Privacy & Security in Practice

Alex McDonald
Standards & Industry Association Group
CTO Office, NetApp
18 May 2017

NetApp

Agenda

1. Background
2. Cloud; The Poster Child for Security & Privacy Concerns
3. Recommendations

General Data Protection Regulations

European Union

- General Data Protection Regulation (GDPR)
- Country specific laws
- Cloud computing directive
- Data sovereignty obligations
- Cybersecurity directive
- Anti-SPAM laws
- Healthcare Privacy Laws
- Data breach regulations
- BREXIT

United States

- Federal Privacy Act (Consumer)
- NIST Regulations
- Cybersecurity Executive Order(Voluntary)
- Data breach regulations
- HIPAA/HITECH
- Regulated industries
- State Regulations
- Proposed Privacy Shield

Asia Pacific Rim

- Country-specific privacy laws
- PHI Privacy Laws
- APEC cyber privacy code
- Cross Border Privacy Rules (CBPR)
- Restrict marketing activities
- Restrictions on cloud computing
- Data breach regulations

Canada

- Privacy Act
- Personal Information Protection and Electronic Documents Act (PIPEDA)
- Digital Privacy Act 2015
- Provincial/ Sovereignty Laws
- Medical Records Laws
- Cybersecurity Regulations
- Anti-SPAM Laws (CASL)
- Data Breach Regs

Latin America

- Cross-border transfer restrictions
- Country-specific privacy laws
- Personal Health Information Privacy Laws
- Cloud computing regulations
- OAS cybersecurity guidelines
- Data breach regulations

Privacy Versus Data Protection

4

NetApp

Data Protection: Various Definitions

- Data Protection (Storage)
  - Assurance that data is not corrupted, is accessible for authorized purposes only, and is in compliance with applicable requirements
    - Source: Storage Networking Industry Association Dictionary
- Data Protection (Security)
  - implementation of appropriate administrative, technical or physical means to guard against unauthorized intentional or accidental disclosure, modification, or destruction of data
    - Source: ISO/IEC 2382:2015
- ISO/IEC 27040; Standard for Storage Security

ISO/IEC 27040

- Scope:
  - Technical guidance on how organizations may define an appropriate level of risk mitigation by employing a well-proven and consistent approach to the planning, design, documentation and implementation of data storage security
- Applicability
  - Security of devices and media
  - Security of management activities related to the devices and media
  - Security of applications and services
  - Security relevant to end-users
- Relevance
  - Anyone owning, operating or using data storage devices, media and networks
  - Senior managers, acquirers of storage product and service, and other non-technical managers or users
  - Information/storage security focused managers and administrators
  - Anyone involved in the planning, design and implementation of the architectural aspects of storage network security

Agenda

1. Background
2. Cloud; The Poster Child for Security & Privacy Concerns
3. Recommendations

Cloud Security Considerations

IaaS	PaaS	SaaS
Virtual Machine	System/Resource Isolation	Data Segregation
Virtual Network	User Level Permissions	Data Access and Policies
Hypervisor	User Access Management	Web Application Security
VM-based Rootkits		
vSwitch Attacks		
Denial-of-Service Attacks		
Co-location		

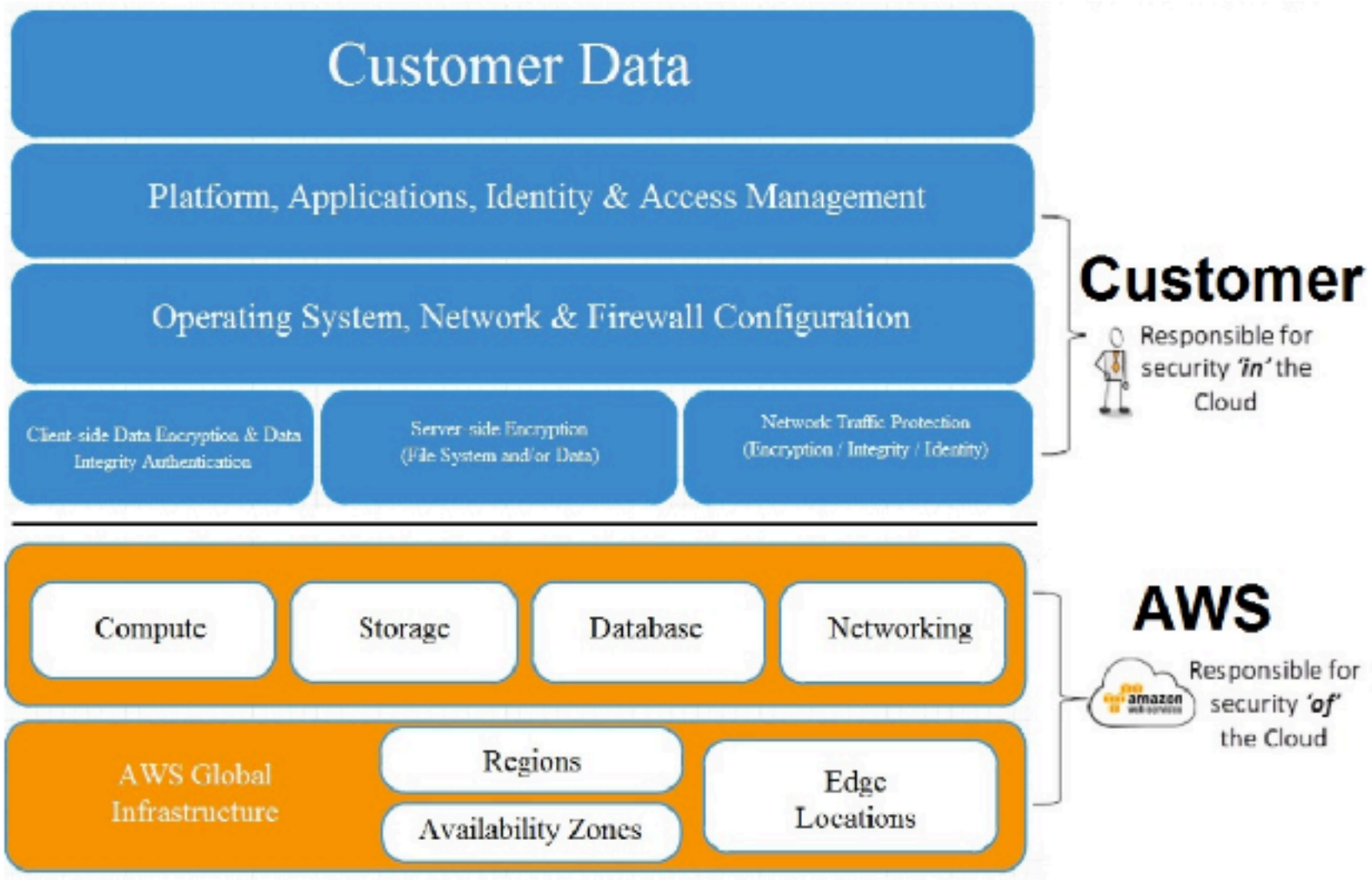
Who is Responsible for What? The Shared Responsibility Model

Cloud Security Alliance model

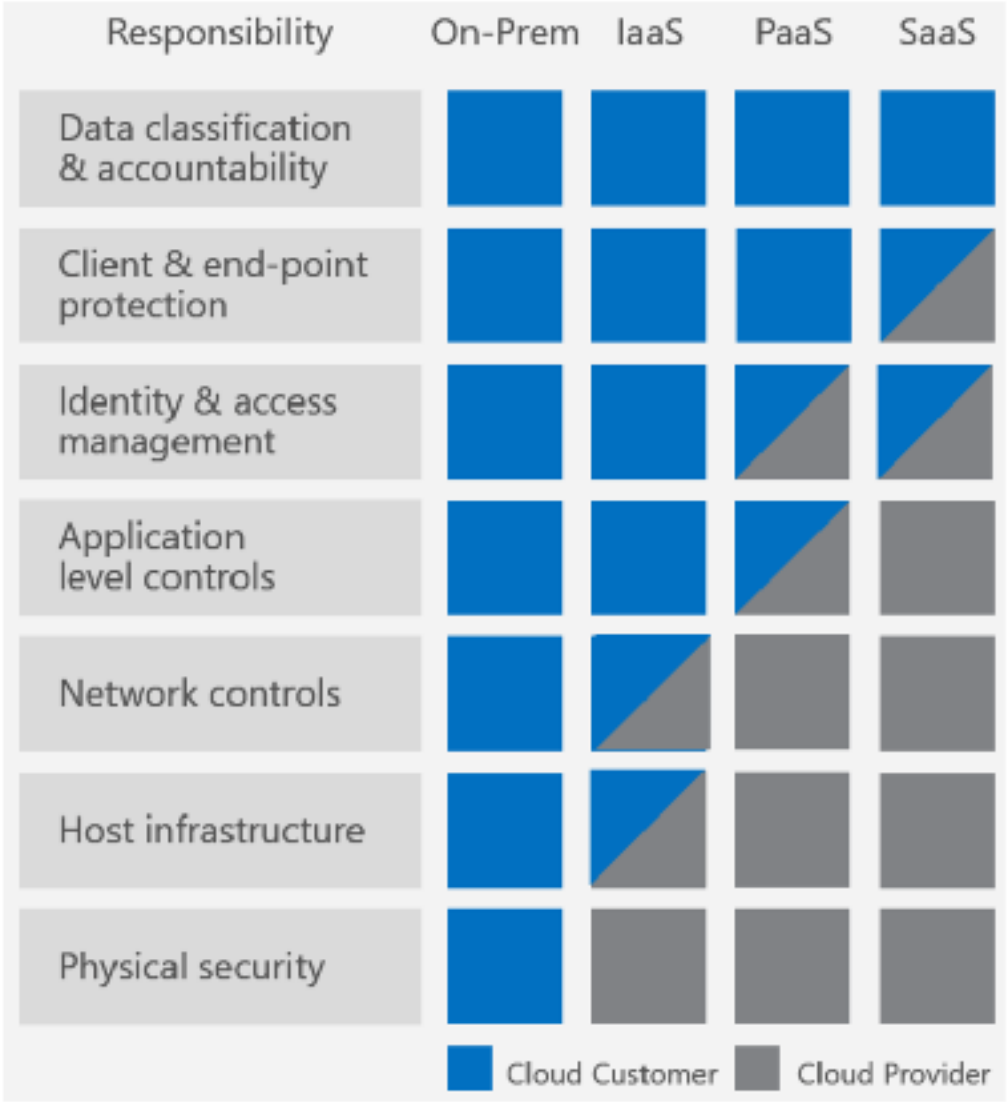
IaaS	PaaS	SaaS
User Access/Identity	User Access/Identity	User Access/Identity
Data	Data	Data
Application	Application	Application
Operating System	Operating System	Operating System
Virtualization	Virtualization	Virtualization
Network	Network	Network
Infrastructure	Infrastructure	Infrastructure
Physical	Physical	Physical

Enterprise Managed **Provider Managed**

AWS



Azure



NetApp

Agenda

1. Background
2. Cloud; The Poster Child for Security & Privacy Concerns
3. Recommendations

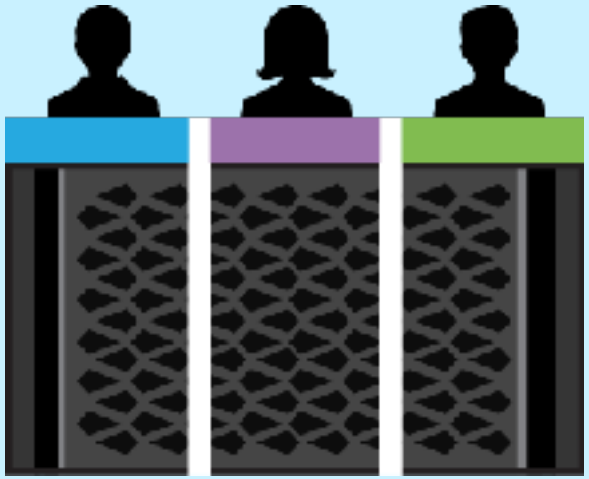
Secure Multi-tenancy (SMT)

End-to-end security and isolation in virtualized, shared environments

"shared pool of configurable computing resources"

– NIST

- Segmentation and isolation
- Different levels of Tenancy in a Data Fabric
  - Cloud Provider
  - Company
  - Groups
- Build in your expectations



Data in Motion

Data that is in transit through network transmission

Data in motion is more susceptible to breach of confidentiality and integrity

- Data transport is over interconnects
- Use hardware based Virtual Private Networks (VPNs)
  - Public Networks
  - Shared resources
- AWS Direct Connect
  - Dedicated, but not encrypted

Data at Rest

Data that is static and not in motion

Ensuring the confidentiality and integrity of data no matter where is in the data fabric

- Don’t use physical security models
- Encrypt, encrypt, encrypt
- Software and hardware based options
- Key Management

Key Management

Keys are used during the encryption process to provide a variable which in conjunction with the cryptographic algorithms, allows for the transformation of plaintext to cipher text or vice versa.

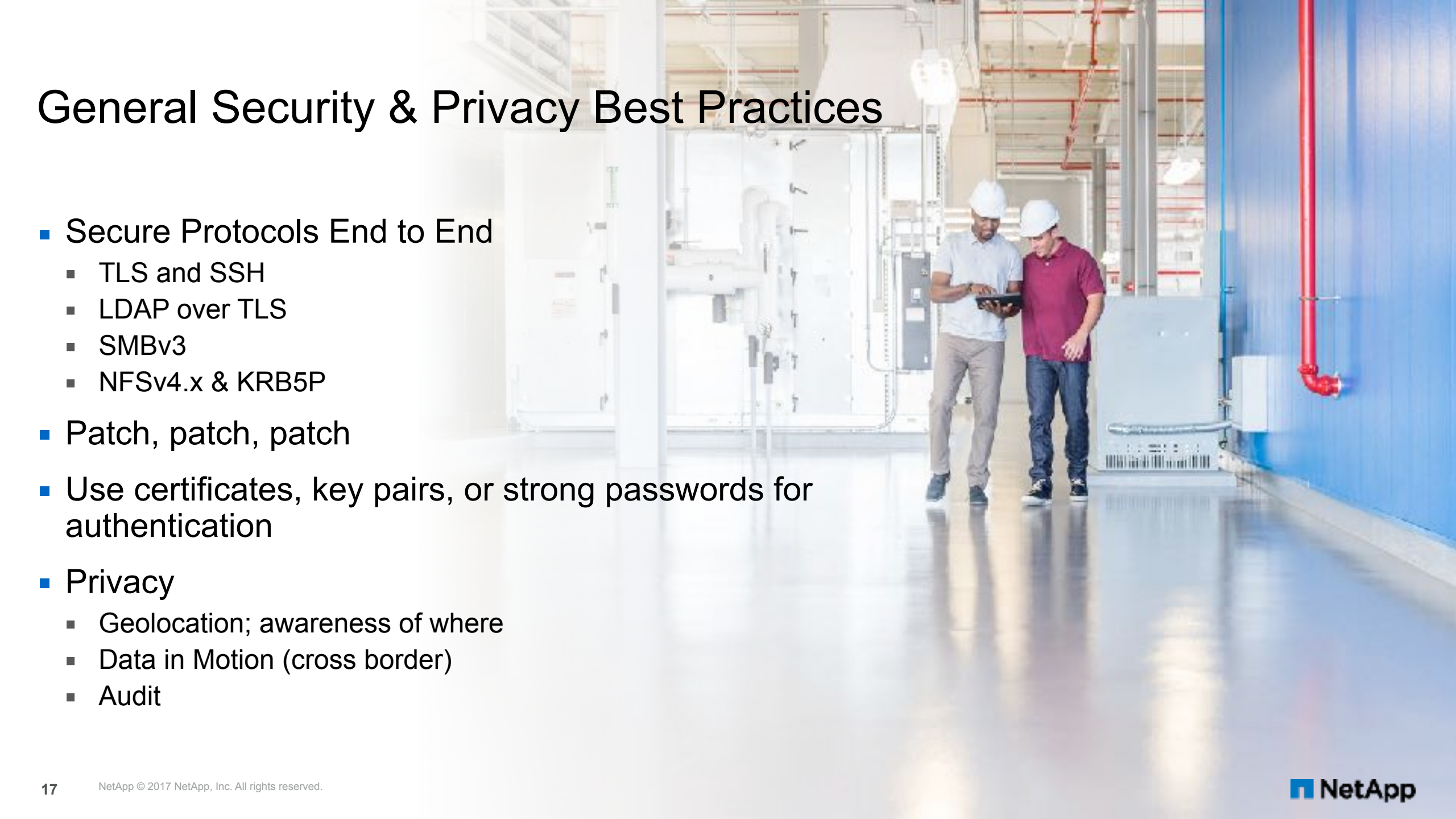
- Keys secure your data
- Asymmetric key cryptography is considered inefficient (PKI)
  - Generally used to exchange a symmetric keys securely
- Symmetric key cryptography is relatively efficient in comparison (AES, 3DES)
- Strong cryptography is only as strong as the key being used
  - Use randomness for key generation
  - Length matters
  - Store and transmit your keys securely
- External, Onboard and Cloud Provider

Data in Use

Data that is being shared or processed

- Shared compute
  - Logical separation
- Work with your provider
- You can get dedicated resources, it will just cost you more

General Security & Privacy Best Practices



- Secure Protocols End to End
  - TLS and SSH
  - LDAP over TLS
  - SMBv3
  - NFSv4.x & KRB5P
- Patch, patch, patch
- Use certificates, key pairs, or strong passwords for authentication
- Privacy
  - Geolocation; awareness of where
  - Data in Motion (cross border)
  - Audit

Thank you

NetApp