Embracing a Secure Cloud

Cloud & Network Virtualisation
India 2017

Cloud Computing

Group of computing resources providing services such as servers, storage, databases, software, applications, networks etc. over the Internet/private network

Benefits

- Flexibility
- Efficiency

Cloud Computing Security Incidents

- Dow Jones Data Leak Results (over 1 million users) sue to an AWS Configuration Error (2017)
- Salesforce Database Failure Wipes Out 5 Hours of Corporate Customer Data (2016)
- Millions of accounts of LinkedIn users have been extracted and put up for sale in Dark Web (2012)
- Intuit Cloud Outage Blocks Access to Financial Software for 36 Hours (2010)

and there are many more…….

Cloud Computing Security Threats

- Sovereignty and legal boundary
- Data leakage
- Compromised credential and broken authentication
- Hacked interface & APIs
- Vulnerabilities & weaknesses
- Malicious insider
- DOS/DDOS attacks
- Shared technology result in common issues

Major challenge for Indian telcos

Sovereignty and

legal boundary of

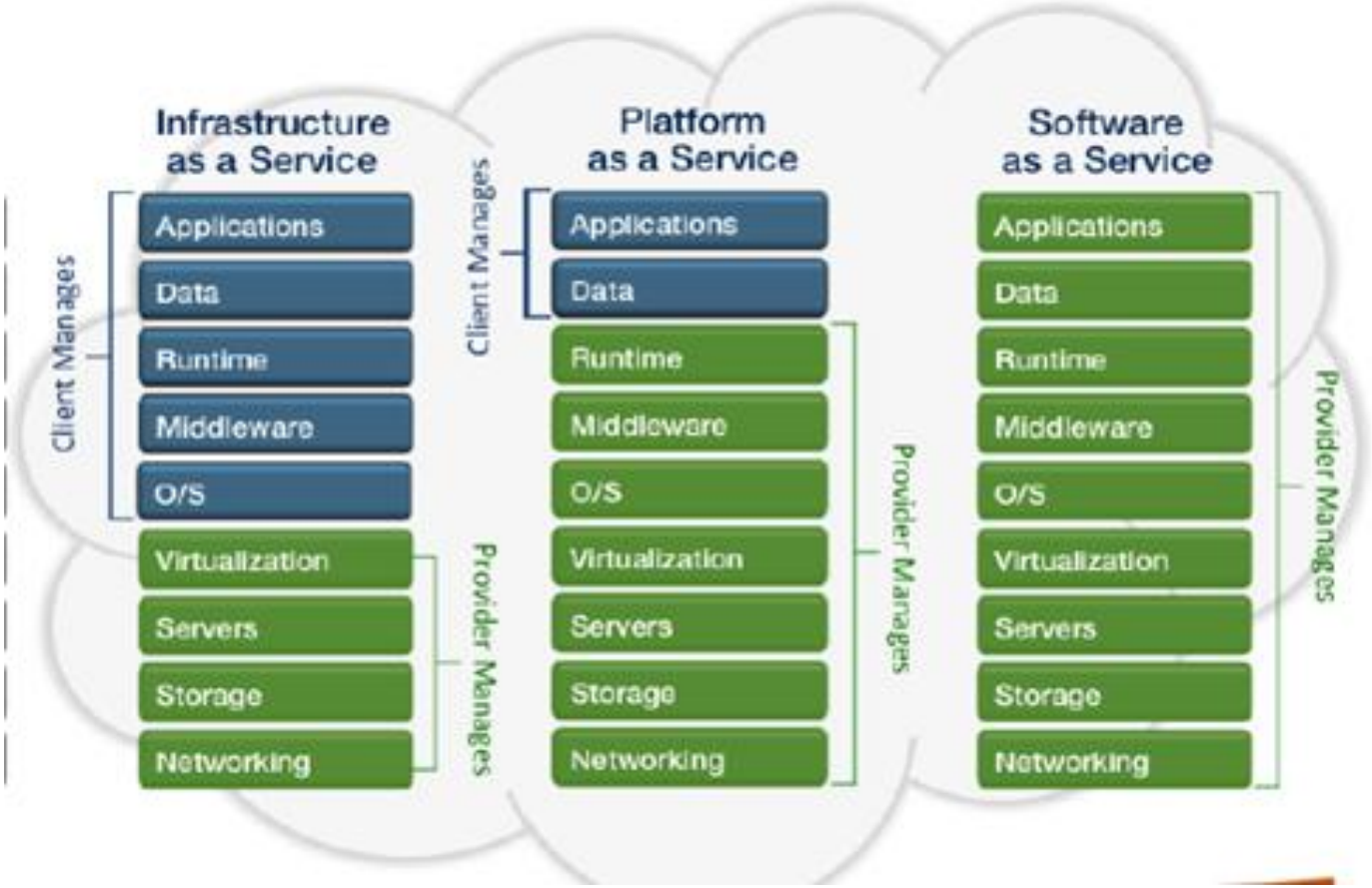
Subscriber's information

Types of Cloud Computing

SAAS

PAAS

IAAS



Way to Implement

Private Cloud

- On premises virtualization
- Behind corporate firewalls
- Complete control of security
- A physical part of the corporate data center
- Can be hosted at a hosting facility

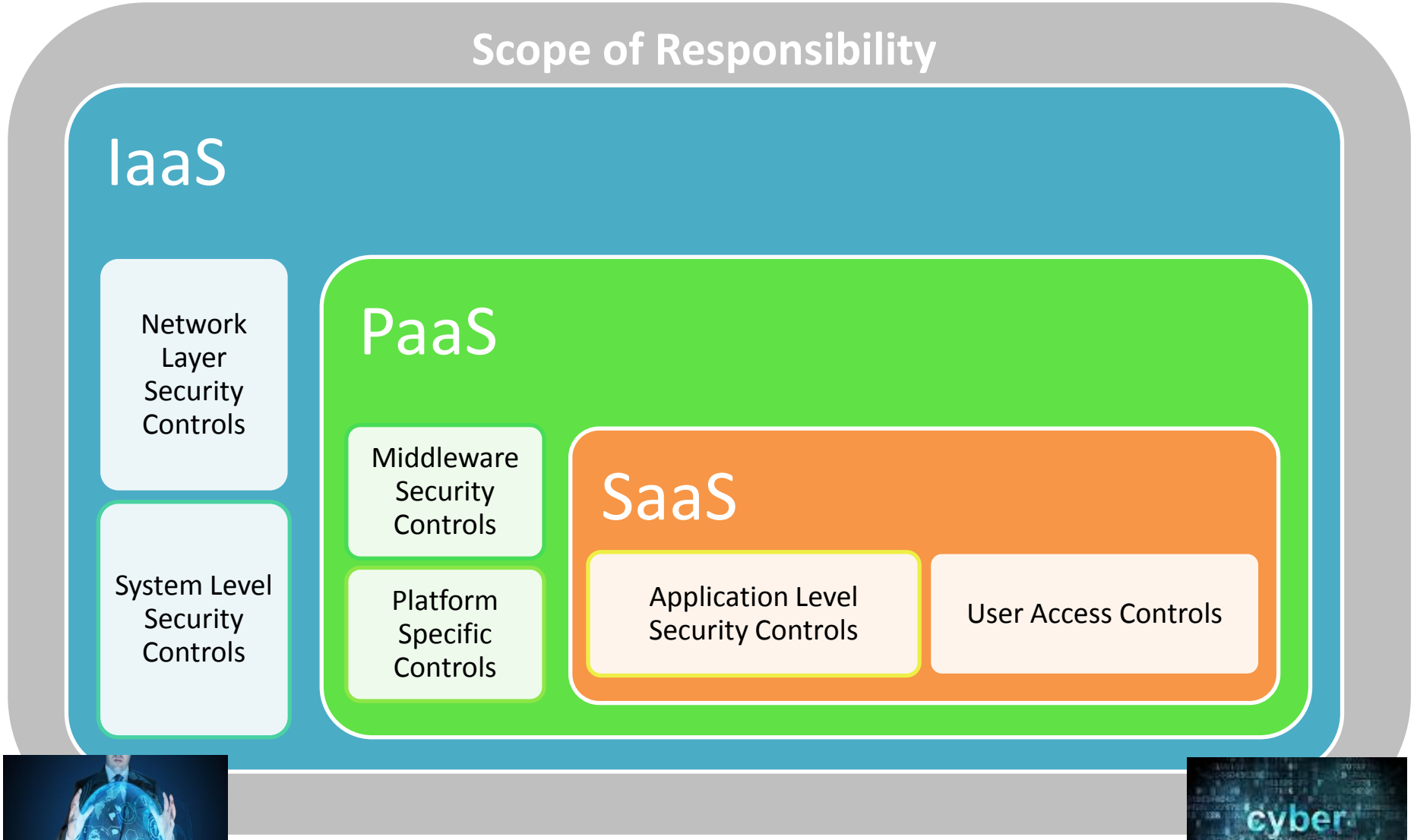
Virtual Private Cloud

- Vendor hosted virtualization
- Isolated from the public Internet
- Vendor specific security, including specialized firewalls
- An extension to the corporate data center

Public Cloud

- Vendor hosted virtualization
- Open to the public Internet
- Per host software firewalls
- Vendor Specific Security Controls
- Not an extension of the corporate Data Center

Information Security Processes in a Cloud



Cloud Security Processes - SAAS

Security Processes	Vendor	← *Shared* →	Customer
User Access Process			X
Data Confidentiality		X	
Application Security Config.			X
System Security	X		
Log Collection / Sec. Intelligence		X	
Patch Management	X		
Network Security	X		
Vulnerability Management	X		
Intrusion Detection / Prevention	X		
Incident Response	X		
Advanced Threat Management		X	
Physical Security	X		

- **Security technology in consideration**
  - Data encryption (In-Transit)
  - Security Information and Event Management (SIEM) for application incidents
  - Automated user access provisioning / de-provisioning
  - Automation of user access reviews
  - Role-based access controls
  - Separation of duties considerations
  - Single-sign on
  - Data Loss Prevention
  - Security Configurations:
  - Transfer of data from DC to the application
  - Timeouts
  - CASB

Cloud Security Processes - PAAS

Security Processes	Vendor	← *Shared* →	Customer
User Access Process			X
Data Confidentiality		X	
Application Security Config.			X
System Security		X	
Log Collection / Sec. Intelligence		X	
Patch Management		X	
Network Security	X		
Vulnerability Management		X	
Intrusion Detection / Prevention	X		
Incident Response		X	
Advanced Threat Management		X	
Physical Security	X		

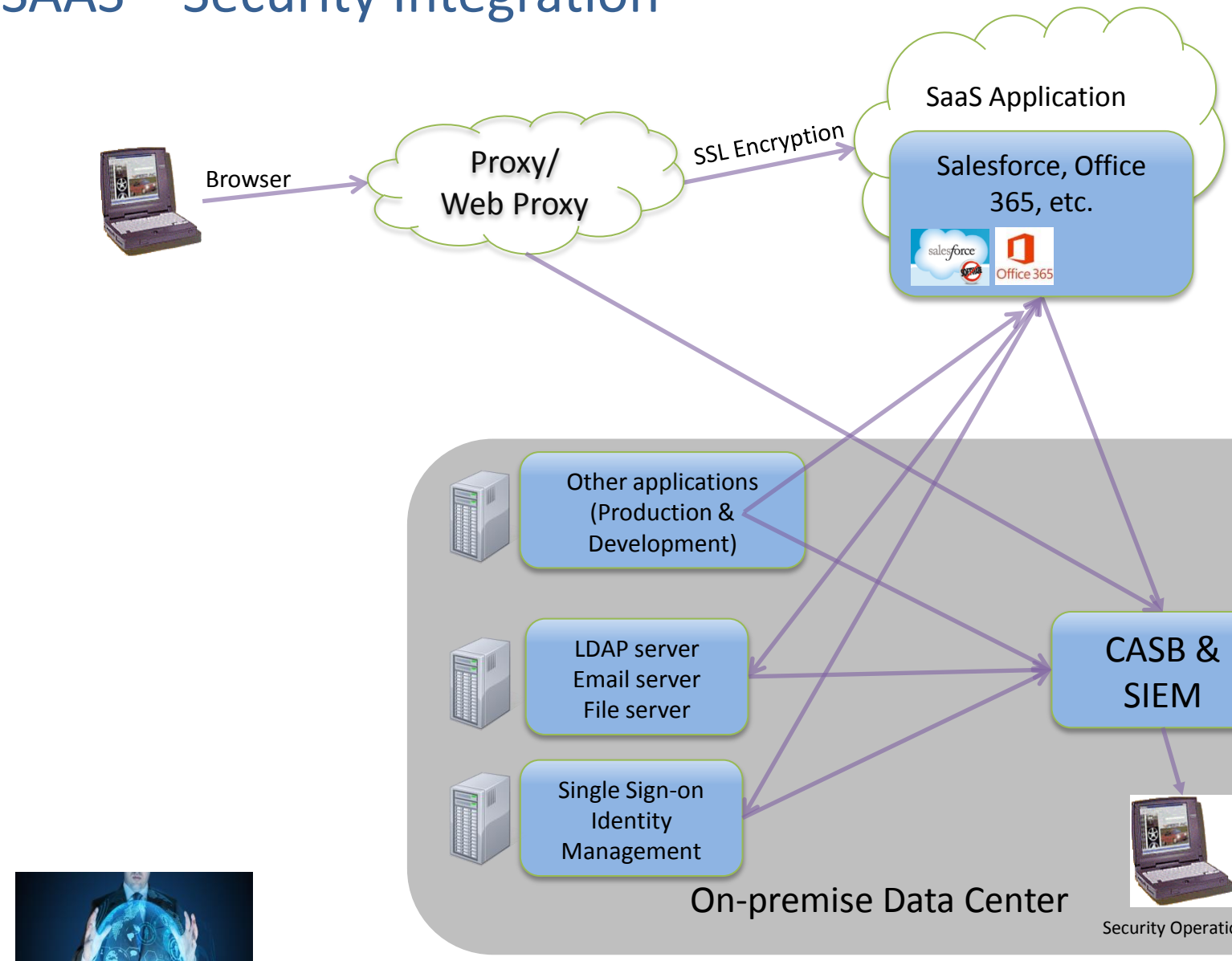
- **In addition to security technology in consideration of SAAS, additional points for PAAS are**
  - Remote access controls
  - API access controls
  - VPN / B2B connectivity
  - Patch Management
  - Vulnerability Management
  - Additional SIEM integrations at the platform level

Cloud Security Processes - IAAS

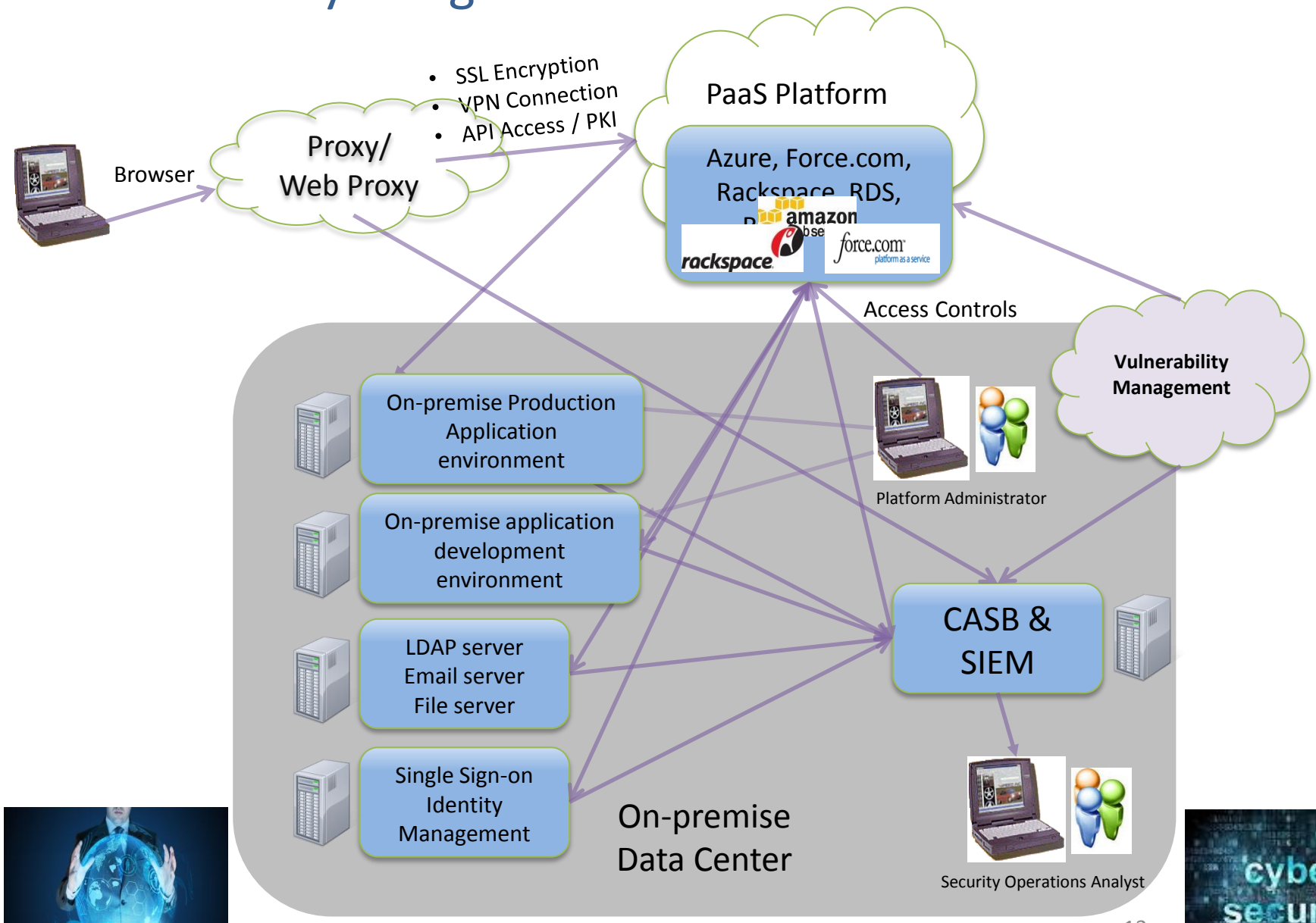
Security Processes	Vendor	← *Shared* →	Customer
User Access Process			X
Data Confidentiality		X	
Application Security Config.			X
System Security			X
Log Collection / Sec. Intelligence		X	
Patch Management			X
Network Security			X
Vulnerability Management		X	
Intrusion Detection / Prevention		X	
Incident Response		X	
Advanced Threat Management		X	
Physical Security	X		

- **In addition to security technology in consideration of SAAS & PAAS, additional points for IAAS are**
  - Encryption (at rest)
  - Direct network connections
  - Network firewalls
  - Security groups (per instance firewalls)
  - Intrusion protection
  - End point malware
  - End point data loss prevention
  - Additional SIEM integration at the virtual hardware level

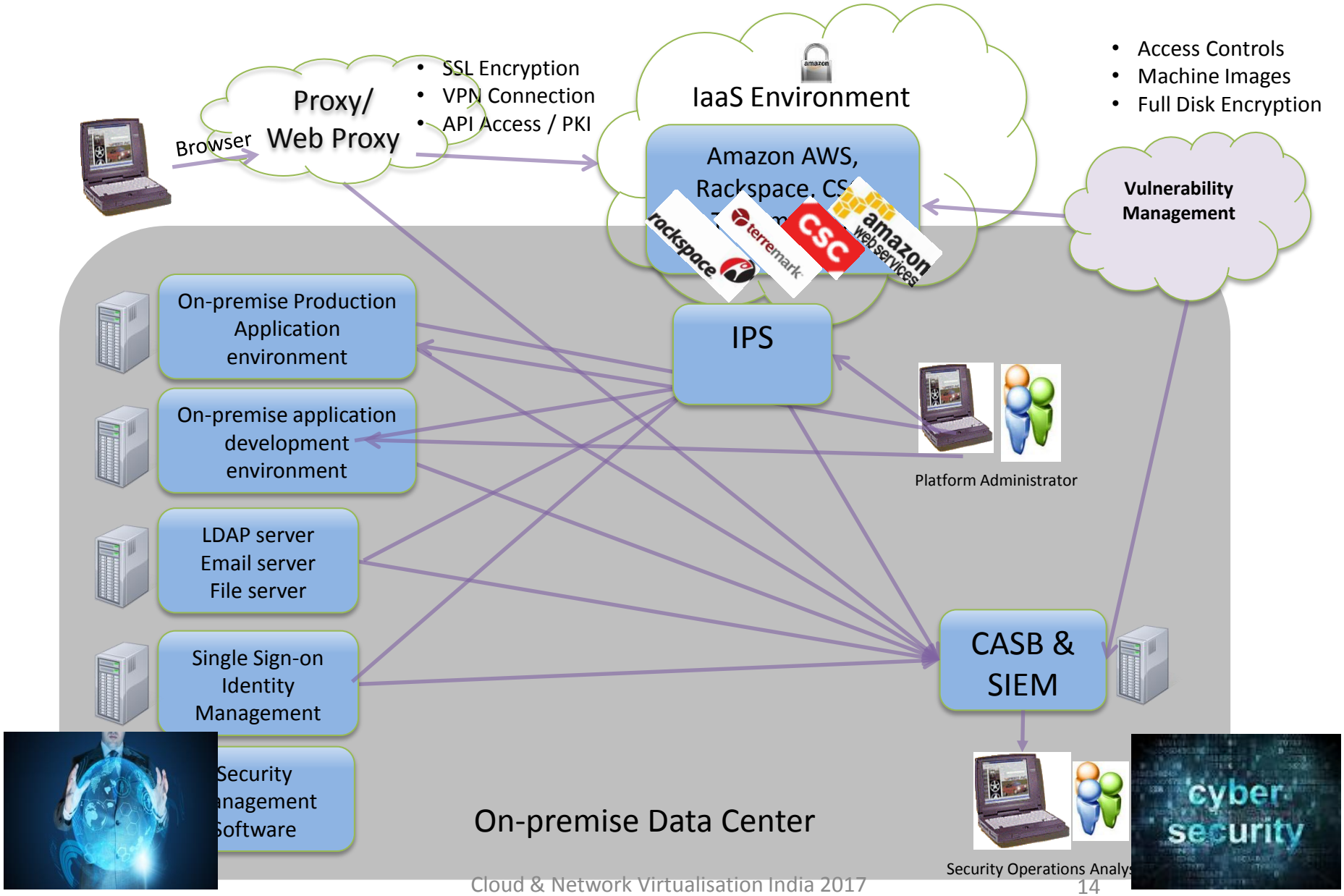
SAAS – Security Integration



PAAS – Security Integration



IAAS – Security Integration



Thank you!