Securing Journey to the Cloud: Part 1

—

Andrew Lemke
Executive Advisor, Inventor

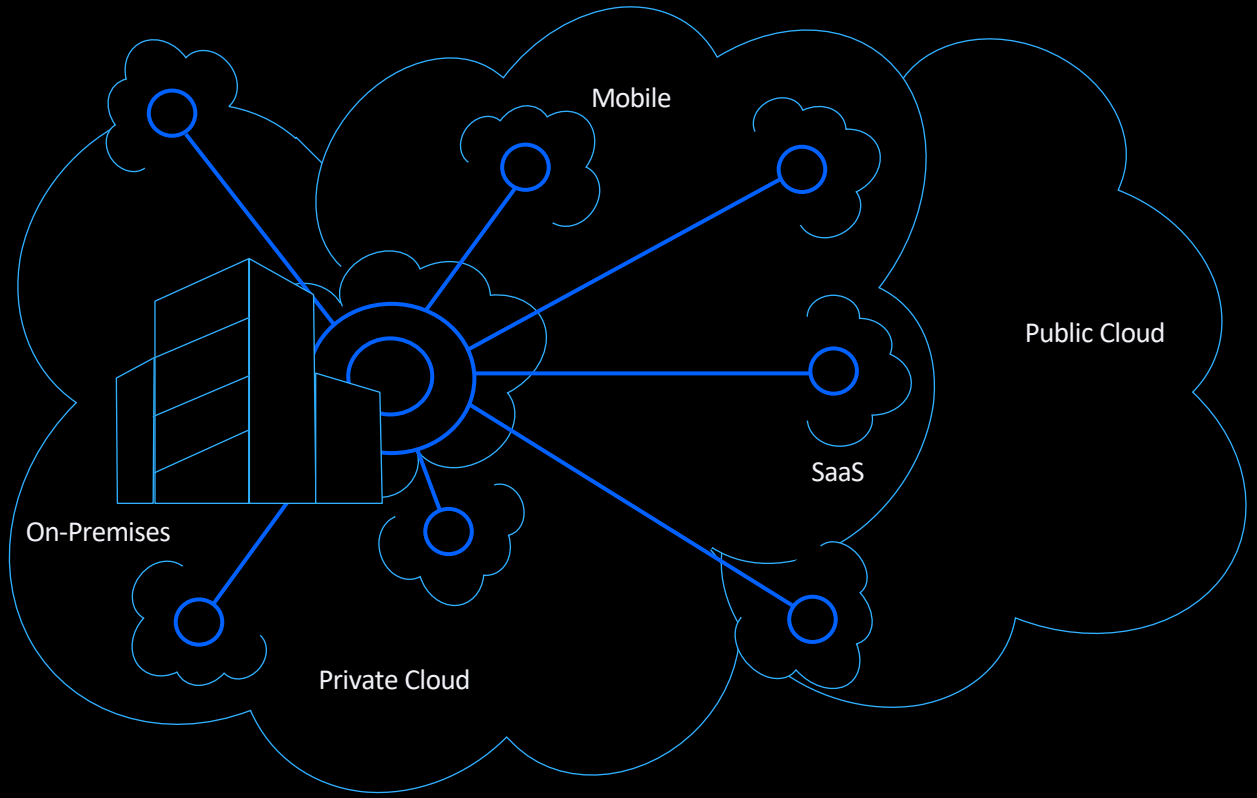
IBM **Security**

IBM

Why we are trusted

- 18,000 customers
- 70B+ security events monitored per day
- Leader in 12 security market segments

Security enabling business



Fixed and finite perimeter

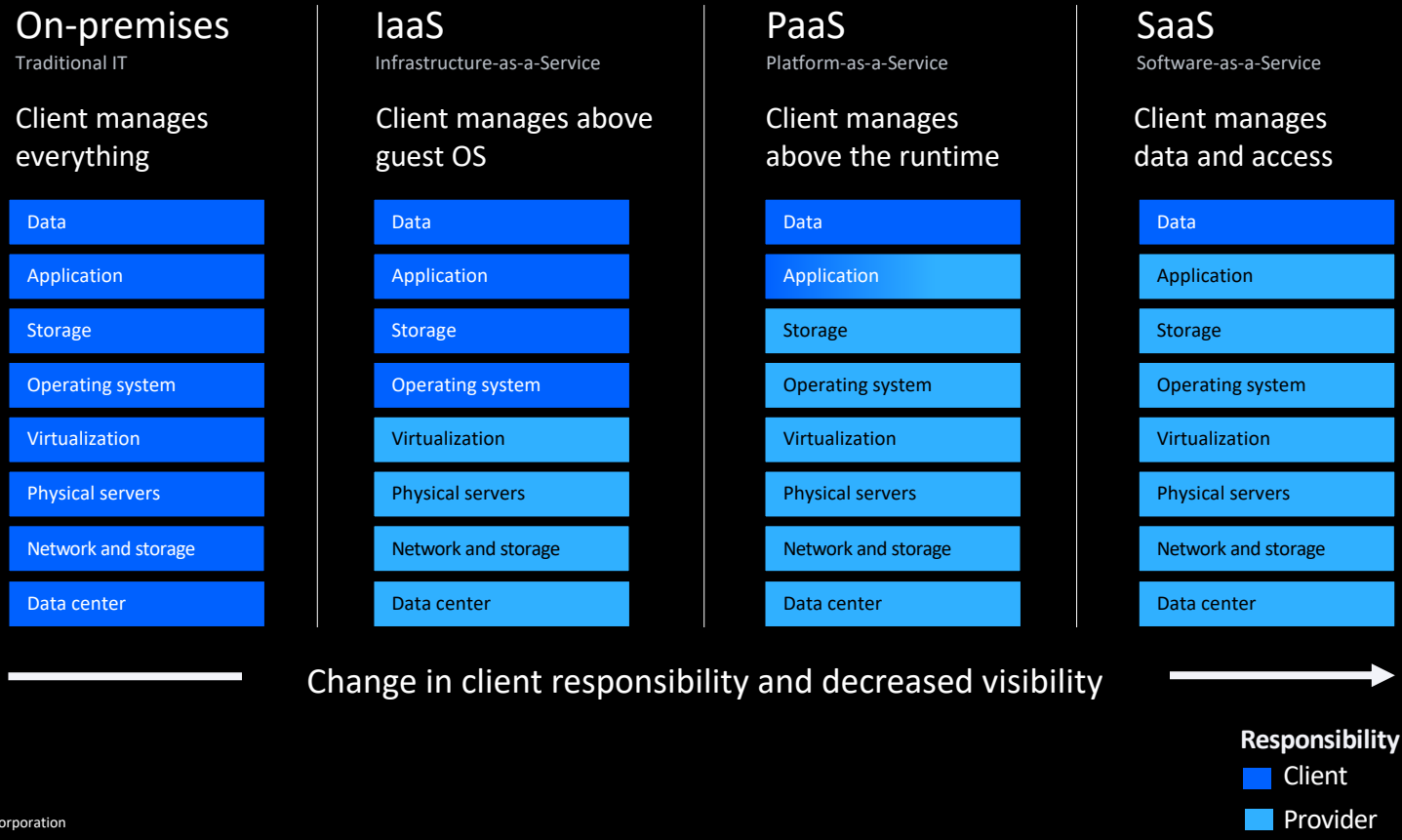
Traditional architecture & development

Perimeter less defined with mobile, BYOD and SaaS

Perimeter dissolved
DevOps driving business
Microservices architecture

Business expansion now dependent upon CISO and DevSecOps

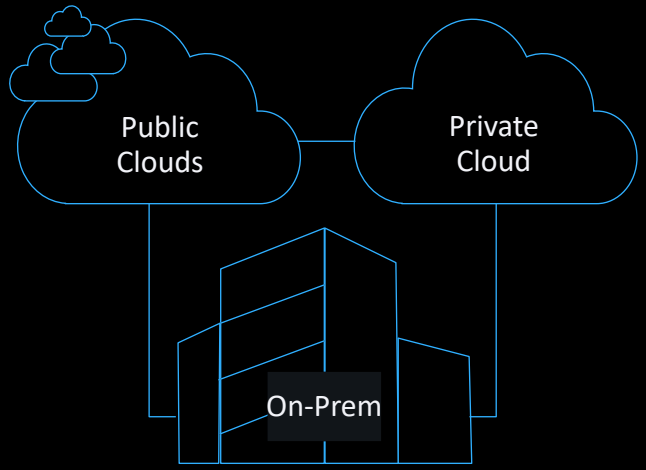
Shared and changing security responsibilities



Today's environment:
Fragmented solutions, visibility, and responsibility

SECURITY TOOLS

Palo alto
Symantec
Qualys
Twistlock
McAfee
Check Point
Cisco



CLOUD PROVIDERS

Native Security Controls

AWS
Microsoft Azure
IBM
Salesforce
Google

BARE METAL / SERVERS > VIRTUAL MACHINES > CONTAINERS > CLOUD CONTROL PLANE & CLOUD NATIVE

Security must enable your journey to cloud

80%

of workloads have not yet migrated to cloud[1]

94%

of organizations have multiple clouds[2]

85

security products across 40 different vendors[3]

1 Forrester, The Public Cloud Market Outlook 2019-2022
2 Cloud Computing Trends: 2019 State of the Cloud Survey, Flexera
3 Thousands of IBM Security Services engagements

Where we've come from

Security as an isolated IT function

Traditional security tools & technologies

Define policies by IPs and hosts

Try to stop all known bad activity

Segment infrastructure into zones

Static data protection controls

Perform regular compliance checks

Disjointed incident response

What will happen

Cumbersome and insecure deployments

Sensitive and regulated data exposed

Costly rework of apps & workloads

Unsanctioned use of shadow IT

Ineffective incident response

Inconsistent security as workloads move

Limited visibility into workload policies

Ad hoc native security control adoption

Where we need to be

Refresh strategy and integrate cloud

Build security into DevOps process

Augment with cloud native security

Implement a zero-trust security model

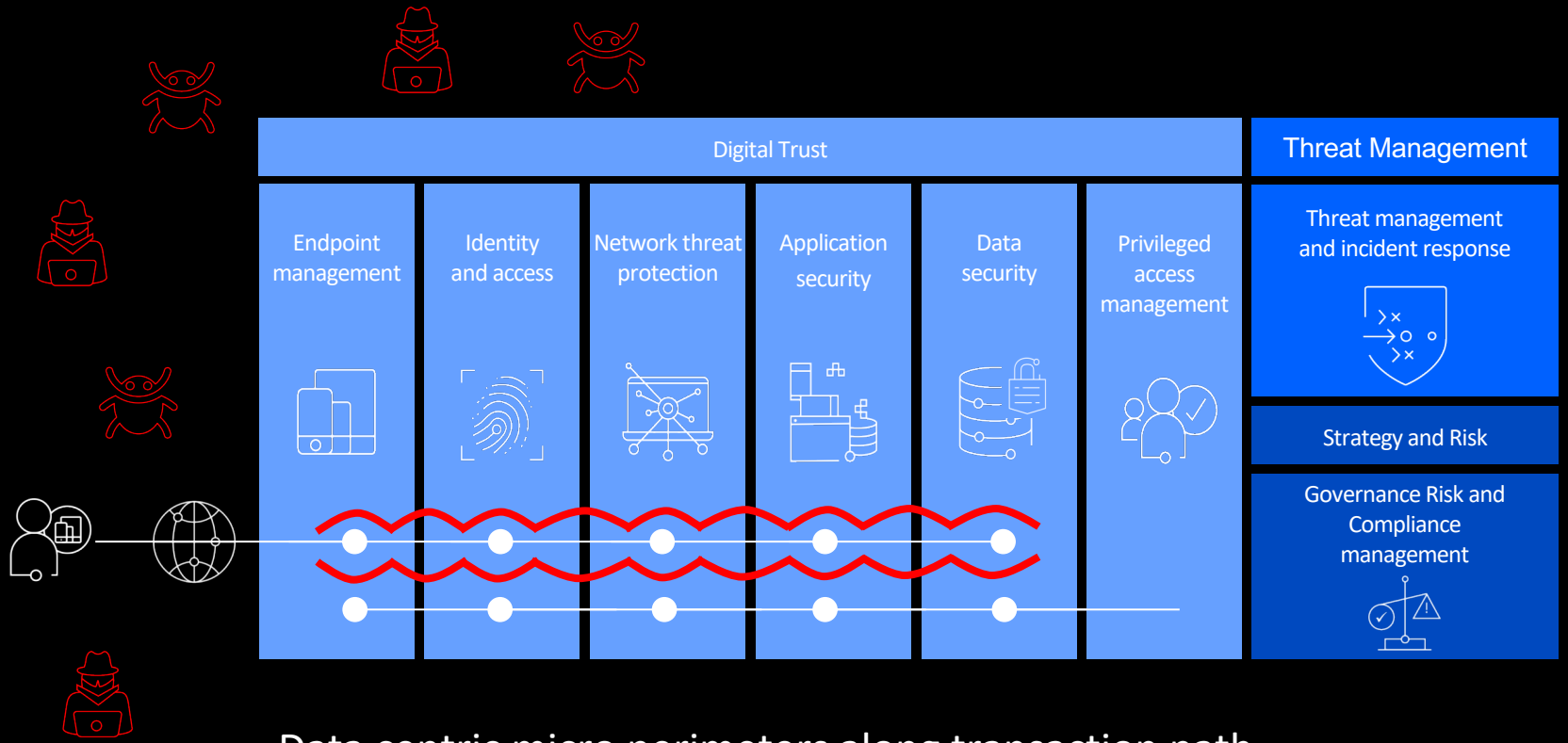
Attach policies to workloads

Protect data wherever it resides

Monitor compliance continuously

Multi-party incident response orchestration

Zero Trust – simplified?



- Data centric micro perimeters along transaction path
- Identity centric micro segmentation – principal of least privilege

IBM **Security**

THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- ibm.com/security/community
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

lemke@us.ibm.com

IBM