

CLOUD SECURITY: ANTICIPATING THE NEW THREAT LANDSCAPE



Marco Estrela, PMP, ITIL
Thanh Nguyen, CISSP

October 14th, 2020
ESI E-Learning Capsule

AGENDA

- Intro
- How's the market?
- Is the cloud a safe place?
- How the cloud is breached
- Demo
- *Cloudy* responsibilities
- Solutions & takeaways



Our Mission



MANAGE data to reach
business objectives

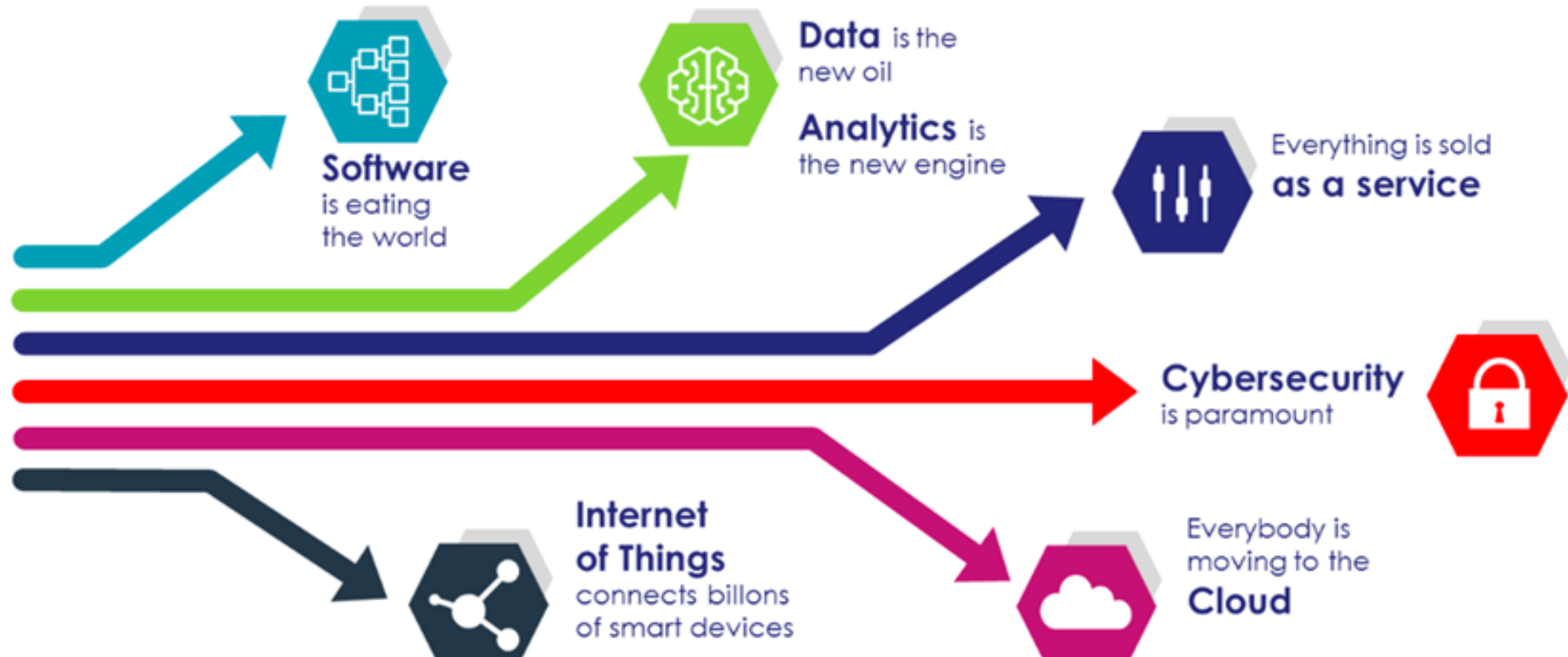


PROTECT data by
mitigating risk



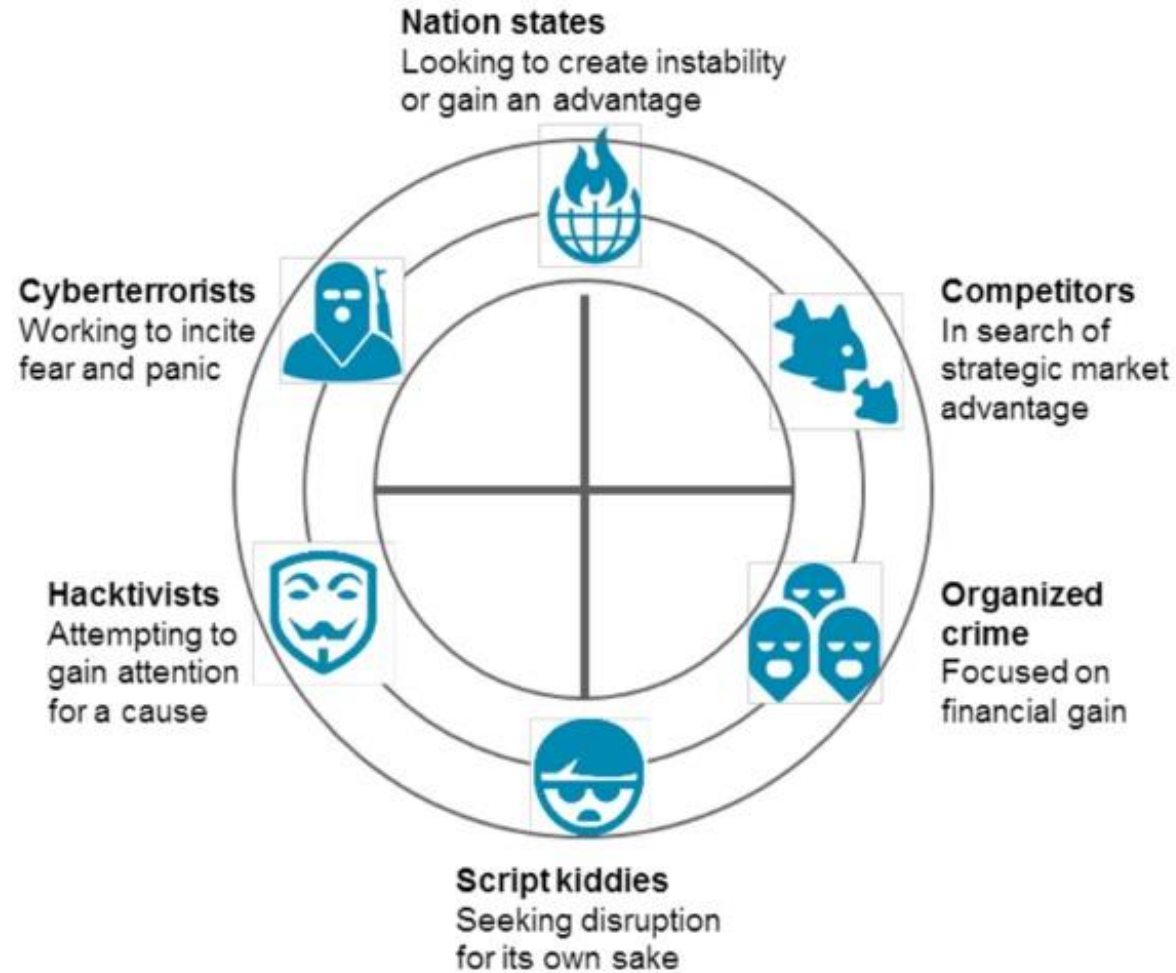
TRANSFORM data into relevant
and actionable information

Cybersecurity is unavoidable



Actors of cybercrime

Cyber Bad Actor Landscape



1

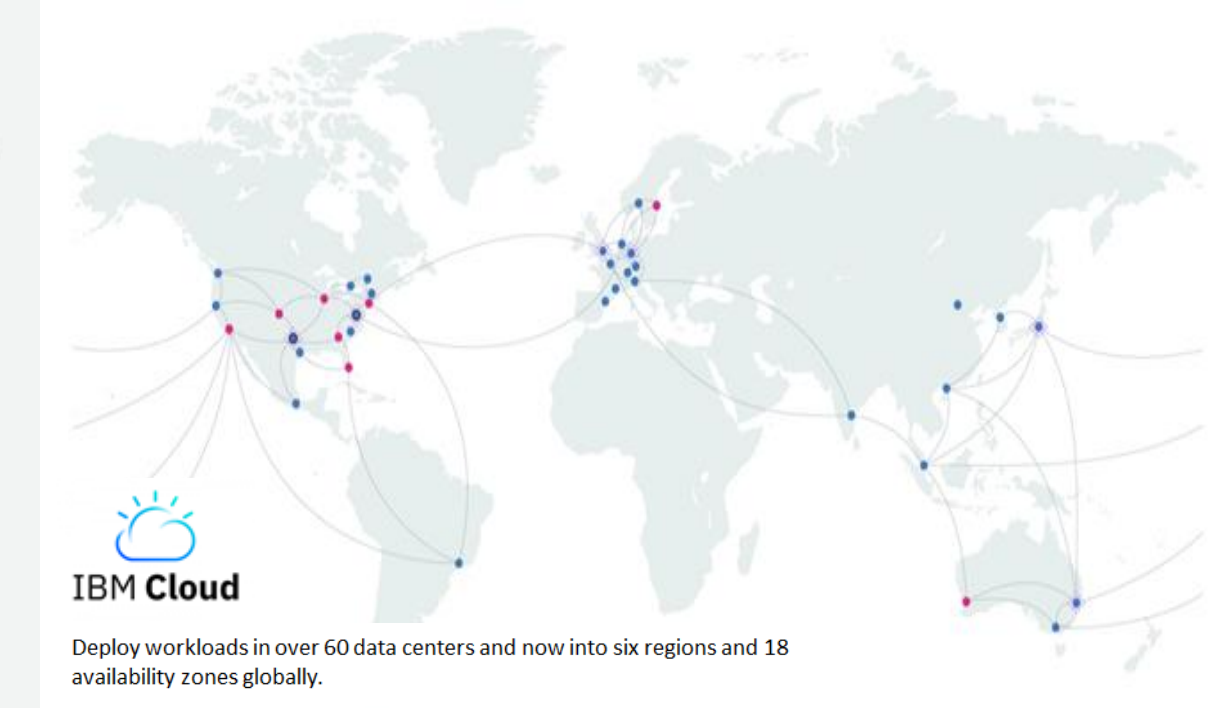
HOW'S THE MARKET?



IS THE CLOUD AN ADOPTED TECHNOLOGY?

→ All major players have heavily opted in!





GARTNER'S MAGIC QUADRANT

Figure 1. Magic Quadrant for Cloud Infrastructure and Platform Services



2

IS THE CLOUD A SAFE PLACE?



A few statistics



Financial gain is the most common motivation factor targeting cloud environments.

Bruteforcing and exploitation of cloud environments are the 2 most common infection vectors accounting for 45% of all cases.

Data theft – such as the appropriation of PII – is the preferred activity of cybercriminals once they penetrate a cloud environment

Misconfiguration of cloud environments led to more than 1 billion lost records in 2019.

Ransomware is the most commonly deployed malware in infiltrated cloud environments accounting for 3 times as many cases as cryptomining and botnet malware.

Leveraging cloud platforms for use as malicious infrastructure is often a favorite ploy of sophisticated threat actors enabling them to ramp up operations with a single compromise.

Attacks occur daily...




Author:
Tara Seals

September 10, 2020

A cloud misconfiguration at the gaming-gear merchant potentially exposed 100,000 customers to phishing and fraud.

An estimated 100,000 customers of Razer, a purveyor of high-end gaming gear ranging from laptops to apparel, have had their private info exposed, according to a researcher.



Water Nue Phishing Campaign Targets C-Suite Office 365 Accounts

12 DAYS AGO by [Asterhawk](#) / Public / TLP: ... write

A series of ongoing business email compromise (BEC) campaigns that uses spear-phishing schemes on Office 365 accounts has been seen targeting business executives of over 100 States and Canada. The fraudsters, whom we named "Water Nue," primarily target accounts of financial executives to obtain credentials for further financial fraud. The phishing email compromised, emails containing invoice documents with tampered banking information are sent to subordinates in an attempt to siphon money through fund transfer requests.

REFERENCE: <https://blog.trendmicro.com/trendlabs-security-intelligence/water-nue-campaign-targets-c-suites-office-365-accounts/>


TAGS: office, water nue, office 365

ADVERSARY: WATER Nue

TARGETED COUNTRIES: Canada, United States of America

ATT&CK ID: T1193 - Spearphishing Attachment

Indicators of Compromise (4) **Related Pulses (5)** Comments (0) History (0)




Phishing Campaign Targeting Executive Office 365 Accounts

9 DAYS AGO by [porter_redwall](#) / Public / TLP: ... write

URL: 2 / Domains: 2

<https://blog.trendmicro.com/trendlabs-security-intelligence/water-nue-campaign-targets-c-suites-office-365-accounts/>




Water Nue Phishing Campaign Targets C-Suite's Office 365 Accounts

10 DAYS AGO by [AmalMohammed](#) / Public / TLP: ... write

URL: 1 / Domains: 2

A series of ongoing business email compromise (BEC) campaigns that uses spear-phishing schemes on Office 365 accounts has been seen targeting business executives of over



Water Nue Phishing Campaign Targets C-Suite Office 365 Accounts

11 DAYS AGO by [Cyber_Hat](#) / Public / TLP: ... write

URL: 2 / Domains: 2

office, water nue, office 365

Nearly 80% of Companies Experienced a Cloud Data Breach in Past 18 Months

June 5, 2020

KEYWORDS access management / cloud security / data breach / Identity Authentication / risk management

Ermetic, cloud access risk security company, **announced** the results of a research study conducted by global intelligence firm IDC which found that nearly 80% of the companies surveyed had experienced at least one cloud data breach in the past 18 months, and nearly half (43%) reported 10 or more breaches.

According to the 300 CISOs that participated in the survey, security misconfiguration (67%),



BUT SAAS APPLICATIONS ARE HACKED...



FORTUNE

TECH • BRIEFING

Deloitte Gets Hacked: What We Know So Far

Office 365


INDEPENDENT

News • UK • Online News

Parliament hit by cyber attack as hackers attempt to access MPs' email accounts

Hackers launch 'sustained and determined attack' on all parliamentary user accounts

[View Details](#) [Share/Bookmark](#) [Security Patch 2017-04-01](#) [CWE-300](#)




Doki Infecting Docker Servers in the Cloud

15 HOURS AGO by [MARQUELL](#) / Public / TLP: ... write

Filehash: ADS5 / Filehash: SNA5 / Filehash: SNA256 / YARA: 1 / Malware: 1

Doki, Docker, Docker, Linux




Cloud Phishing from Google App Engine and Azure App Service

15 HOURS AGO by [MARQUELL](#) / Public / TLP: ... write

URL: 0 / Domains: 1 / Malware: 1


o365-themed, phish, phishing



NextCloud Bruteforce Attempts

1 DAY AGO by [TheQuackLord](#) / Public / TLP: ... write

BruteForce IP addresses against a private NextCloud server. These IP addresses are external only, recorded with the Fail2Ban IPS software. Fail2Ban is configured to log the IP address of an adversary after 3 sets of failed login. Fail2Ban, Apache, HTTP, BruteForce, NextCloud




A Big Catch: Cloud Phishing from Google App Engine and Azure App Service - Netskope

1 DAY AGO by [james_james](#) / Public / TLP: ... write

URL: 0 / Domains: 1 / Malware: 2

Netskope Threat Labs has identified an ongoing O365 phishing campaign hosted in Google App Engine with the credential harvester mostly hosted in Azure App Service. This phishing campaign typically targets O365 users in o365-themed, phish, phishing




Flaws in SAP Solution Manager could have facilitated intrusions

11 DAYS AGO by [joshua234](#) / Public / TLP: ... write

CVE-3

Used by 80% of the companies that make up the Global 2000 list of Forbes magazine, which ranks the world's largest publicly traded companies, according to estimates, SAP Solution Manager (SolMan)



Office365 Bruteforce IP - 070720

14 DAYS AGO by [QoS_Lunatic](#) / Public / TLP: ... write





















IP of a cloud VM trying multiple permutations of various user IDs to gain access to Australian MSO365 accounts

There is no discrimination of attacks against their targets

Figure 1: Exposure to Cloud Data Breaches

Q. Has your company experienced a cloud data breach in the past 18 months?

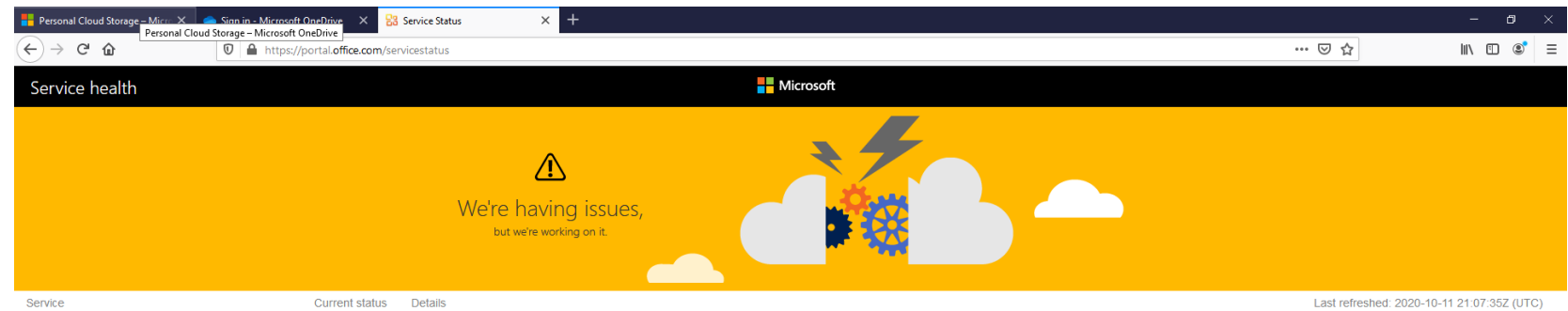
Percentage of respondents who answered "Yes"

INDUSTRY		Yes (%)	BUSINESS SIZE		Yes (%)
	Manufacturing	58%	 1,500 - 2,499		81%
	Banking	94%	  2,500 - 4,999		89%
	Health	81%	   5,000 - 9,999		79%
	Government	70%	    10,000 - 19,999		71%
	Retail	71%	     20,000 +		72%

As access policies must be frequently adjusted, the potential for human error increases sharply. Some of the most high-profile cybersecurity incidents in recent years were the direct result of customers failing to properly configure their cloud environments, or granting excessive or inappropriate access permissions to cloud services, rather than a failure of the cloud provider in fulfilling its responsibilities. For example, the Capital One breach in 2019 where 106 million credit card applications were exposed was the result of excessive permissions assigned to a WAF that were used by the attacker to gain access to a sensitive AWS S3 bucket.

Sometimes, hackers
don't need to do
anything!

Source: <https://portal.office.com/servicestatus>



Microsoft cloud outages continue as Office and Outlook customers report problems

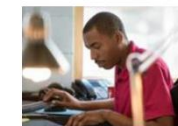
Microsoft's cloud services problems are continuing this week with more Azure and Microsoft 365 services issues for some customers. Here's what's happened and why.

By Mary Jo Foley for All About Microsoft | October 8, 2020 -- 13:57 GMT (06:57 PDT) | Topic: Cloud

	Americas		Europe		Asia Pacific		Middle East and Africa		Azure Government		Azure China	
PRODUCTS AND SERVICES	INDONESIA	EAST US	EAST US 2	CENTRAL US	NORTH CENTRAL US	SOUTH CENTRAL US	WEST CENTRAL US	WEST US	WEST US 2	CANADA EAST	CANADA CENTRAL	BRASIL SOUTH
IMPACTED SERVICES												
Azure Active Directory	▲											
Network Infrastructure		▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲
COMPUTE												
Azure VMware Solution by CloudSimple		●				●		●				
Virtual Machines		●	●	●	●	●	●	●	●	●	●	●
SAP HANA on Azure Large Instances		●						●	●			
Windows Virtual Desktop	●											
Virtual Machine Scale Sets		●	●	●	●	●	●	●	●	●	●	●
Azure Functions		●	●	●	●	●	●	●	●	●	●	●
Service Fabric		●	●	●	●	●	●	●	●	●	●	●
Batch		●	●	●	●	●	●	●	●	●	●	●
Cloud Services		●	●	●	●	●	●	●	●	●	●	●

Microsoft Azure status page on Oct. 7 around 3:30 p.m. ET

MORE FROM MARY JO FOLEY



Microsoft: Most employees can work from home less than 50 percent of the time



Windows 10 New Windows 10 test build adds set-up customization options



Cloud Microsoft's Azure AD authentication outage: What went wrong



Enterprise Software Microsoft adds more features to Dynamics 365 Customer Insights as rollout of Wave 2

3

HOW THE CLOUD IS BREACHED



What is the MITRE ATT&CK?



- Mitre is a MA-based corporation
- ATT&CK stands for: *Adversarial Tactics Techniques & Common Knowledge*
- Cloud matrix: Tactics and attacks targeting specifically **AWS, GCP, Azure, Azure AD, Office365, SaaS**.

Initial Access 5 techniques	Persistence 5 techniques	Privilege Escalation 1 techniques	Defense Evasion 5 techniques	Credential Access 4 techniques	Discovery 10 techniques	Lateral Movement 2 techniques	Collection 4 techniques	Exfiltration 1 techniques	Impact 4 techniques
Drive-by Compromise	Account Manipulation (3)	Valid Accounts (2)	Impair Defenses (1)	Brute Force (4)	Account Discovery (2)	Internal Spearphishing	Data from Cloud Storage Object	Transfer Data to Cloud Account	Defacement (1)
Exploit Public-Facing Application	Create Account (1)		Modify Cloud Compute Infrastructure (4)	Steal Application Access Token	Cloud Service Dashboard	Use Alternate Authentication Material (2)	Data from Information Repositories (2)		Endpoint Denial of Service (3)
Phishing (1)	Implant Container Image		Unused/Unsupported Cloud Regions	Steal Web Session Cookie	Cloud Service Discovery		Data Staged (1)		Network Denial of Service (2)
Trusted Relationship	Office Application Startup (6)		Use Alternate Authentication Material (2)	Unsecured Credentials (2)	Network Service Scanning		Email Collection (2)		Resource Hijacking
Valid Accounts (2)	Valid Accounts (2)		Valid Accounts (2)		Network Share Discovery				
					Permission Groups Discovery (1)				
					Remote System Discovery				
					Software Discovery (1)				
					System Information Discovery				
					System Network Connections Discovery				

4

DEMO



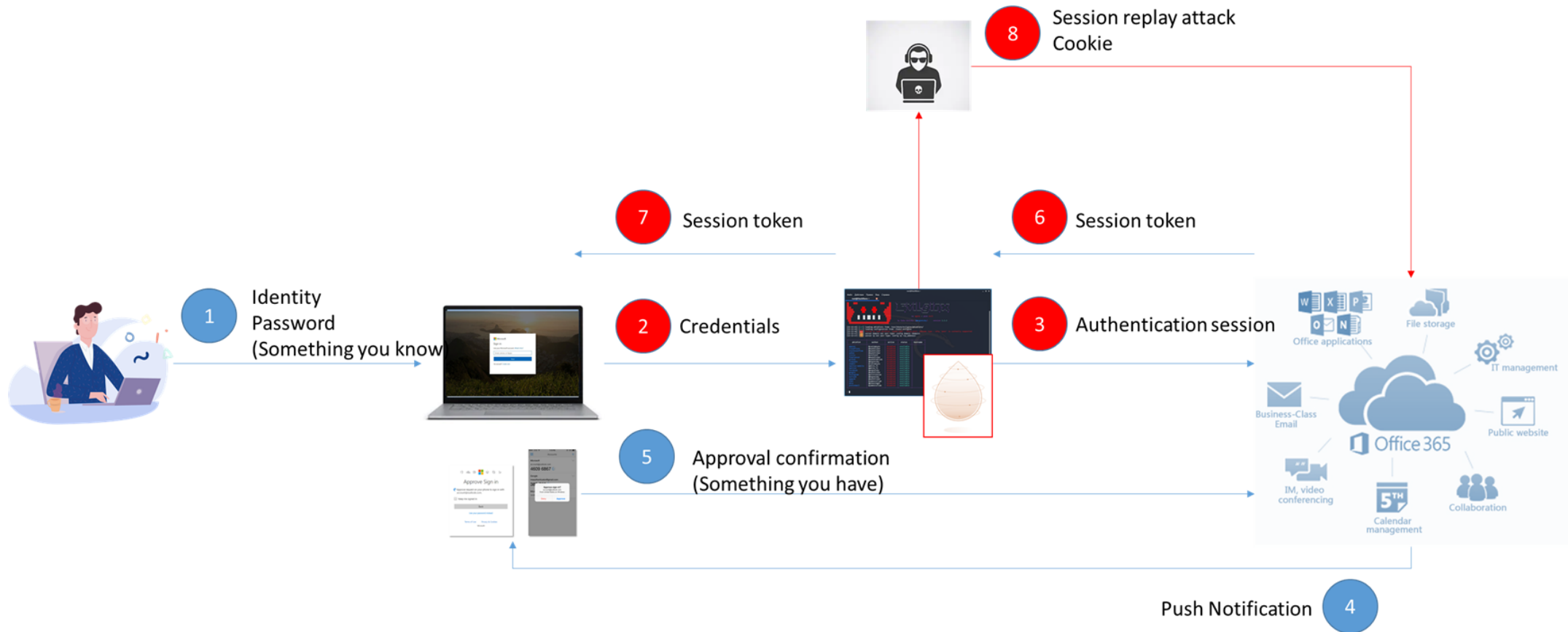
A (simulated) company "Sample-Montreal Inc."

- Very impressed by the great bundle of available services: OneDrive, SharePoint, Teams, Outlook and Azure Directory
- The CTO decides to migrate services to Office 365
- To be safe, he decides to enhance their cloud security with Two Factor Authentication enforced for ALL users.
- IT Team frequently checks for Office 365 security alerts

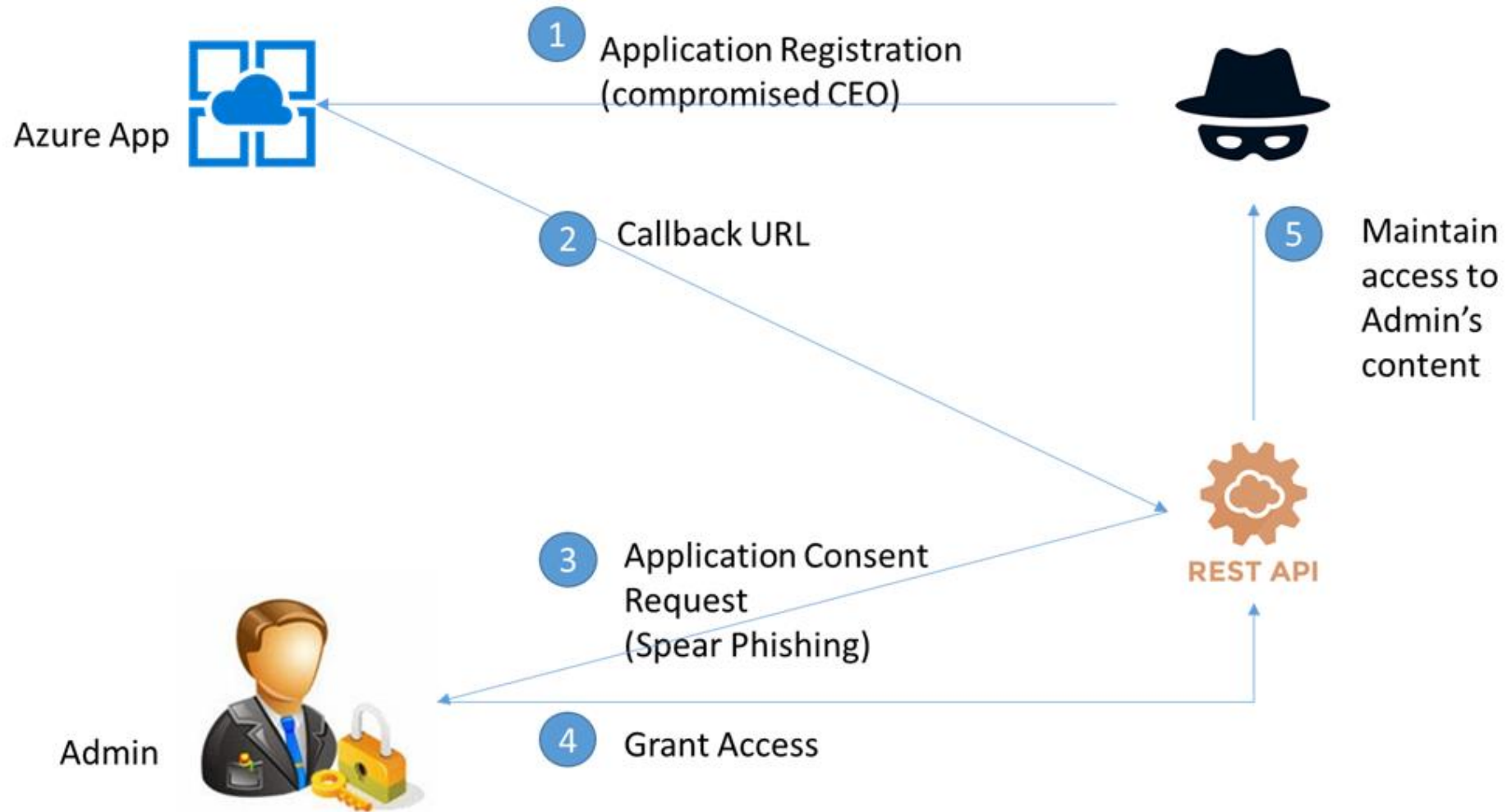


Image copied and changed from Internet www.mtlblog.com

Demo 1: Phishing bypass Two-Factor Authentication



Demo 2: Persistent Access with Application API



5

CLOUDY **RESPONSIBILITIES**



The Cloud Shared Responsibility Matrix : who does what?

→ Shared Responsibility:

- In 2017 Gartner estimated that 95% of responsibility was on customer's shoulders
- In 2018, GDPR said almost 100%

→ Ultimately, data security is YOUR responsibility!

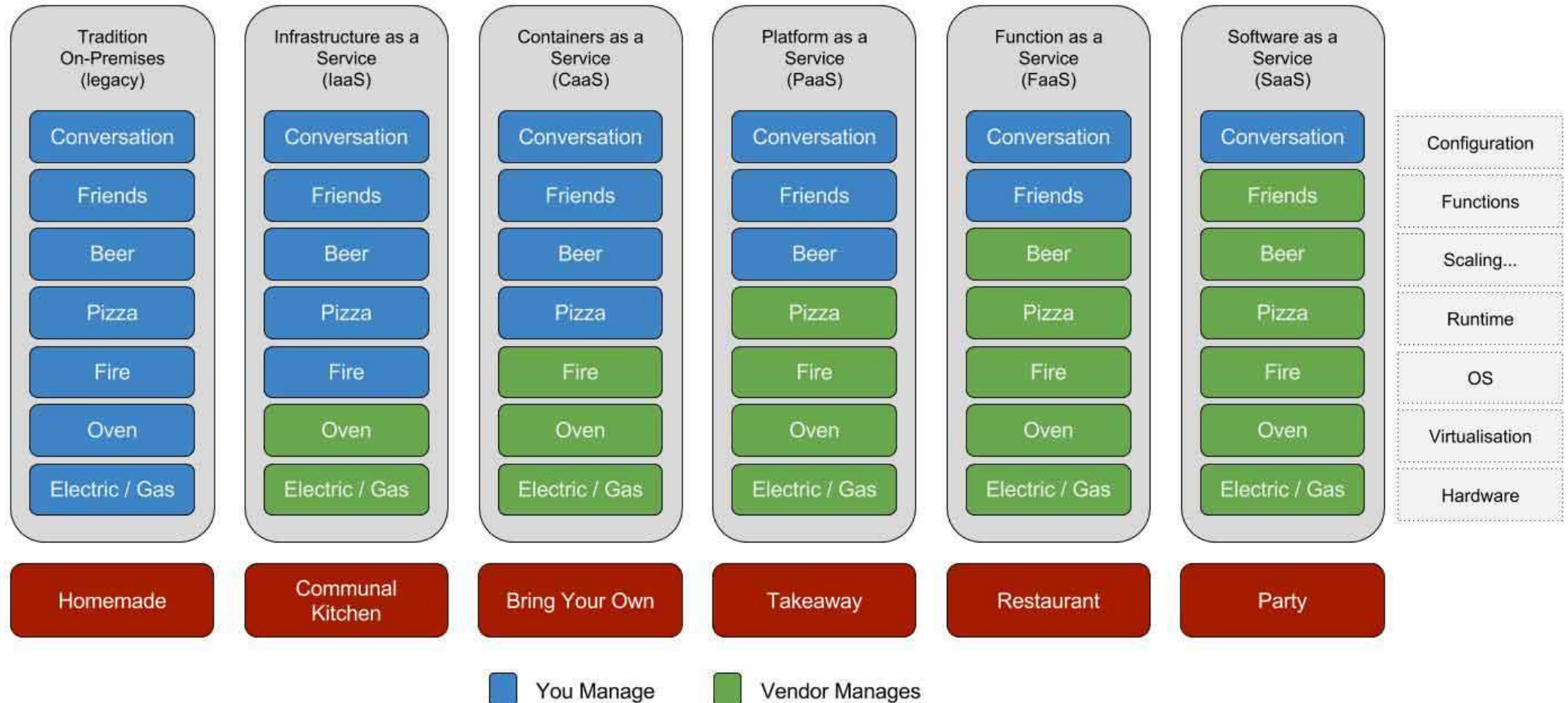
CSP	Customer
Physical security of infrastructure	User identity management and access control of service systems
Security of computing, storage, and network hardware	Data security
Security of basic networks, such as anti-distributed denial of service and firewalls	Security management and control of terminals that access cloud services, including hardware, software, application systems, and device rights
Cloud storage security, such as backup and recovery	User behavior
Tenant identity management and access control	The credentials of your organization and employees (strong PW but in insecure storage?)
Secure access to cloud resources by tenant	API of your applications
Formulating and rehearsing service continuity assurance plans and disaster recovery plans for infrastructure	

The Cloud Shared Responsibility Matrix: who does what?



Pizza as a Service 2.0

<http://www.paulkerrison.co.uk>




6

SOLUTIONS & TAKEAWAYS



REGULAR TESTING

- Web application/site security testing
- OWASP 4.1 now has cloud testing
- Monitoring your assets in the cloud

 PROJECTS CHAPTERS EVENTS ABOUT

Donate Join

Watch 129 Star 1,598

WSTG - v4.1

Test Cloud Storage

ID
WSTG-CONF-11

Summary

Cloud storage services facilitate web application and services to store and access objects in the storage service. Improper access control configuration, however, may result in sensitive information exposure, data being tampered, or unauthorized access.

A known example is where an Amazon S3 bucket is misconfigured, although the other cloud storage services may also be exposed to similar risks. By default, all S3 buckets are private and can be accessed only by users that are explicitly granted access. Users can grant public access to both the bucket itself and to individual objects stored within that bucket. This may lead to an unauthorized user being able to upload new files, modify or read stored files.

Test Objectives

Assess whether Cloud Storage Service's access control configuration is properly in place.

The OWASP® Foundation works to improve the security of software through its community-led open source software projects, hundreds of chapters worldwide, tens of thousands of members, and by hosting local and global conferences.

WSTG Contents (v4.1)

- 0. Foreword by Eoin Keary
- 1. Frontispiece
- 2. Introduction
- 2.1 The OWASP Testing Project
- 2.2 Principles of Testing
- 2.3 Testing Techniques Explained
- 2.4 Manual Inspections and Reviews
- 2.5 Threat Modeling
- 2.6 Source Code Review
- 2.7 Penetration Testing
- 2.8 The Need for a Balanced Approach
- 2.9 Deriving Security Test Requirements
- 2.10 Security Tests Integrated in Development and Testing Workflows
- 2.11 Security Test Data Analysis and





Table des content

1. INTRODUCTION	5
1.1 Contexte	5
1.2 Portée	5
2. CONFORMITE	6
3. LISTE DE TEST DÉTAILLÉ	7
3.1 Cloud AWS Penetration Test	8
3.1.1 AWS Patterns	8
3.1.2 AWS Metadata SSRF	8
3.1.3 AWS Shadow Admin	8
3.1.4 AWS - Gaining AWS Console Access via API Keys	8
3.1.5 AWS - Mount EBS volume to EC2 Linux	8
3.1.6 AWS - Copy EC2 using AMI Image	8
3.1.7 AWS SSH key push to EC2 instance	8
3.1.8 AWS Lambda - Extract function's code	8
3.1.9 AWS SSM Command Execution	8
3.1.10 AWS Golden SAML Attack	8
3.1.11 AWS Shadow Copy Attack	8
3.2 Cloud Azure Penetration Test	8
3.2.1 Azure Storage Account Blob	8
3.2.2 Azure AD Enumeration	8
3.2.3 Azure Password Spray	8
3.2.4 Azure Service principal signing	8
3.2.5 Azure AD connect - Password Extraction	9
3.2.6 MSOL Account and DCSync	9
3.2.7 Azure Single Sign On Silver Ticket	9
3.2.8 Azure Common Execution as NT System	9
3.3 Kubernetes	9
3.3.1 Listing Secrets	9
3.3.2 Access Any Resource or Verb	9
3.3.3 Pod Creation	9
3.3.4 Privilege to Use Pods/Exec	9

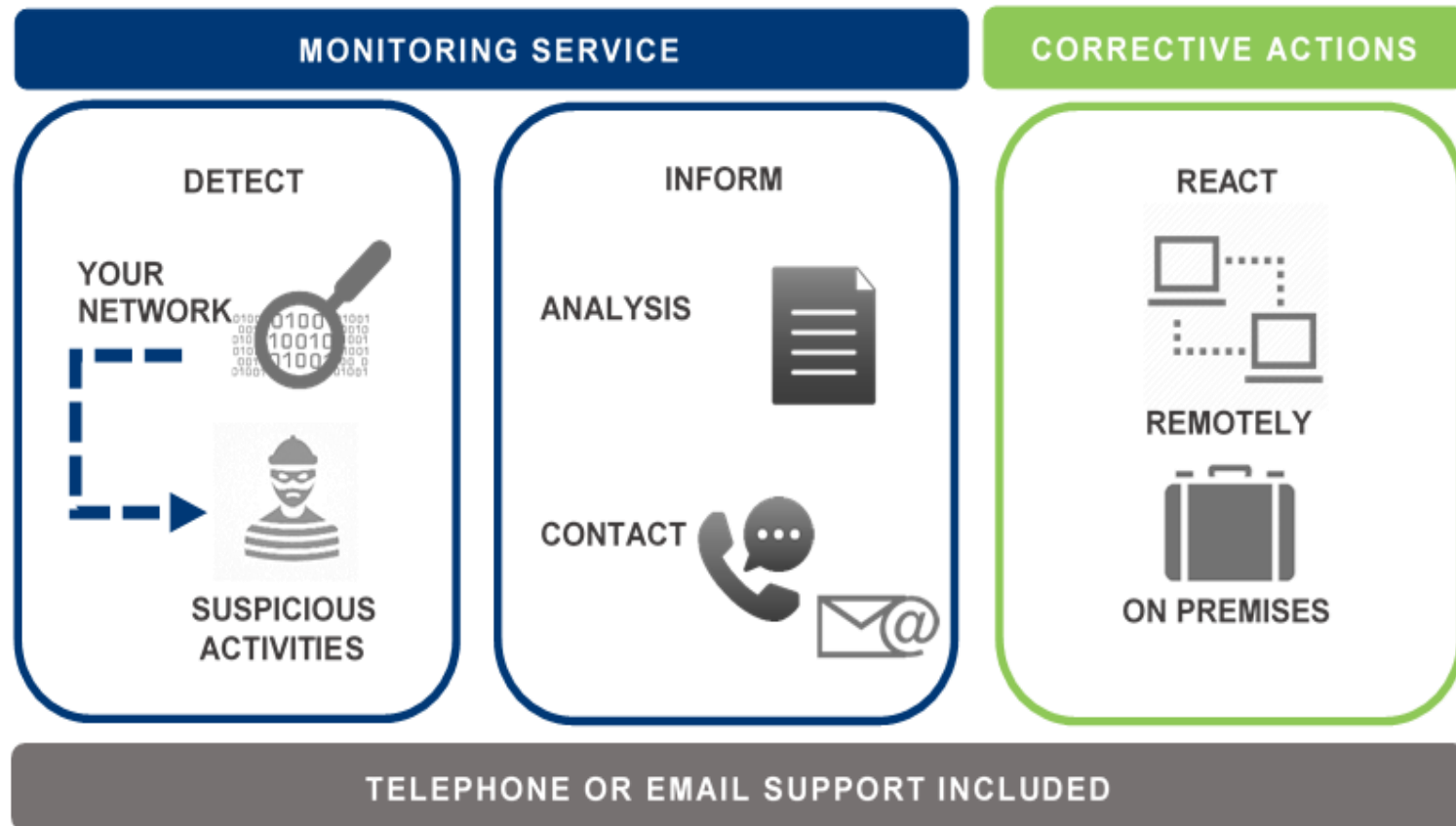
© ESI Technologies

3





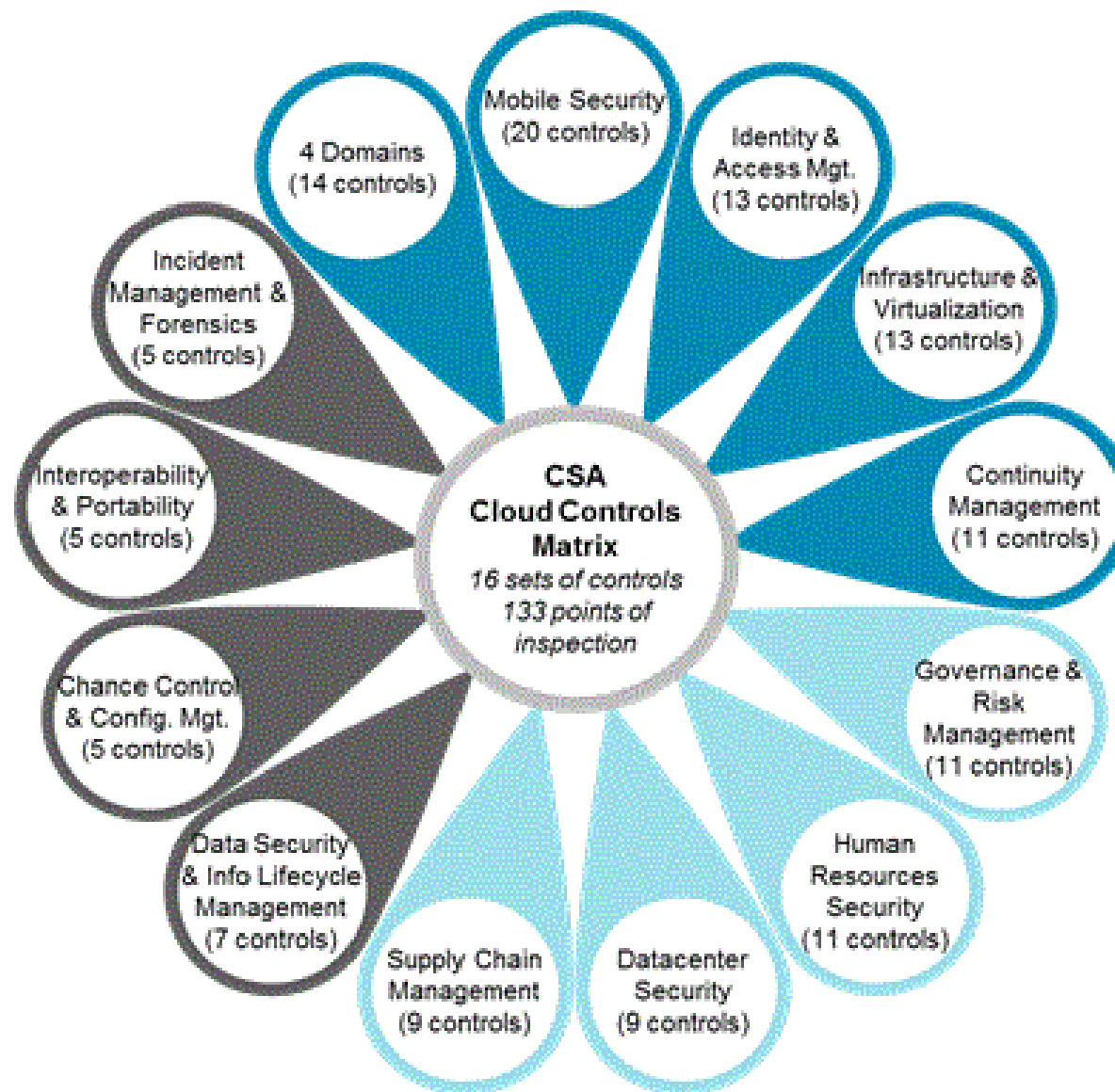
MONITORING THE CLOUD TO PROTECT ASSETS



- Sensor installed on a VM in customer infrastructure to collect data and detect anomalies.
- Alerts analyzed by trained and certified NOC & SOC specialists.
- ESI informs customer of any performance issues or cyber threats to its business.
- A reaction to the threat is orchestrated to mitigate risks and bring situation back to normal.

**MORE CONTROLS =
ADDITIONAL RISKS**

CSA Cloud Control Matrix



Source: Cloud Security Alliance

IF THERE ARE SO MANY RISKS, WHY ARE ORGANIZATIONS MOVING TO THE CLOUD?

→ **Business Agility** becomes the primary goal

1

As the pandemic situation evolves and organizations move through the stages of recovery, their business focus will shift along with their technology investment priorities.

2

Technology plays a critical role in helping organizations maintain business resiliency through the downturn & recession, ultimately preparing for a return to growth & “the next normal” where digital capabilities will be vital to success.

3

Until COVID-19 is eradicated and/or a vaccine is widely available, we should expect waves of new COVID-19 infections and lockdowns. For many businesses this means they revert to an earlier stage, i.e., to recession, slow down or even crisis mode.

4

In this dynamic and uncertain environment, technology suppliers must adapt in order to meet their customers' needs at the corresponding stage. Some organizations may arrive in the next normal without experiencing any significant growth.

LOOKING FOR A SAFE MANAGED CLOUD?


- ESI has a cloud migration team capable of bringing your organization into the cloud, safely
- ESI has a cloud hosted in 2 datacenters
- SOC
- Professional consulting services
- Looking only to bring certain things into the cloud? ESI offers:
 - > BaaS
 - > IaaS
 - > PaaS



FIVE TAKEAWAYS



1. Amazon, Microsoft, Google cloud are not impregnable
2. You are ultimately responsible of your assets' security in the cloud
3. Web testing should be conducted regularly
4. Monitoring is a good way to keep an eye on your assets in the cloud
5. ESI can provide expert advice to ensure your business agility



ESI Technologies Toronto – Montreal – Quebec City - USA

Thanh Nguyen, CISSP
Marco Estrela, PMP – 514 236-0056
Toll Free: 1 800 260-3311

