A Practical Lesson in Cloud Controls from Breach Analysis

Shain Singh | Cloud/5G Security Architect | ss@f5.com | @shainsingh

Shahn Backer | Principal Security Advisor | s.backer@f5.com | @sbacker27

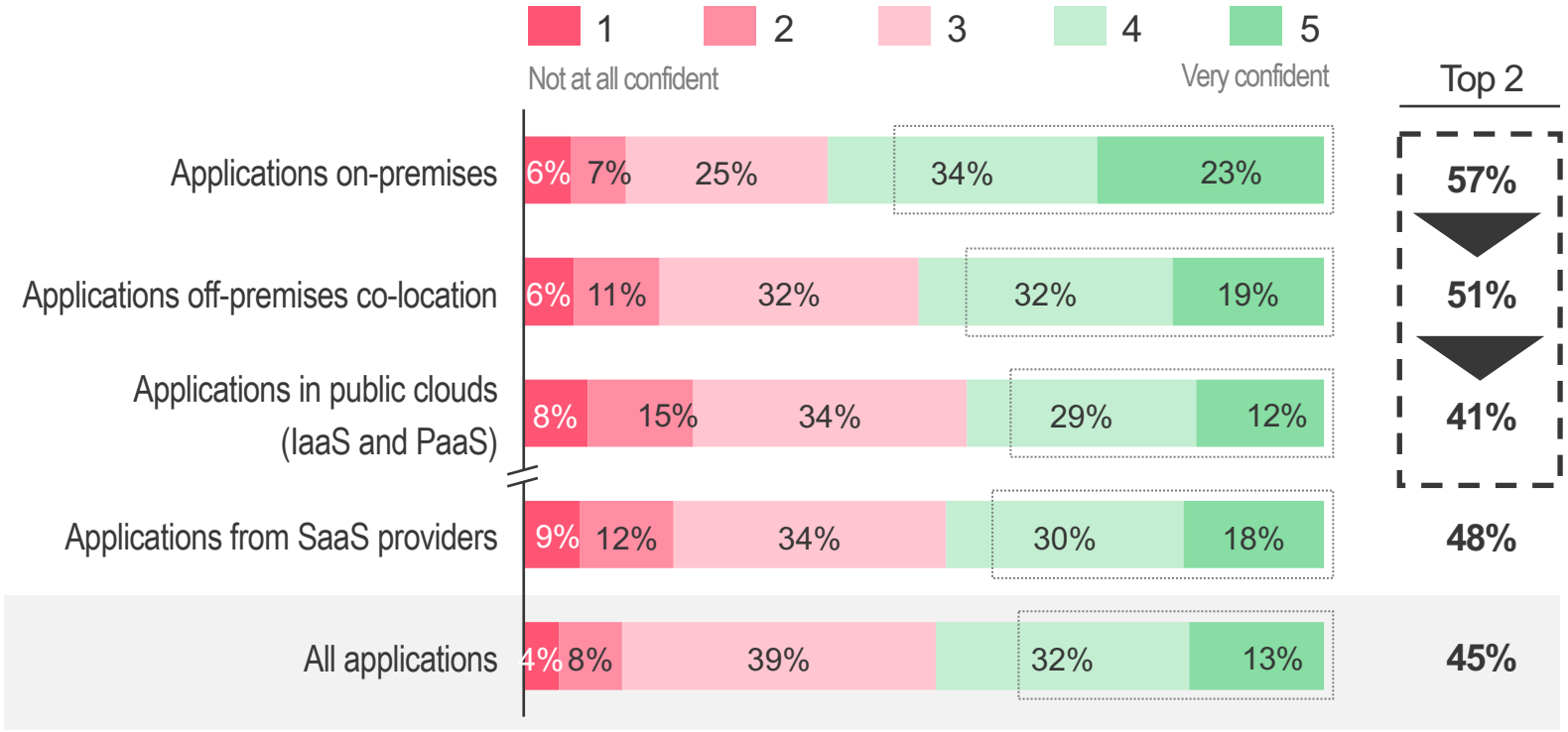
The average organization uses 983 apps

How many are mission critical?

App Security Challenges

SECURITY IS AN EVEN MORE ACUTE ISSUE IN PUBLIC AND MULTI-CLOUD ENVIRONMENTS

Level of confidence to withstand an application-level security attack



n = 1986
Q: On a scale of 1 to 5, please rate your confidence in your company's ability to withstand an application level security threat.

SOURCE: STATE OF APPLICATION SERVICES, F5 NETWORKS, JANUARY 2019

87% of Organizations are Multi Cloud

"Multi-Cloud Makes it Harder"

Policy Sprawl | Compliance Gaps | Operational Complexity | Uncontrolled Apps | Cloud Lock-In

Cloud Platforms

amazon web services™
Google Cloud Platform
Microsoft Azure
CISCO
vmware
Alibaba Cloud aliyun.com
openstack
SOFTLAYER
ORACLE Cloud

Architectures

- Private Clouds
- Public Clouds
- Microservices
- Containers
- Cloud Interconnect
- Two-Tier (N/S and E/W)

App Owners

- Traditional IT
- DevOps Team
- Business Owner
- App Developers
- Security Team

Toolsets

CHEF
ANSIBLE
SALTSTACK
puppet
ATLAS
sumologic
MESOS
kubernetes
Container Connectors
New Relic.
docker
splunk>
APPDYNAMICS
RED HAT OPENSHIFT

Applications are a leading source of enterprise risk

MULTI-CLOUD DEPLOYMENTS INCREASE THIS RISK

86%

EXPANDING THREAT SURFACE AREA

of all cyber-threats target applications and application identities.[1]*

85%

NEW ARCHITECTURES

of new app workload instances are container-based, growing to 95% by 2021.[2]

87%

DISTRIBUTED DEPLOYMENTS

of customers are adopting multi-cloud.[3]

0%

INADEQUATE VISIBILITY

of customers can report the number of applications in their portfolio with confidence.[3]

[1]F5 LABS APPLICATION PROTECTION REPORT 2018
[2]CISCO GLOBAL CLOUD INDEX: 2016-2021
[3]F5 SOAS REPORT 2019

*REMAINING 14% IS PHYSICAL ATTACKS AND "OTHER" (INCLUDING VPN, NETWORK, DNS AND DIRECT DATABASE AND ATM ATTACKS)

All applications must be protected

NOT JUST THE MISSION-CRITICAL ONES

LARGE RETAILER

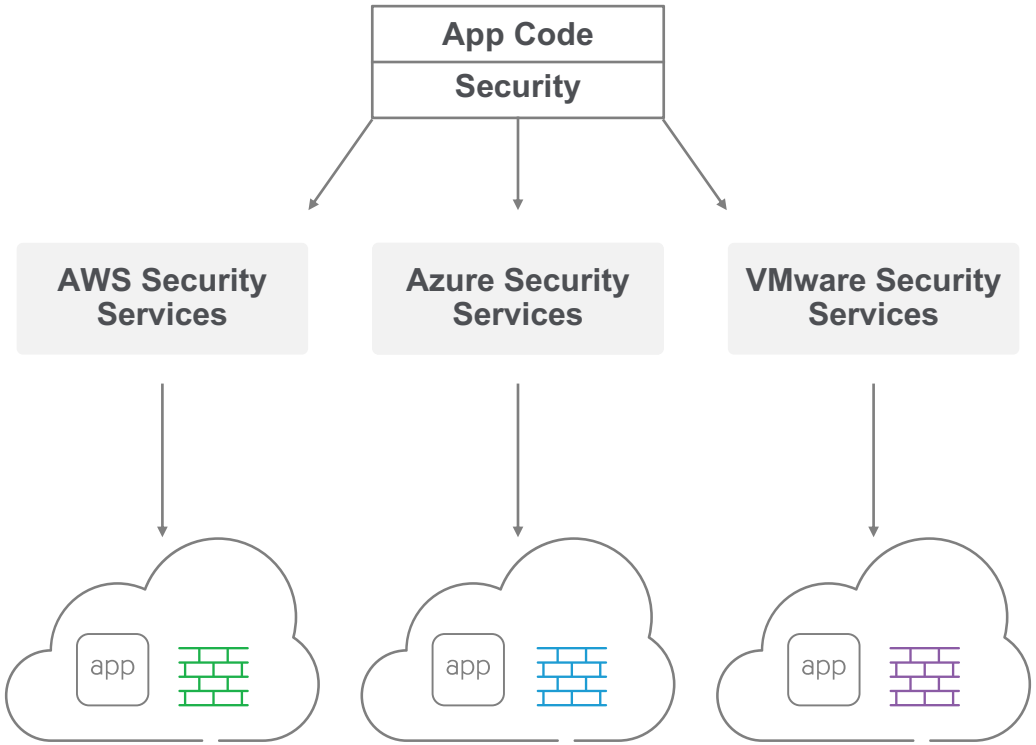
- Millions of customer records exfiltrated
- Billions in damages, market cap; CEO fired
- Entry point through HVAC system

CASINO OPERATOR

- High-roller database taken
- Most lucrative customers at risk
- Entry point through a digital thermometer in the lobby aquarium

Developers can’t be solely responsible for app security

1. Developers spend significant amounts of time securing app code
2. Developers individually configure unique cloud-native security services
3. Developers must manage these services and resolve issues



Leads to reduced developer efficiency and weakened security posture

Multi Cloud Challenges

TOP THREE EVERY YEAR REMAIN THE SAME

	2018	2019	2020
#1 Applying consistent security policy across all company applications	42%	40%	24%
#2 Protecting applications from existing and emerging threats	40%	39%	23%
#3 Optimizing the performance of the application	33%	39%	22%
Migrating apps among clouds/data centers	x	x	22%
Complying with regulations	x	x	22%
Gaining visibility into application health (status, performance, capacity)	31%	39%	20%
Determining which cloud is the most-cost efficient for our application	29%	36%	19%
Not having the right skillset within the organization.	x	X	15%
Controlling application sprawl	x	x	13%

SOURCE: F5 STATE OF APPLICATION SERVICES, 2020

Compliance can assist to set guardrails

CJIS
Criminal Justice Information Services

DoD SRG
DoD Data Processing

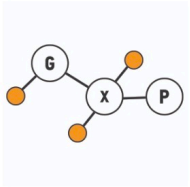
FedRAMP
Government Data Standards

FERPA
Educational Privacy Act

FFIEC
Financial Institutions Regulation

FIPS
Government Security Standards

FISMA
Federal Information Security Management



GxP
Quality Guidelines and Regulations

HIPAA
Protected Health Information

HITRUST CSF
Health Information Trust Alliance Common Security Framework

CSA
Cloud Security Alliance Controls

ISO 9001
Global Quality Standard

ISO 27001
Security Management Controls

ISO 27017
Cloud Specific Controls

ISO 27018
Personal Data Protection

PCI DSS Level 1
Payment Card Standards

SOC 1
Audit Controls Report

SOC 2
Security, Availability, & Confidentiality Report

SOC 3
General Controls Report

FISC [Japan]
Financial Industry Information Systems

IRAP [Australia]
Australian Security Standards

K-ISMS [Korea]
Korean Information Security

MTCS Tier 3 [Singapore]
Multi-Tier Cloud Security Standard

OSPAR [Singapore]
Outsourcing Guidelines

Industry standards define deployment patterns

Cloud Controls Matrix
Security Guidance For Critical Areas of Focus in Cloud Computing

Benefits, Risks and Recommendations For Information Security

Cybersecurity Framework

Secure Cloud Computing Architecture

CIS Benchmarks

RISKS

Strategy and Architecture

Potential Risks

- Customer Responsibility
- Often Missed /Solution with little security strategy
- No check on compliance to strategy and architecture

Victims

- Hotel Reservation Platform with misconfigured S3 buckets
- Data from 2013 - 2020
- Data Exposed : PII, Credit Card Details, Payment Details, Reservation Details

Hotel reservation platform with misconfigured AWS S3 buckets exposed PII and payment details

MITIGATION

Strategy and Architecture

Prevention

- Leverage automation as early as possible into the design for infrastructure and service builds
- Ensure data in transit and rest is encrypted, with placement of decryption and inspection capabilities at ingress/egress locations
- Implement a Zero Trust approach with more reliance on context based than location and session-based controls
- Ensure feedback loops from telemetry for event-based actions

Implement a Zero Trust approach for context-based controls

RISKS

Lack of Identity and Access Management

Potential Risks

- Customer Responsibility
- Weak Password + No 2FA for Root Account
- No access control

Victims

- Cloud hosting company on public cloud
- Hacker got access to privileged credentials
- Deleted all Data and Backup
- Created backup admin accounts

Cloud hosting solution provider - lost all data and backups via privileged credential breach

MITIGATION

Lack of Identity and Access Management

Prevention

- Implement federated access controls instead of local user logins
- Leverage use of anti-fraud/anti-bot technologies for public web assets for authenticated and un-authenticated application flows
- Implement use of MFA for all privileged and non-privileged authenticated application flows
- Look to implementing device and browser fingerprinting technologies for log enrichment and use across authenticated application flows

Use of MFA for privileged and unprivileged application flows

RISKS

Insecure Interfaces

Potential Risks

- Customer Responsibility
- Little / No access control
- Insecure API or SSH endpoints

Victims

- Cyber security vendors database breached with Stolen API Keys
- Data Exposed : email, hashed password, TLS key
- 13,000 password changed 13,500 SSL Certificate rotated

Cybersecurity vendor database breached with stolen API keys

MITIGATION

Insecure Interfaces

Prevention

- Implement web application and API protection (WAAP) technologies in front of API gateways
- Leverage threat intelligence for protection against known malicious endpoints and zero-day application vulnerabilities

Implement web application and API protection (WAAP) in front of API gateways

RISKS

Economic Denial of Sustainability

Potential Risks

- Customer Responsibility
- Traffic is made up of
  - Network Floods
  - Malformed Requests
  - Scanner & Bots

Victims

- A service provider with a cloud first approach
- Got surge in traffic
- Got billed for the mostly bot traffic

Large service provider billed for bot traffic

MITIGATION

Economic Denial of Sustainability

Prevention

- Leverage anti-bot and DoS technologies to mitigate against unwanted traffic surges
- Ensure event-based alerts for telemetry events involving auto-scaling to humans not just machines
- Limit scaling options to a specified amount with manual intervention for higher volumes

Leverage anti-bot and DoS technologies

RISKS

Inside Threats

Potential Risks

- Customer Responsibility
- Privilege account holders go unchecked
- Internal working of the system is exposed to privileged user

Victims

- Major American bank
- Details for 106 millions users
- Misconfigured web application firewall
- Access internal details

Major American bank lost details for 106m users due to a misconfigured WAF

MITIGATION

Insider Threats

Prevention

- Design for decryption technologies at egress points that enable proper use of Data Loss Prevention (DLP) technologies for exfiltration mitigation
- Event-based alerts of traffic monitoring to highlight any anomalies such as higher egress than ingress traffic patterns
- Practice least-privilege access controls

Design for decryption technologies at egress points

Summary

- Multi - Cloud
- Security cannot be an after thought
- Strategy & Architecture
- Identity and Access Management
- Insecure Interfaces
- Insider Threats
- Economic Denial of Sustainability

Q&A