

Securing Journey to the Cloud: Part 1

—

Andrew Lemke

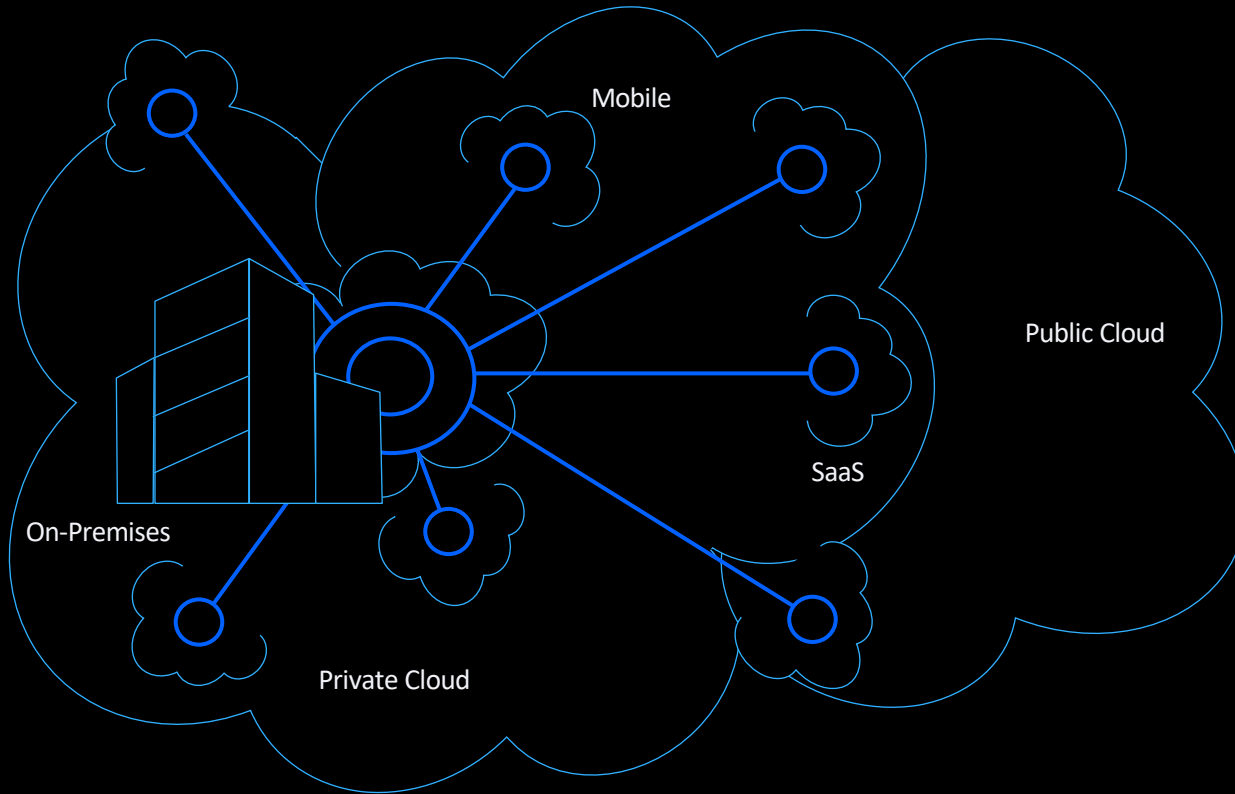
Executive Advisor, Inventor

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

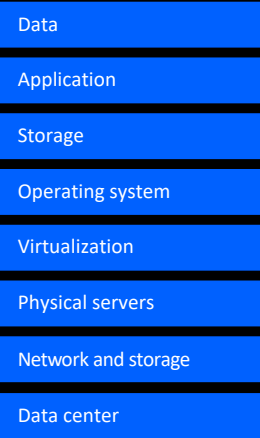
Business expansion now
dependent upon CISO
and DevSecOps

Shared and changing security responsibilities

On-premises

Traditional IT

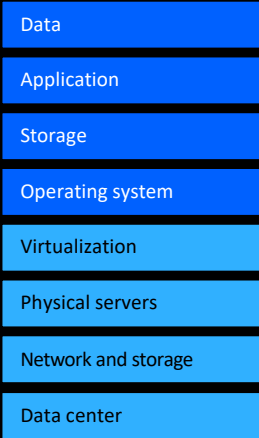
Client manages everything



IaaS

Infrastructure-as-a-Service

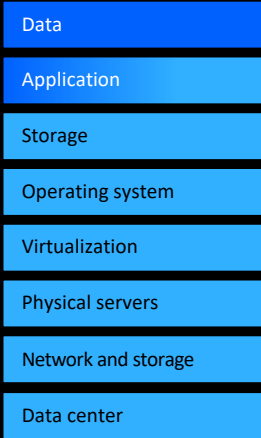
Client manages above guest OS



PaaS

Platform-as-a-Service

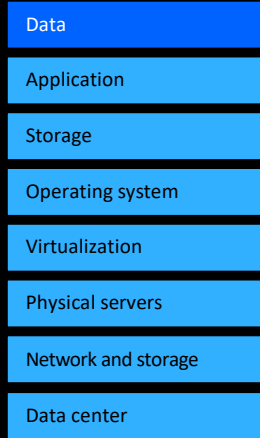
Client manages above the runtime



SaaS

Software-as-a-Service

Client manages data and access



Change in client responsibility and decreased visibility



Responsibility

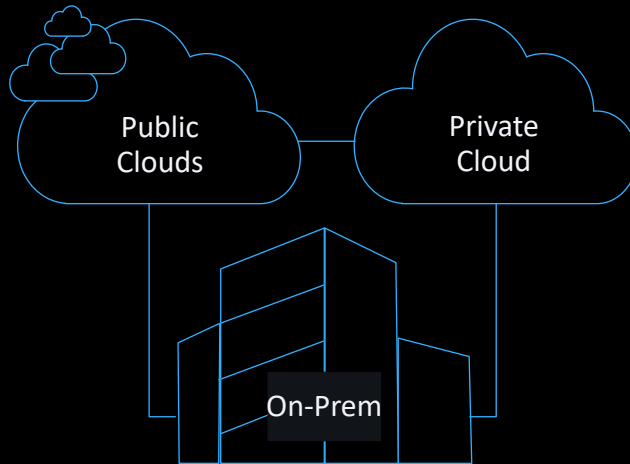
■ Client

■ Provider

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

SECURITY TOOLS

Palo alto Symantec
Qualys
McAfee Twistlock
Cisco Check Point



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 cloud¹

94%

of organizations have multiple clouds²

85

security products across 40 different vendors³

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

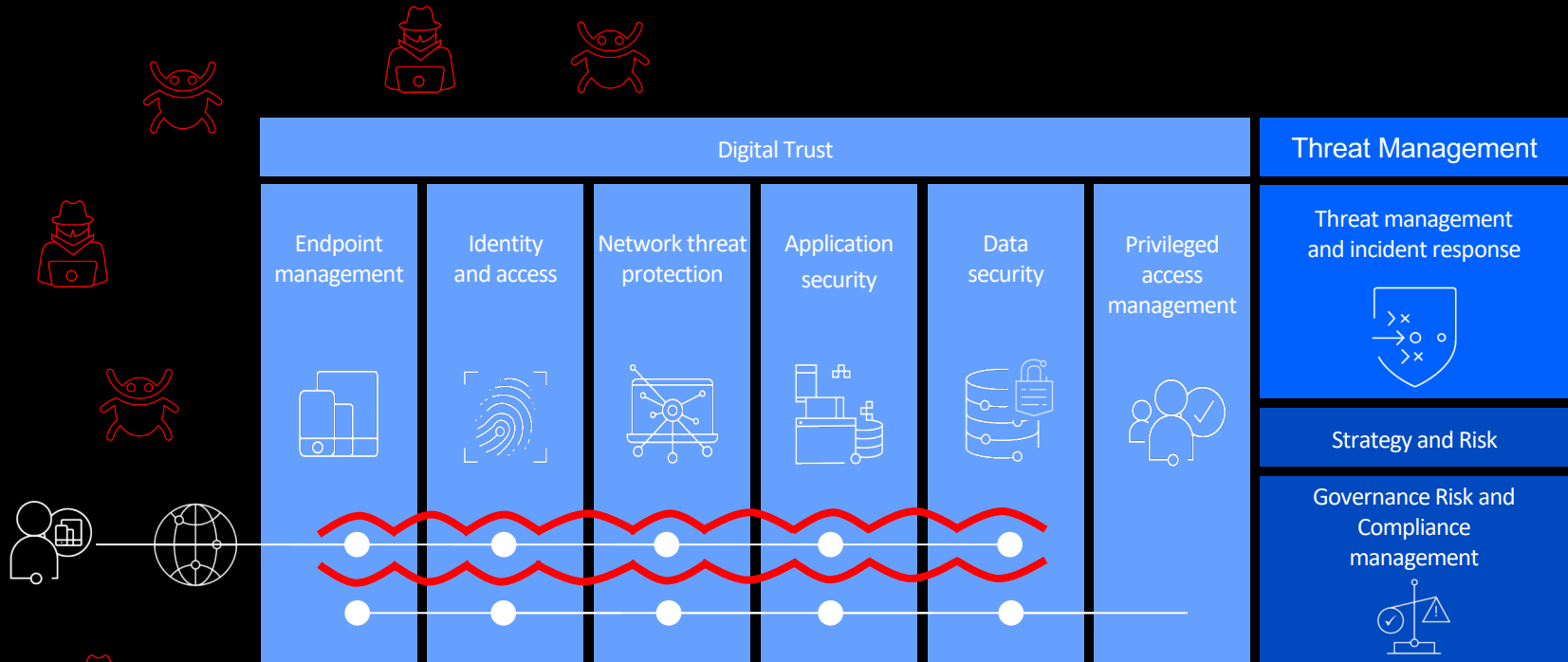
Attach policies
to workloads

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](https://twitter.com/ibmsecurity)



youtube/user/ibmsecuritysolutions



lemke@us.ibm.com

© Copyright IBM Corporation 2019. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

