

Cloud Security

Jornada TIC UPC 2021 - Memorial Víctor Huerta



A bots i barralls...

Jordi Guijarro Olivares

Cybersecurity Innovation Director - i2CAT
Barcelona cloudadmins.org



UNIVERSITAT POLITÈCNICA
DE CATALUNYA
BARCELONATECH



Never stop
designing the
digital future

i2CAT.net



Cloud Computing Vision



"If computers of the kind I have advocated become the computers of the future, then computing may some day be organized as a public utility, just as the telephone system is a public utility... The computer utility could become the basis of a new and important industry."

-- John McCarthy, MIT Centennial, 1961



Cloud Computing Vision



"If computers of the kind I have advocated become the computers of the future, then computing may some day be organized as a public utility, just as the telephone system is a public utility... The computer utility could become the basis of a new and important industry."

-- John McCarthy, MIT Centennial, 1961

- computing == fungible utility!
- limitations exist: API lock-in, hardware dependence, latency, privacy, security...







WHY FACEBOOK WENT DOWN?

Detecting BGP Suspicious Changes

<https://socprime.com/blog/what-is-bgp-and-how-its-failure-took-facebook-down/>



THE WALL STREET JOURNAL.

Subscribe | Sign In

English Edition | Print Edition | Video | Podcasts | Latest Headlines

Home World U.S. Politics Economy Business Tech Markets Opinion Books & Arts Real Estate Life & Work WSJ Magazine Sports

Search 🔍

SHARE



TECH

Amazon Outage Disrupts Lives, Surprising People About Their Cloud Dependency

When Amazon Web Services was interrupted, some vacuum cleaners, light switches and cat-food dispensers stopped working



How Cloud Computing Became a Big Tech Battleground

Big tech firms are investing in data centers as they compete for the \$214 billion cloud computing market. WSJ explains what cloud computing is, why big tech is betting big on future contracts. (Video from 11/19/19)

By [Sarah E. Needleman](#)

MOST POPULAR NEWS

1. Southern California's Container-Ship Backlog Moves Farther Out to Sea



2. Sky-High Vaccination Rates, Zero Taxes Create Boomtown



3. Meet the Kidd Who Goes Toe to Toe With Warren Buffett



4. Rupert Murdoch Buys \$200 Million Montana Ranch From the Koch Family



5. U.S. Inflation Hits 39-Year High



MOST POPULAR OPINION

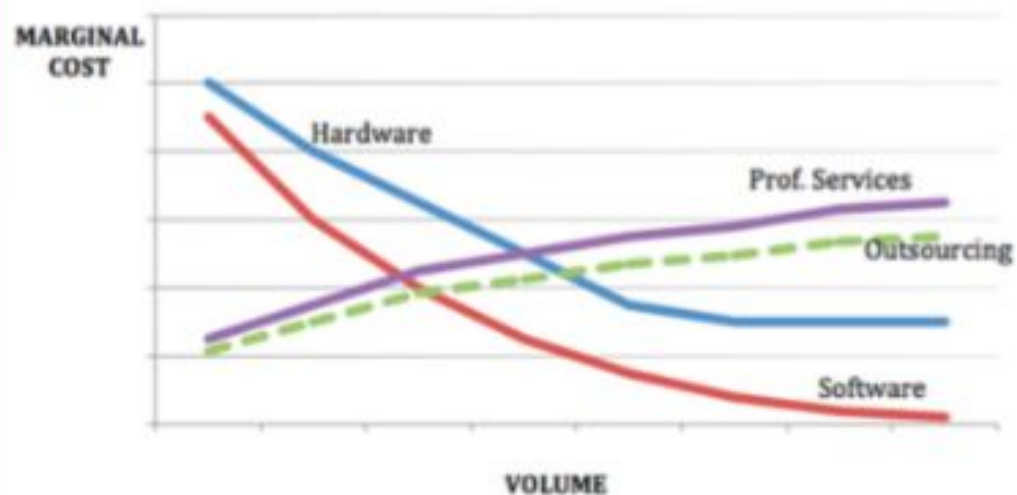
1. Opinion: Kamala Harris Needs to Get



Cloud Economics - Where's the Margin?

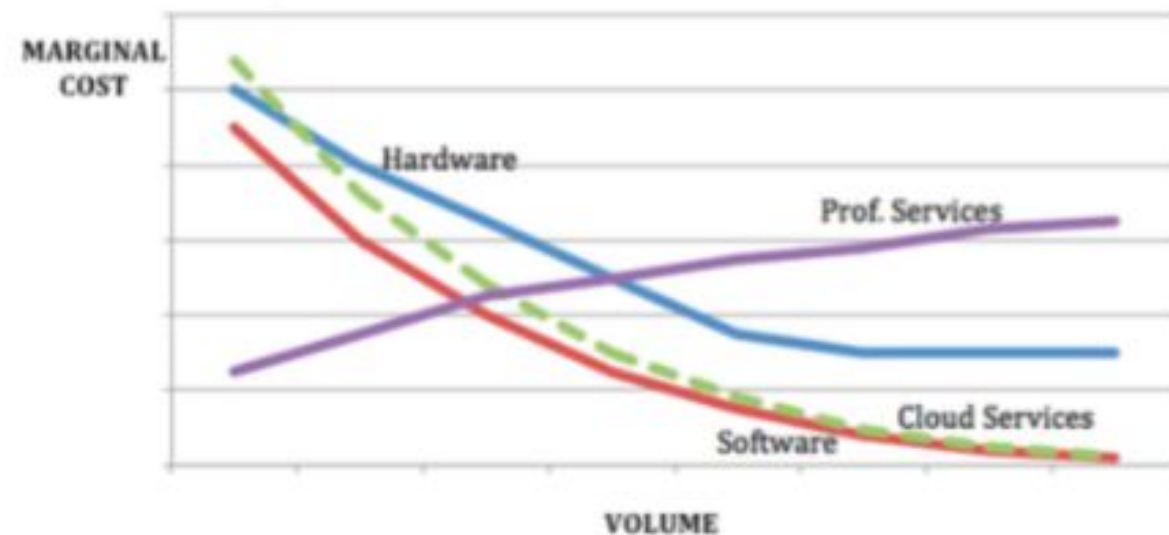
Pre-Cloud Era

Enterprise IT Economics: 1990 - 2010



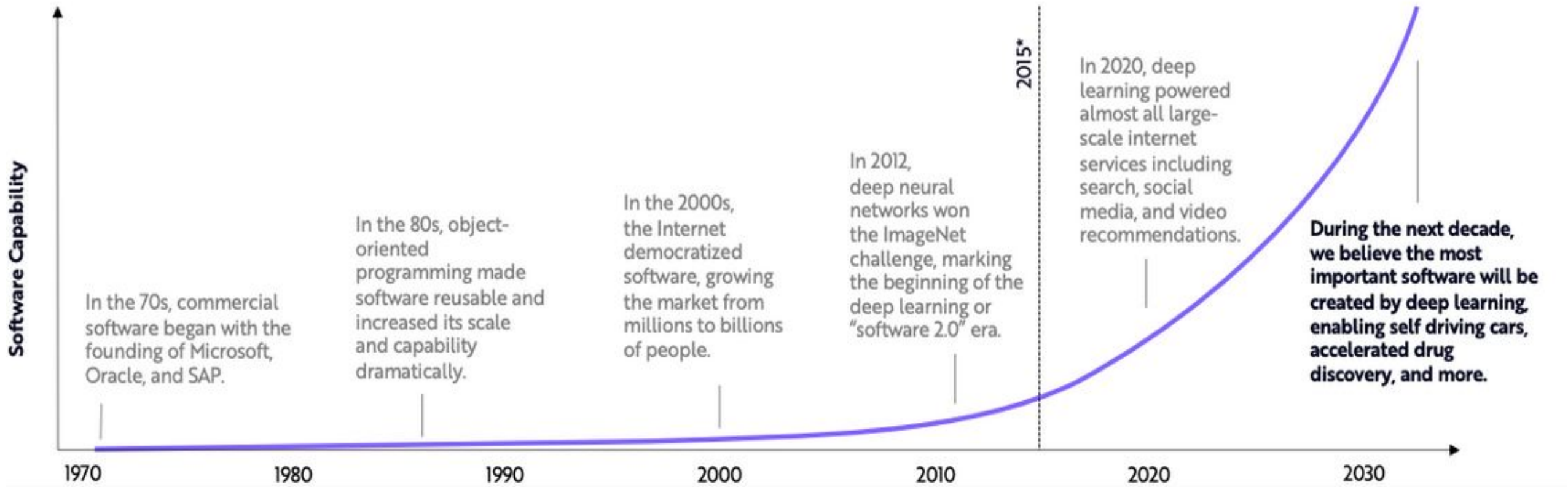
Post-Cloud Era

Enterprise IT Economics - 2010 - 2030



Software 1.0 Code Written by Humans

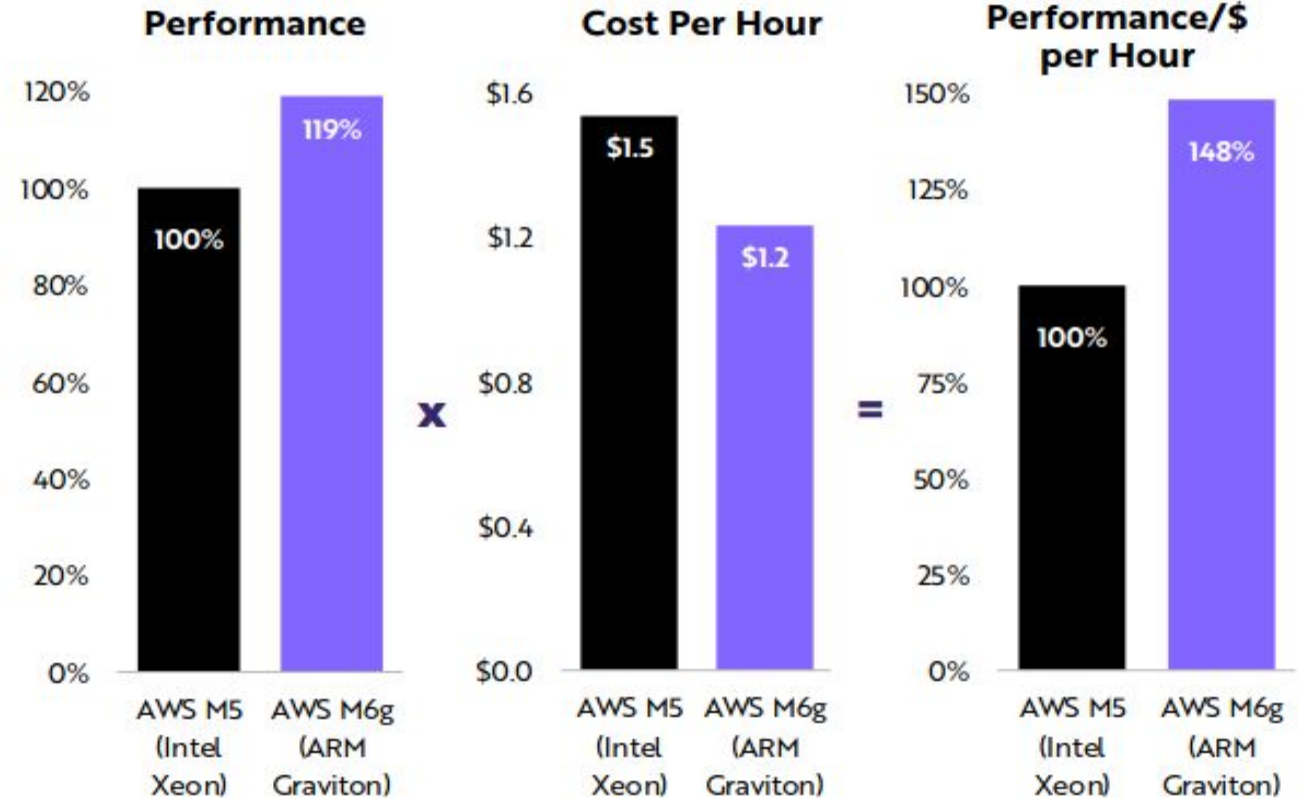
Software 2.0 Code Written by Data





ARM Could Become The New Standard In The Cloud

- The public cloud, the default platform for deploying new applications, generated \$140 billion in global revenues in 2020.
- Amazon Web Services (AWS)—the largest public cloud provider in the world—launched the Graviton 2 ARM CPU in 2020, reducing its need to purchase chips from Intel and AMD.
- AWS Graviton 2 is cheaper and faster than Intel CPUs, offering 48% higher performance per dollar.
- In the future, AWS is likely to migrate most of its servers to ARM based processors.



Forecasts are inherently limited and cannot be relied upon. | For informational purposes only and should not be considered investment advice, or a recommendation to buy, sell or hold any particular security. Note for Third Chart: Time is implied. The math is: $(119/1.2)/(100/1.5)-1$. Source: ARK Investment Management LLC, 2020 based on data sourced from: "Global Cloud Services Market Q2 2020." Canalys, www.canalys.com/newsroom/worldwide-cloud-infrastructure-services-Q2-2020, Michael Larabel. "Benchmarking Amazon's Graviton2 Performance With 64 Neoverse N1 Cores Against Intel Xeon, AMD EPYC." Phoronix, May 2020, www.phoronix.com/scan.php?page=article&item=amazon-graviton2-benchmarks&num=12, Daly, Donald J., and Donald J. Daly. "Economics 2: EC2." Amazon, CGA Canada Publications, 1987, aws.amazon.com/ec2/pricing/.



Top Threats to Cloud Computing

1. Data Breaches (1)
2. Misconfiguration and Inadequate Change Control
3. Lack of Cloud Security Architecture and Strategy
4. Insufficient Identity, Credential, Access and Key Management
5. Account Hijacking (5)
6. Insider Threat (6)
7. Insecure Interfaces and APIs (3)
8. Weak Control Plane
9. Metastructure and Applistructure Failures
10. Limited Cloud Usage Visibility
11. Abuse and Nefarious Use of Cloud Services (10)

<https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-egregious-eleven/>



Investment in cloud security must match cloud spend

In the early days of the COVID-19 pandemic, there was a rapid uptick in demand for cloud services. Utilizing data pulled from our global array of sensors, our elite cloud threat researchers found a correlation: Organizations globally increased their cloud workloads by more than 20%, leading to an explosion of security incidents. Our research shows that cloud security programs for organizations globally are still in their infancy when it comes to security automation (i.e., DevSecOps and shift left). We concluded that rapid cloud scale and complexity without automated security controls embedded across the entire development pipeline are a toxic combination.



Matthew Chiodi
Chief Security Officer, Public Cloud



Cloud Growth vs. Cloud Security Incidents

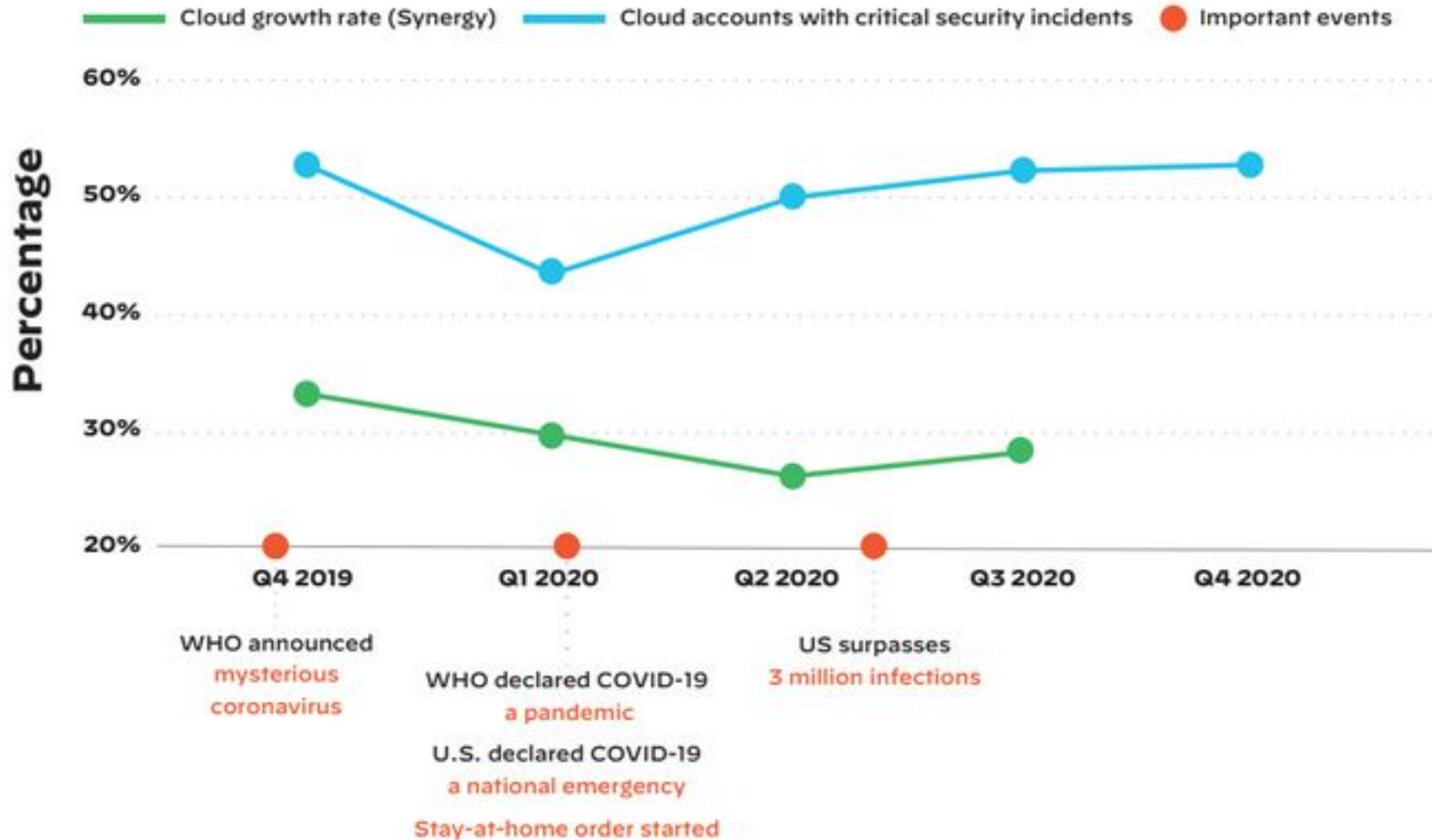
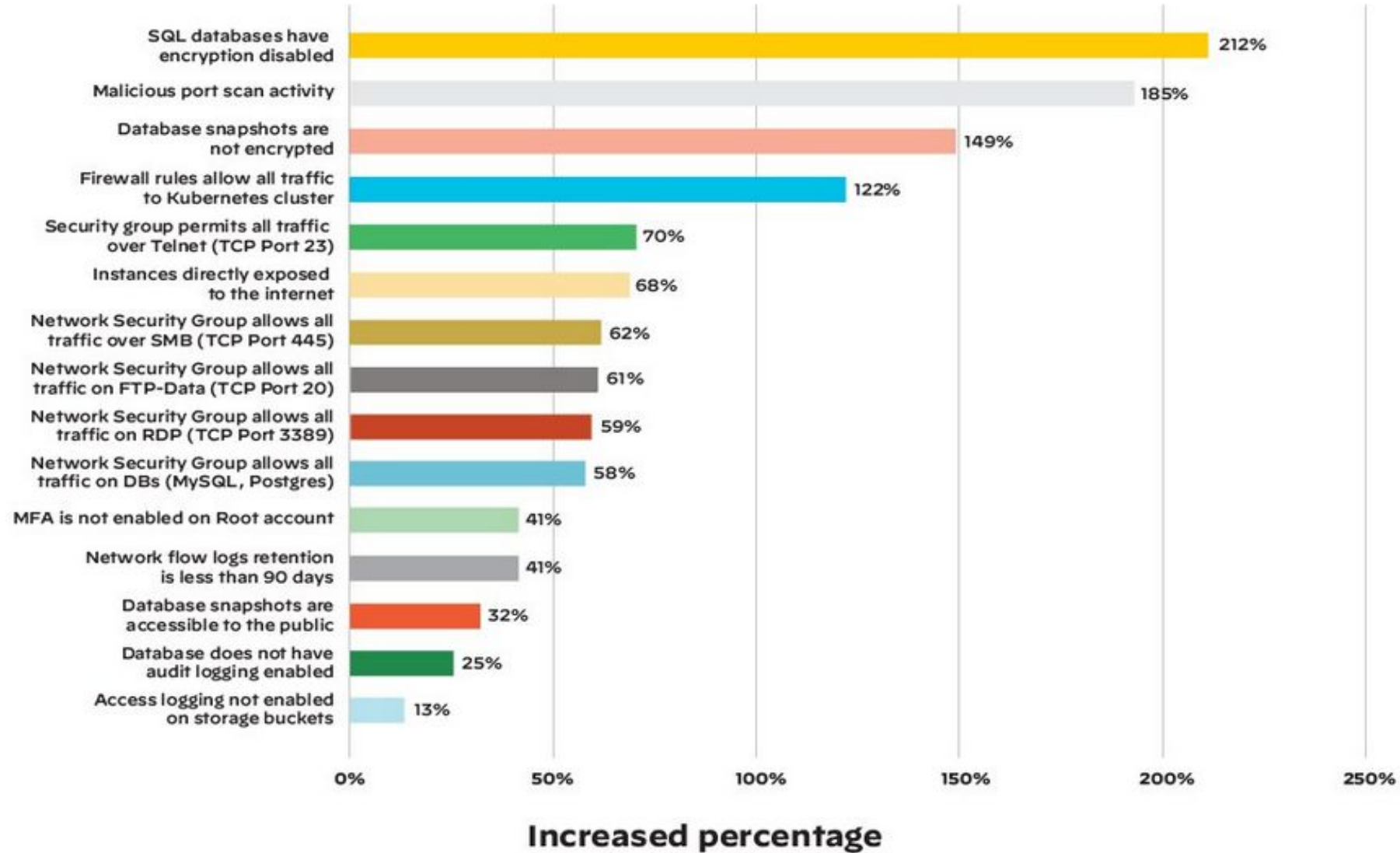


Figure 1: Cloud growth and security incidents



Security incidents with the biggest increase



COVID-19 and Data Security

Businesses are favoring cloud storage due to its reliability, availability, and scalability. Our research shows that 64% of data in the cloud contains sensitive information (e.g., PII, intellectual property, healthcare and financial data). Within that 64% subset, 69% contains PII, and 34% contains intellectual property (see figure 8).

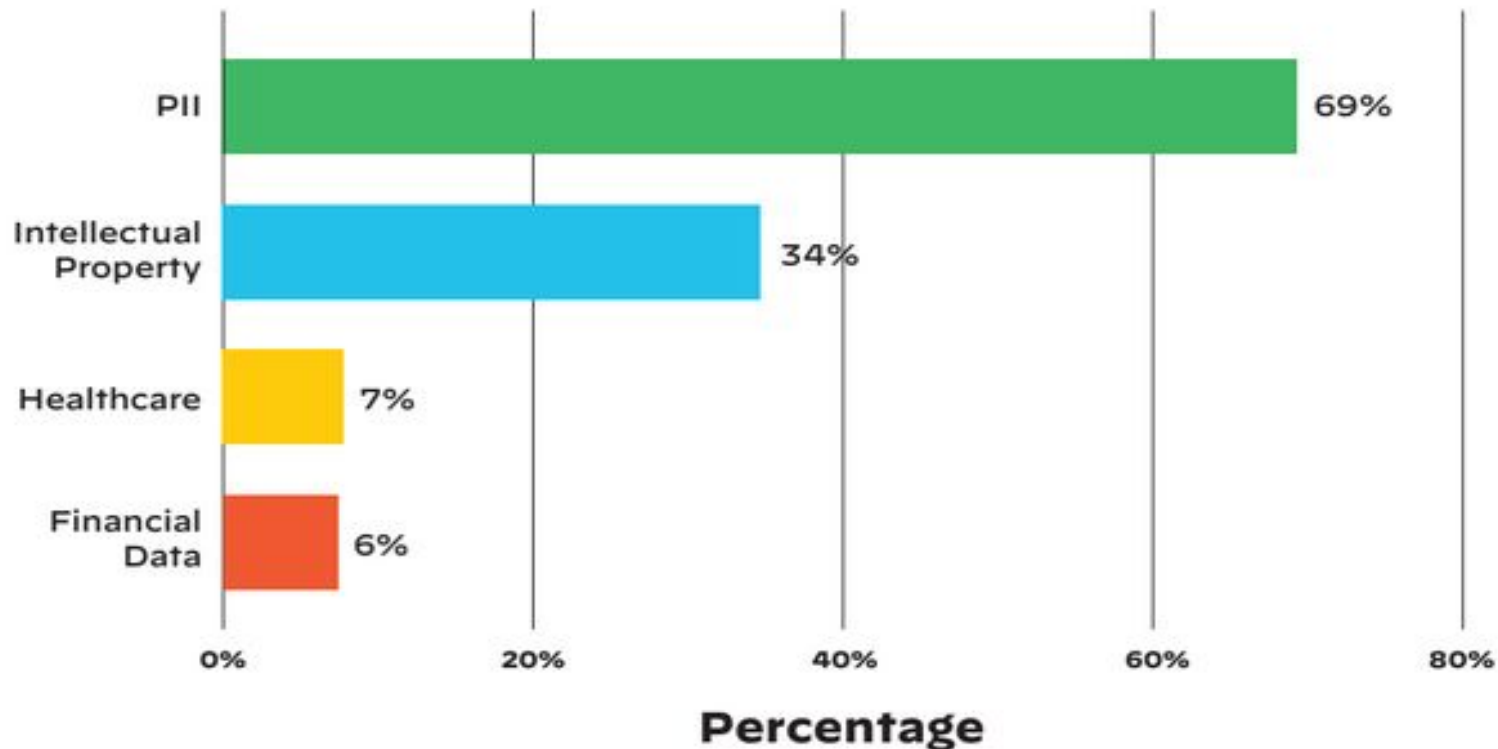


Figure 8: Prevalence of sensitive data types among sensitive data stored in clouds



Mining Trends and Market Events

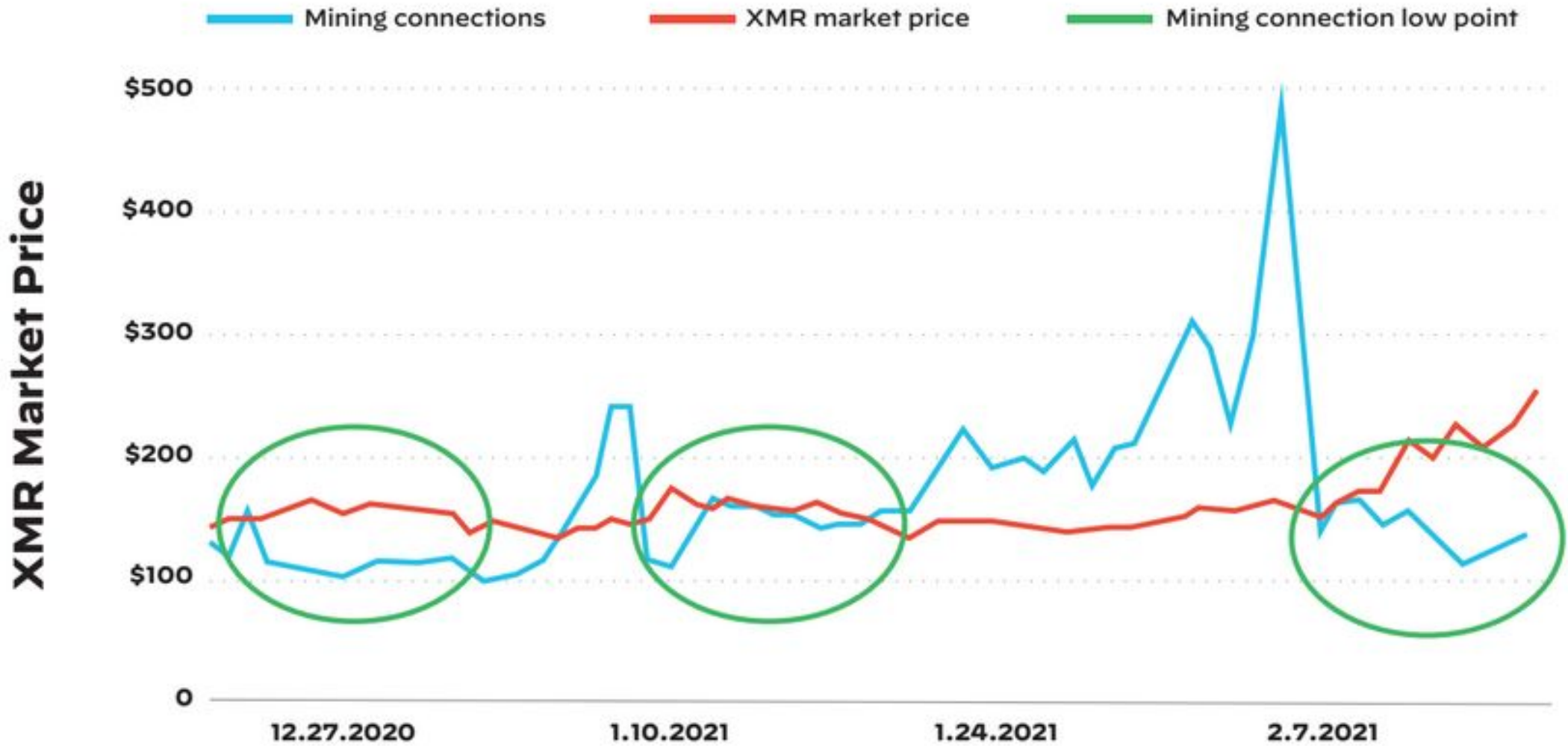


Figure 10: Comparison of cryptomining connections and XMR price



Cloud Governance



Shared Responsibility Model

Responsibility	On-premises	IaaS	PaaS	SaaS	FaaS	CIS Controls Companion Guide	CIS Foundations Benchmarks
Data classification and accountability	●	●	●	●	●	✓	✓
Client and end-point protection	●	●	●	●/○	●/○	✓	✓
Identity and access management	●	●	●/○	●/○	●/○	✓	✓
Application-level controls	●	●	●/○	●/○	●/○	✓	✓
Network controls	●	●/○	○	○	○	✓	✓
Host infrastructure	●	●/○	○	○	○	✓	
Physical security	●	○	○	○	○		

● Cloud Customer ○ Cloud Provider



Cloud Security Mapping



Mapping of On-Premises Security Controls Versus Services Offered by Major Cloud Providers



ON-PREMISES	AZURE	AWS	GOOGLE	ORACLE	IBM	ALIBABA	TENCENT
Firewall & ACLs	Azure Firewall Network Security Groups	AWS Network Firewall AWS Network ACLs	VPC Firewall	SmartNIC Oracle CloudGuard	Virtual Router Appliance	Cloud Firewall	VPC Network ACLs Security Groups
IPS/IDS	Azure Firewall	AWS Network Firewall Amazon Detective				Cloud Firewall	Cloud Workload Protection
Web Application Firewall (WAF)	Azure Web Application Firewall (WAF)	AWS WAF AWS Firewall Manager	Cloud Armor WAF	Oracle WAF	Cloud Internet Services	Cloud WAF	Web Application Firewall
SIEM & Log Analytics	Azure Sentinel	Amazon Detective Security Hub/GuardDuty	Chronicle Backstory Event Threat Detection	Oracle Security Monitoring and Analytics	Cloud Log Analysis Cloud Activity Tracker	Log Analysis	Security Operations Center
Data Loss Prevention (DLP)	Azure Inf. Protection M365 Compliance Center	Amazon Macie	Cloud Data Loss Prevention API			Web Application Firewall	
Key Management	Azure Key Vault	Key Management Service AWS Secrets Manager	Cloud Key Management Service	Cloud Infrastructure Key Management	Key Protect Cloud Security	Key Management Service (KMS)	Secrets Manager Key Management Service
Encryption At Rest	Storage Encryption for Data at Rest	EBS/EFS Volume Encryption, S3 SSE	Google Cloud Platform (native)	Cloud Infrastructure Block Volume	Hyper Protect Crypto Services	Data Encryption Service	Key Management Service (Beta)
DDoS Protection	Azure DDoS Protection	AWS Shield	Cloud Armor	Built-in DDoS defense		Anti-DDoS	Anti-DDoS
SSL Decryption Reverse Proxy	Application Gateway	Application Load Balancer	HTTPS Load Balancing		Cloud Load Balancer		
Certificate Management	Azure Key Vault	AWS Certificate Manager	Secret Manager Cloud Key Management		Certificate Manager	Cloud SSL Certificates Service	
Container Security	Azure Defender	Amazon ECR Container Service (ECS)	Kubernetes Engine	Oracle Container Services	Containers - Trusted Compute	Container Registry	
Identity and Access Management	Azure Active Directory PIM	Identity and Access Management (IAM)	Cloud IAM	Oracle Cloud Infrastructure IAM	Security Verify	Resource Access Management (RAM)	Tencent Cloud Organization
Privileged Access Management (PAM)	Azure AD Privileged Identity Management				Security Verify		
Multi-Factor Authentication (MFA)	Azure MFA	AWS MFA (part of AWS IAM)	Titan Security Key	Oracle Cloud Infrastructure IAM	Security Verify	Resource Access Management (RAM)	
Centralized Logging / Auditing	Azure Monitor Azure Sentinel	CloudWatch / S3 bucket	Stackdriver Mon / Logging Access Transparency	Oracle Cloud Infrastructure Audit	Log Analysis with LogDNA	ActionTrail	FlowLogs
Load Balancer	Azure Load Balancer	Application Load Balancer Classic Load Balancer	Cloud Load Balancing HTTPS Load Balancing	Cloud Infrastructure Load Balancing	Cloud Load Balancer	Server Load Balancer (SLB)	Cloud Load Balancer
LAN	Virtual Network	Virtual Private Cloud (VPC)	Virtual Private Cloud (VPC)	SmartNIC	VLANs	Virtual Private Cloud (VPC)	Virtual Private Cloud (VPC)
WAN	ExpressRoute	Direct Connect	Dedicated Interconnect	FastConnect	Direct Link	VPN Gateway Express Connect	Direct Connect (DC)
VPN	Azure Virtual Network Gateway	VPC Customer Gateway AWS Transit Gateway	Google VPN	Dynamic Routing Gateway (DRG)	IPSec VPN Secure Gateway	VPN Gateway	VPN Connection
Governance Risk and Compliance Monitoring	Azure Security Center M365 Compliance	AWS Security Hub AWS Compliance Center	Cloud Security Command Center		Cloud Security & Compliance Center	ActionTrail	CloudAudit
Backup and Recovery	Azure Backup Azure Site Recovery	AWS Backup CloudEndure DR	Object Versioning Cloud Storage Nearline	Archive Storage	Cloud Backup	Hybrid Backup Recovery	
Vulnerability Assessment	Azure Defender Azure Security Center	Amazon Inspector AWS Trusted Advisor	Cloud Security Scanner	Security Vulnerability Scanning Service	Cloud Security Advisor Vulnerability Advisor	PenetrationTest Website Threat Inspector	Cloud Workload Protection
Patch Management	Azure ARC Update Management	AWS Systems Manager		Risk Management Cloud	IBM Cloud Orchestrator		
Change Management	Azure Automation Change Tracking and Inventory	AWS Config				Application Configuration Management (ACM)	
IoT Security	Azure Defender for IoT	AWS IoT Device Defender	Edge TPU IoT Core		Watson IoT Platform Edge Application Manager	IoT Platform Link IoT Edge	
Extended Storage	Azure Data Explorer (ADX) Azure Log Analytics	Amazon S3 Glacier	Cloud Storage for Data Archiving	Archive Storage	Cloud Block Storage	Log Service	
Secure Operation & Management	Azure Bastion		Google Cloud Operation Suite (form. Stackdriver)	OCI Bastion		BastionHost	
Application Security		Amazon Inspector					Mobile Security
Email Protection	Defender for Office 365		Various controls embedded in G-Suite				
Antimalware	Azure Defender					Threat Detection Service (TDS)	
Endpoint Protection	Defender For Endpoint Azure Defender		Shielded VM			Server Guard	
File Integrity Monitoring (FIM)	Azure Defender		Shielded VM				
Cloud Access Security Broker (CASB)	Microsoft Cloud App Security (MCAS)			Oracle CASB			

Shared Responsibility Model



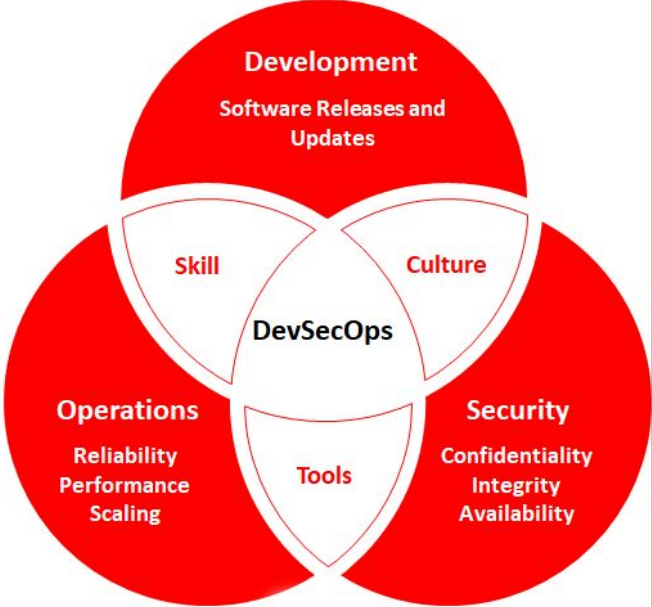
CIS Benchmarks™



With our global community of cybersecurity experts, we've developed CIS Benchmarks: more than 100 configuration guidelines across 25+ vendor product families to safeguard systems against today's evolving cyber threats.

Join a Community

DevSecOps is a MUST!



Log4Shell

Critical Log4j Vulnerability Threatens Major Internet Players



vulnerability in Apache Log4j which affects many major internet-facing services. Log4j is a Java logging package that's used in many popular services and utilities. With a CVSS score of 10, this vulnerability ([CVE-2021-44228](#)) impacts Apache Log4j versions 2.0-beta9 to 2.14.1 according to [Apache](#).





Google Cloud

IDENTITY & SECURITY

Google Cloud Armor WAF rule to help mitigate CVE-2021-44228 Apache Log4j vulnerability

Log4Shell

Critical Log4j Vulnerability

Net Players



The Cloudflare Blog

Thanks for being here

Email Address

Product News

Speed & Reliability

Security

Serverless

Zero Trust

Developers

Deep Dive

Inside the Log4j2 vulnerability (CVE-2021-44228)

10/12/2021

☰ README.md

Logout4Shell



cybereason®

Description



However, enabling these system property requires access to the vulnerable servers as well as a restart. The [Cybereason](#) research team has developed the following code that *exploits* the same vulnerability and the payload therein forces the logger to reconfigure itself with the vulnerable setting disabled - this effectively blocks any further attempt to exploit Log4Shell on this server.

This Proof of Concept is based on [@tangxiaofeng7's tangxiaofeng7/apache-log4j-poc](#)

SOFT LAW & CLOUD PROVIDERS



International standards (ISOs) would be part of the Soft Law that, although not mandatory, establishes the principles of quality in the provision of cloud services by the companies that comply with them.

The most relevant ISO in the provision of cloud services would be:

ISO 27001: For information security management systems. It focuses on risk assessment and the application of essential controls for their mitigation and elimination.

ISO 27002: Good practice guide that describes the control objectives and recommended controls in relation to information security.

ISO / IEC 27017: Security controls for cloud services. It focuses on aspects of responsibility, elimination and return of assets at the end of the contract, operations and administrative procedures, ...

ISO / IEC 27018: For the control of data protection in Cloud services.

It is also important to highlight the National Institute of Standards and Technology Framework (NIST) and the Cloud Security Alliance (CSA) which is a voluntary tool intended to help organizations identify and manage the risk of privacy to build innovative products and services, protecting the privacy of people.







Your Security Response Toolkit

This site offers a proposed collection of tools in a [plug&play live image](#) to provide first steps to new incident handling teams. Information on this site reflects the experience of a number of [European CSIRTs](#), with tools used and supported by [active CSIRTs](#).

[START!](#)

WITH COLLABORATION OF



*The Internet
Research Center
Fostering your
Innovation*



Gartner Says Four Trends Are Shaping the Future of Public Cloud

Regional Cloud Ecosystems

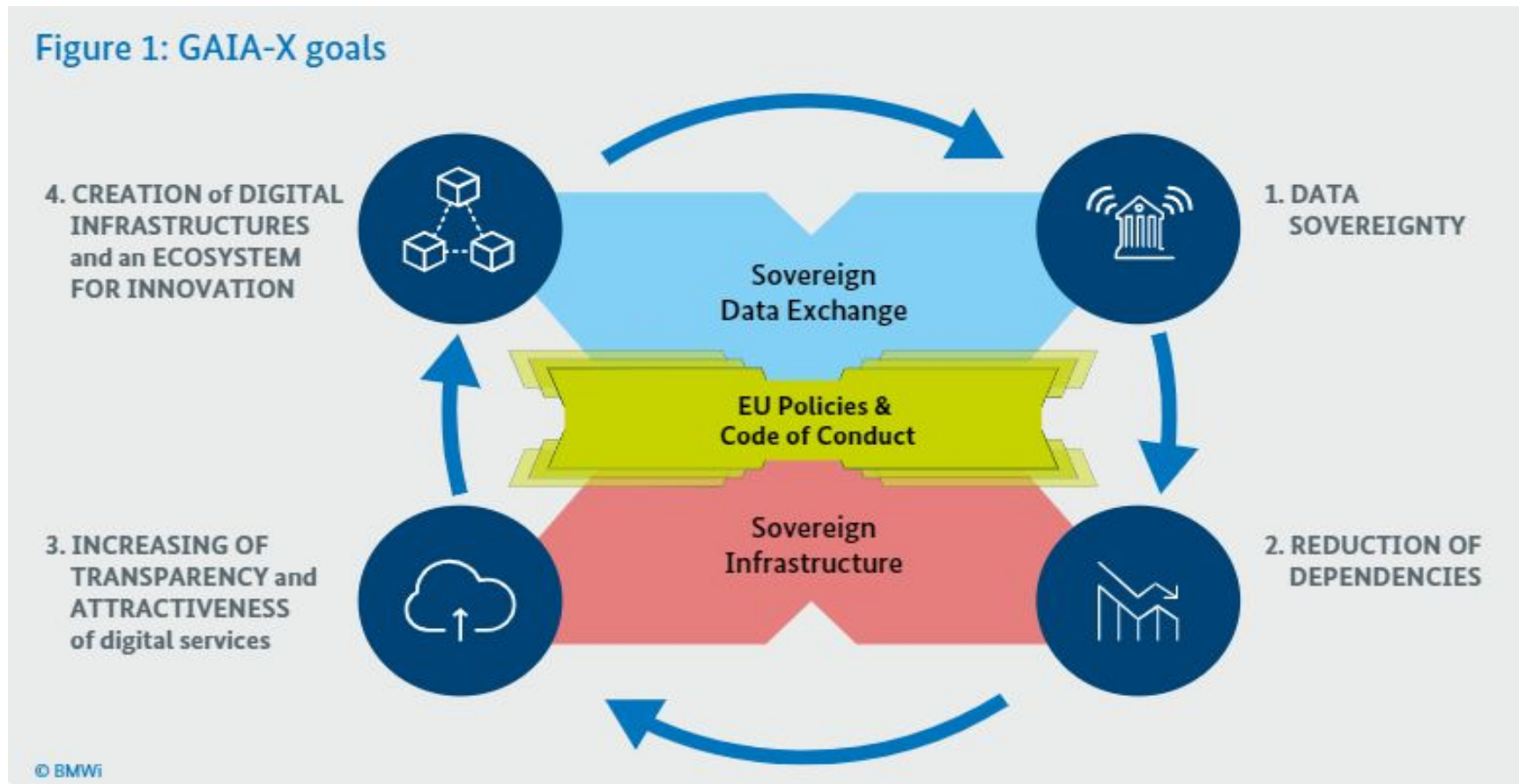
Growing geopolitical regulatory fragmentation, protectionism and industry compliance are driving the creation of new regional and vertical cloud ecosystems and data services. Companies in the financial and public sectors are looking to reduce critical lock-in and single points of failure with their cloud providers outside of their country.

Regions not able to create or sustain their own platform ecosystems will have no choice but to leverage the platforms created in other regions and resort to legislation and regulation to maintain some level of control and sovereignty. Concerns among politicians, academia and tech providers in these regions are increasing, leading to initiatives such as [GAIA-X](#) in European countries.

Sovereign Data Driven Clouds: Gaia-X initiative



<https://gaia-x.eu/>





i2cat[®]

THE INTERNET
RESEARCH CENTER



Research i2cat[®] Te
Impact i2cat[®] Knowledge i2
i2cat[®] Co-creation i2cat[®] Empe
Talent i2cat[®] Innovation i2
i2cat[®] Technology i2cat[®] Cre
i2cat[®] People i2
Commitment i2cat[®] In
i2cat[®] Vision i2
Collaboration i2cat[®] Comu
i2cat[®] Co-creation i2
Impact i2cat[®] Know

Thanks! Q&A

@jordiguijarro



Never stop
designing the
digital future



BONUS SLIDE



Cloud Admins Barcelona

Barcelona, España
300 miembros · Grupo público
Organizado por George S. y otras 4 personas

Compartir: [f](#) [t](#) [in](#)

Newsletter | Subscríbete y recibe GRATIS el primer capítulo del libro Devops y Seguridad Cloud. Recibe los últimos artículos y eventos, directamente en tu buzón

[Suscríbete →](#)



Recording 🚀 Cyberops e-TechDay Barcelona 24/11/21 16h CEST

The Cloudadmins TechDays (now turned virtual due to the COVID-19 pandemic) are educational and networking events organized by...

Jordi Guijarro
1 Dic. 2021 · 1 min de lectura

