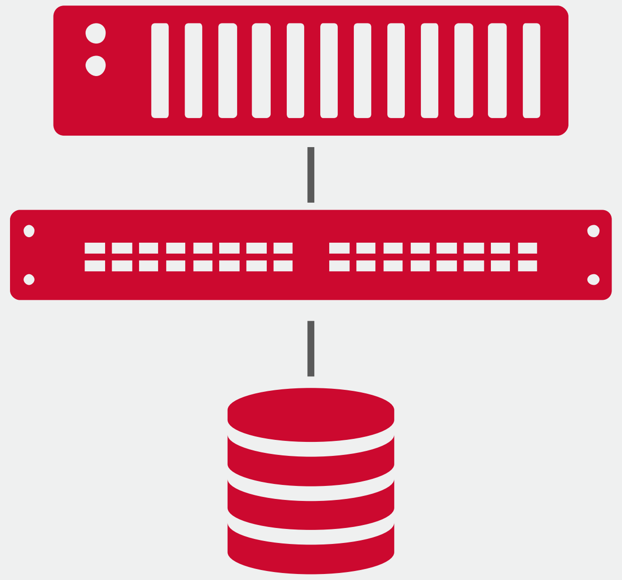
Virtualized (Contained within other storage volumes)

3



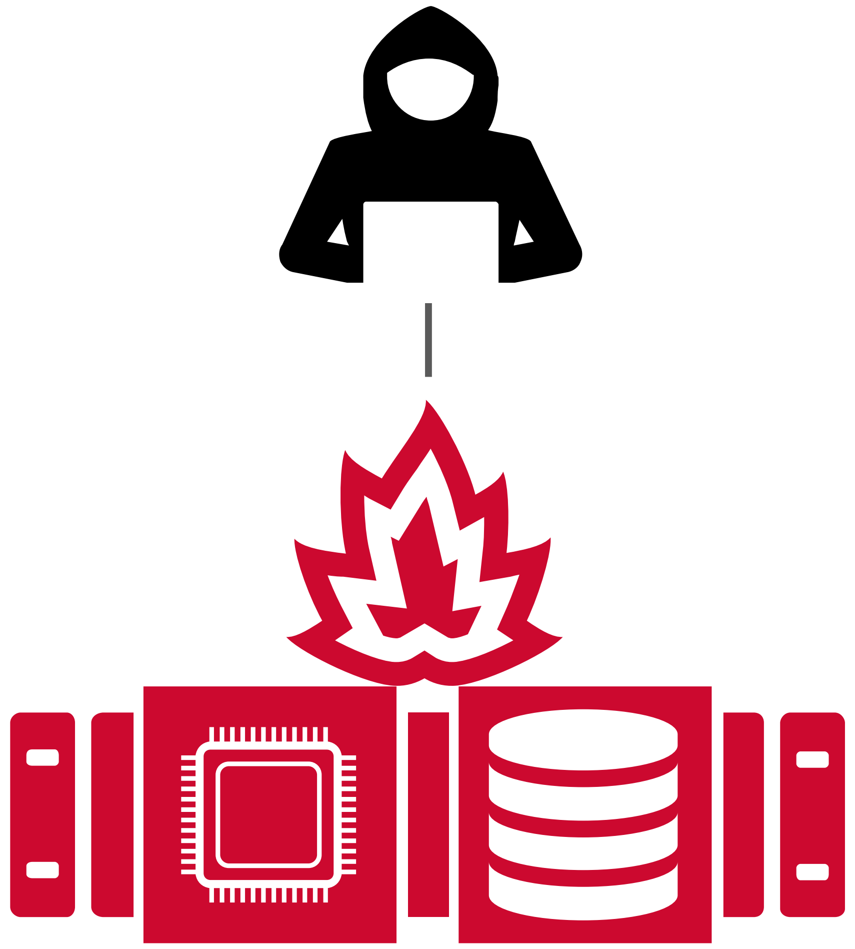
IP network attached (A distinct communications link)

4

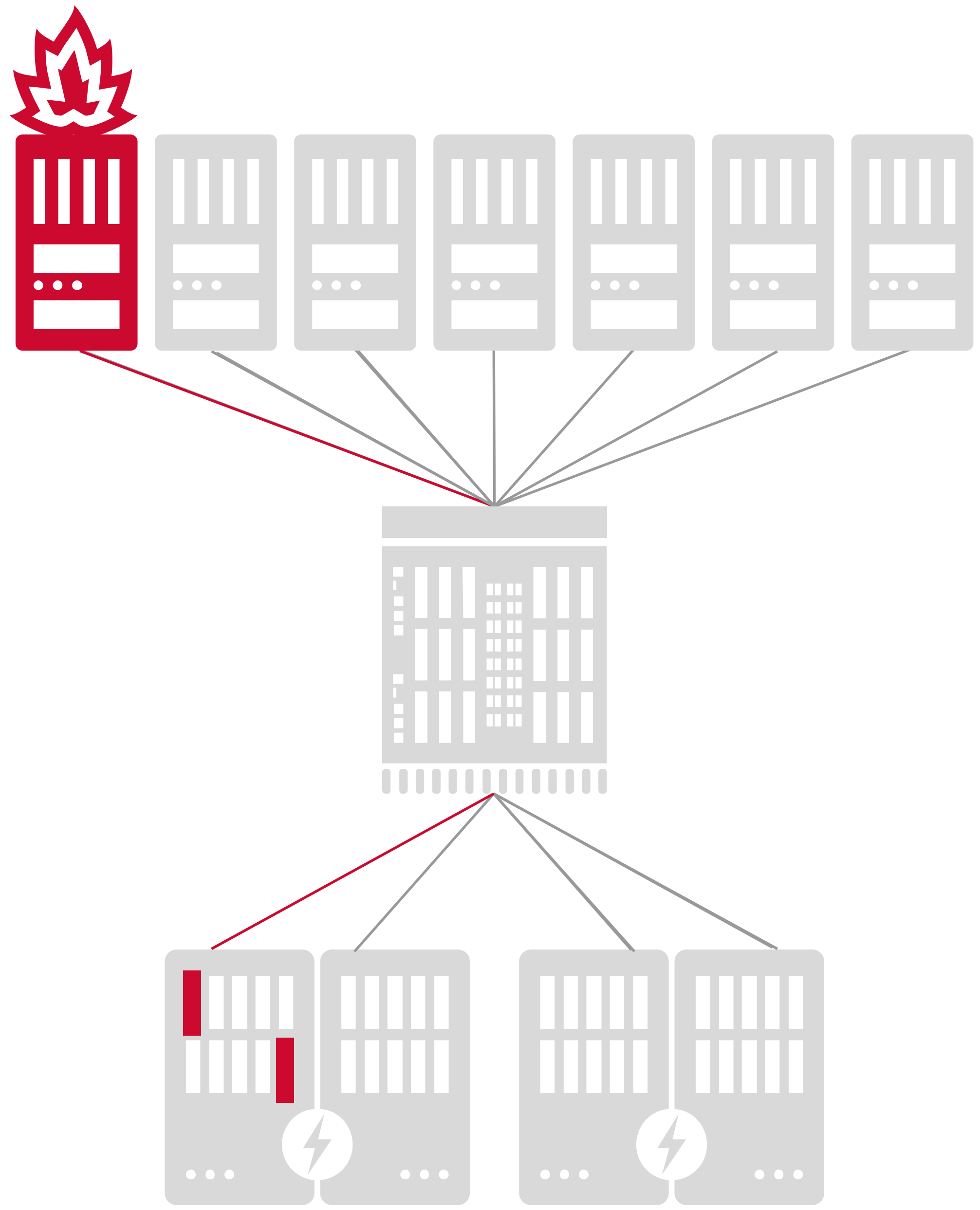


Storage attached network (A dedicated storage link)

Administrative Domains of Control

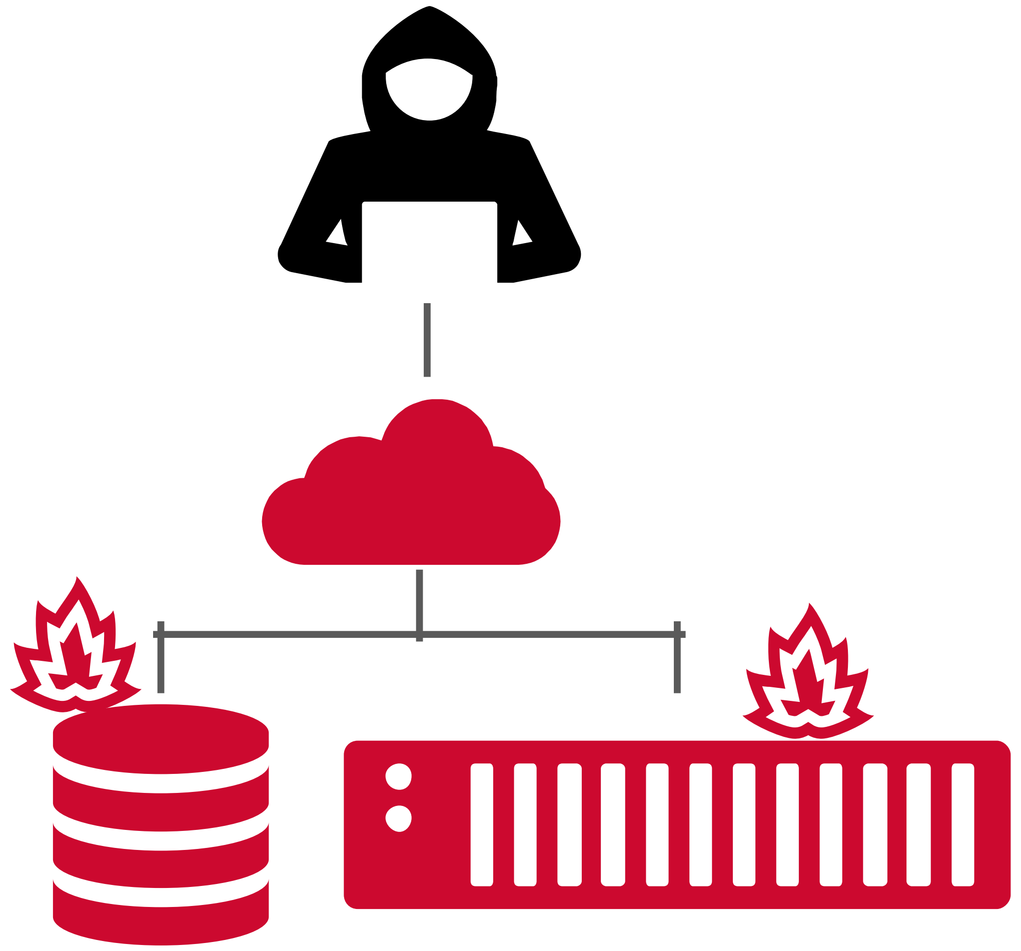


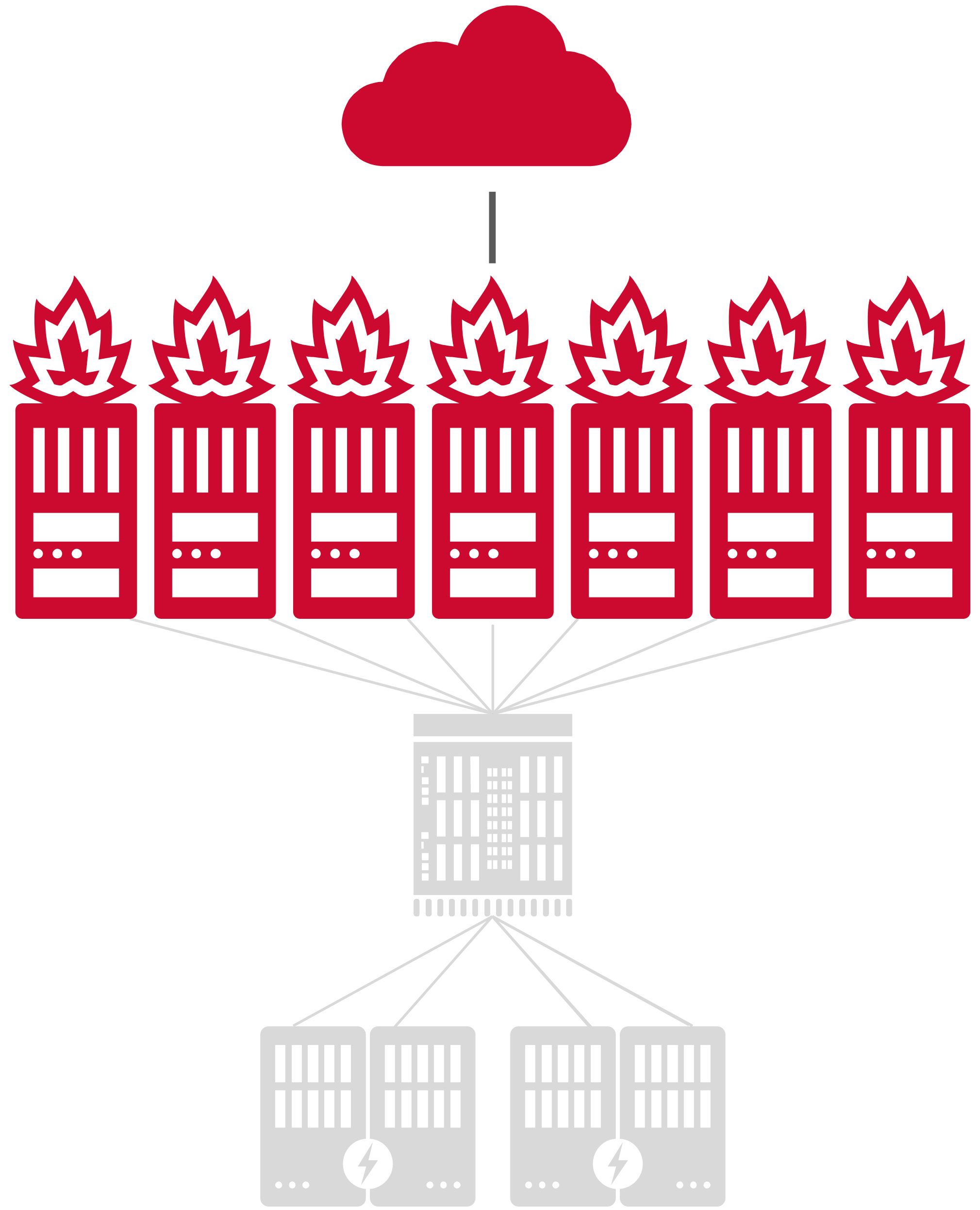
- **HCI/Single Platform**
  - Control of processing and storage under the control of one domain
  - The processing platform is the gateway to the “outside world”
  - It is therefore the most likely attack target
  - The compromise of that platform impacts both apps and storage
  - Can be especially wide reaching if administrative control spans nodes



- **Storage Area Networks (SAN)**
  - The risk is limited to those volumes explicitly presented to apps on that platform
  - Because the platform has control of the volumes, the contents are at risk but not control of the volumes
  - The volumes cannot be contaminated and redistributed by a compromised host

Storage as Target of Attack





- **Shared IP storage Network**
  - Host attached storage/IP storage arrays may be attacked directly
  - Any storage which can be addressed via IP is a direct target
  - Compromising any host gives a platform for possible direct attack
  - iSCSI/HCI/Direct attached hosts will surrender their storage if breeched

- **Storage Area Networks (SAN)**
  - SAN attached storage has no direct exposure to IP networks
  - All data transfers take place over Fibre Channel
  - The Fibre Channel network is a data plane, not a control plane
  - Fibre Channel requires special hardware and protocols
  - Direct attacks are much more difficult and would require control plane access

Storage Policy Enforcement

- Where is storage policy enforced?
  - Which applications can see which volumes
  - What type of access will apps have (RW/RO)

HCI/Direct Attached

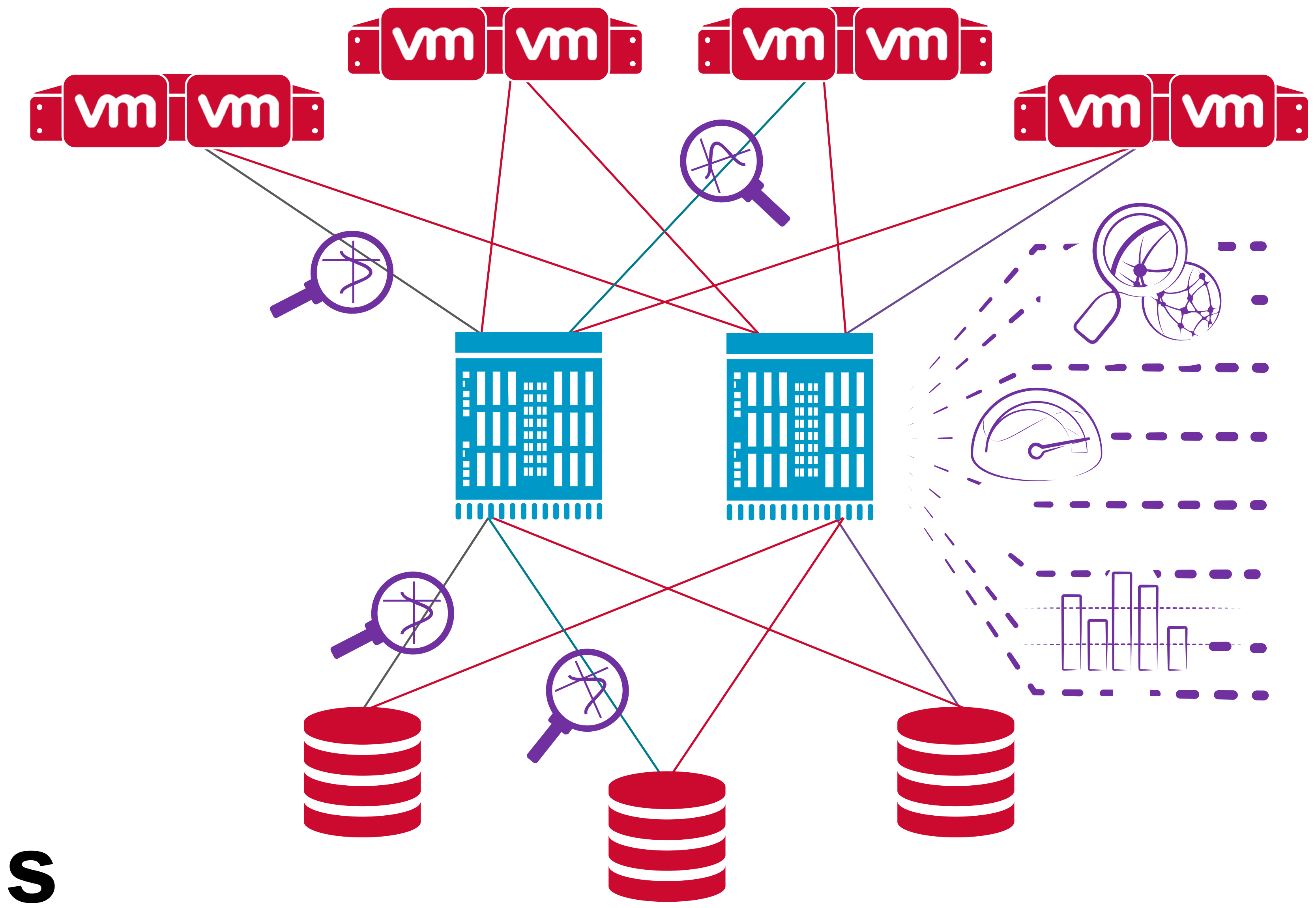
- HCI/Direct Attach hosts enforce their own policies
  - A compromised or rogue host can decide to change policy
  - All volumes under the control of the node impacted
  - Not just those mounted to those applications

Storage Area Network (SAN)

- SAN-Attached storage allows policy to be enforced separately
  - A read-only volume cannot be changed to read-write by the processing platform
  - Content can be immediately separated from nodes if policy violations occur
  - Much more difficult if there is no separate domain of control

Visibility of I/O Traffic Patterns

- **HCI/Single Platform**
- HCI/Direct-attached provides no natural interception point for observing I/O patterns
  - – If system counters are used, the very use of the counters may impact the performance of the applications platforms
  - – PCIe snoopers are expensive and intrusive and do not provide a scalable solution



- **SANs**
- Allow for the non-intrusive monitoring of I/O traffic
  - – The level of granularity goes all the way down to the virtual machine level
- This visibility provides a perfect data source for machine learning and intelligent security tools
  - – ML can watch and learn typical and expected traffic patterns and can trigger alerts to indicate something has changed

SAN Storage Advantages

- SAN storage can have specialized features not typically found in HCI/Direct-attach storage

Allows links to recover without performance degradation

Identify network and media errors remotely

Automatic mitigation of misbehaving devices

Optics and cable integrity tests

Automatic bit corruption recovery

Prioritizes traffic in congested networks

- Snapshot with no application impact
  - Quickly restore data in the event of corruption or loss
  - Create data set images for testing and analytics
  - Strong protection against Ransomware
- De-dup/compression save disk space
- Scalability beyond ranges typically found in HCI/Direct-attach

Summary

- SANs offer security benefits not found in other architectures
- This is not because of a feature set
- It is due to the inherent features of SAN attachment characteristics
  - Separate domain of control
  - No direct attack path because of insulating storage infrastructure
  - Independent policy enforcement
  - Visibility of traffic for analytics and verification
  - Advanced features found only on specialized storage arrays
- This may not be why you chose a SAN, but it is certainly a nice side effect

Thank You