Citihub Digital
a Synechron company

June 2021

Essential Capabilities for building Defense in Depth for Public and Hybrid Cloud

Contents

Author

Chris Zanelli
chris.zanelli@citihub.com

Introduction

In today's environment of frequent and persistent cyber attacks by domestic and international bad actors its essential to ensure security safeguards and multi-layered controls are implemented across your public cloud landing zones and hybrid cloud perimeters within your DMZ. Cloud architectures require a significantly different approach to building **Defense in Depth** for Public and Hybrid Cloud – basically standing traditional perimeter and domain-based controls on their heads and exposing fundamental gaps in how layered, perimeter-based security models and control assurance alone are inadequate for organizations operating part-or-all their operations in Public Cloud."

So how does one effectively take control of complex cloud deployments, which are highly prone to configuration and human error-driven exploits? How do we design and build Defense in Depth in Public and Hybrid Cloud environments? How can an organization 'flatten', simplify, and assure a set of controls and configurations across subscription, landing zone, management hierarchy, identity, resource, service, and object levels? And lastly, how are overlapping controls bolster the 5 pillars of Cyber Security that NIST 800-53 prescribes - Identify, Detect, Protect, Respond, and Recover?

Over a decade ago, security perimeters for most scaled enterprises consisted of a DMZ, internal networks for Production, internal networks for lower SDLC environments, and, optionally, for a tier of mainframe infrastructure. Security was largely focused at the boundaries – DMZ environments containing services for internet, distributed branches, colocation facilities, and B2B circuits / leased lines. Internal applications enjoyed significantly relaxed controls, limited VLAN segregation, and fairly flat network topologies relying mostly on identity authentication and a mix of fine-grained entitlement management solutions tied to corporate identities and groups. Security and Risk officers were given reasonable assurances that exposures on the edge would be remediated aggressively whilst risk exceptions and tradeoffs were frequently made within internal networks to allow for productivity and efficiency.

In the early 2010's, as cyber security threats and exploits started becoming more of a public occurrence and conversation at the board level, defense in depth because the universally accepted strategy to minimize the occurrences and disruption of the inevitable – eventual catastrophic breach. Significant focus was placed on enhanced network segregation and controls, end user multi-factor authentication, secrets management, enhanced controls over identities (humans and systems) & identity providers, and locking down server & device administrative interfaces and shells. As layered security was being implemented and applied, employees were provided annual education on cyber security threats in an effort to raise awareness beyond the typical response of "my application isn't external-facing, so what's the risk?"

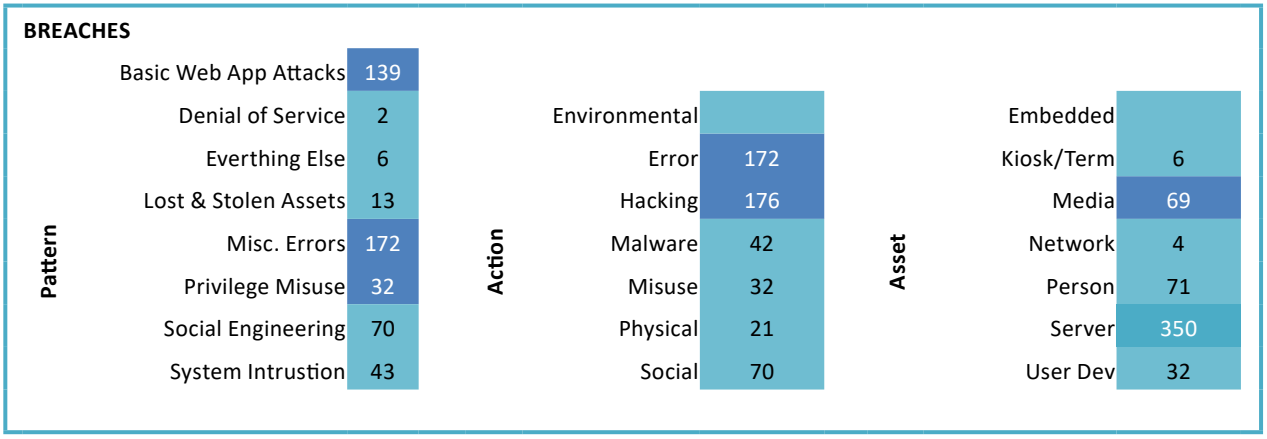
As enterprises start to build more of their application functions in the Public cloud, they gain the flexibility and velocity that Public Cloud infrastructure providers offer but they lose out on many of these internal capabilities built over the years – safeguards, guardrails, narrowed jump-host entry, and manual provisioning processes that have been the bulwark of enterprise security strategy for on-premise infrastructure. In contrast, Cloud resource configurations and controls, although continuously improving, still have a razor-thin margin of error that makes an immediate difference between publicly accessible and unencrypted, to identity-oriented object level access.

Leaky cloud services, are often the outcome when misconfiguration errors are combined with the need to manage complex layers of configurations and cloud resource objects. Today our best source of cyber incident research is often the **annual DBIR report**, although we would expect over time continuing improvements and transparency around breaches and affected cloud service providers. Given the persistent threats and combination of organized crime with unaffiliated individual bad actors, there's a growing need for better information sharing and coordination with local and federal law enforcement agencies. Regardless of what industry you are in, your enterprise, supply chain and customer information is at risk in the digital age.

Incidents	Total	Small (1-1,000)	Large (1,000+)	Unknown	Breaches	Total	Small (1-1,000)	Large (1,000+)	Unknown
Total	29,207	1,037	819	27,351		5,258	263	307	4,688
Accommodation (72)	69	4	7	58		40	4	7	29
Administrative (56)	353	8	10	335		19	6	7	6
Agriculture (11)	31	1	0	30		16	1	0	15
Construction (23)	57	3	3	51		30	3	2	25
Education (61)	1,332	22	19	1,291		344	17	13	314
Entertainment (71)	7,065	6	1	7,058		109	6	1	102
Finance (52)	721	32	34	655		467	26	14	427
Healthcare (62)	655	45	31	579		472	32	19	421
Information (51)	2,935	44	27	2,864		381	35	21	325
Management (55)	8	0	0	8		1	0	0	1
Manufacturing (31-33)	585	20	35	530		270	13	27	230
Mining (21)	498	3	5	490		335	2	3	330
Other Services (81)	194	3	2	189		67	3	0	64
Professional (54)	1,892	793	516	583		630	76	121	433
Public (92)	3,236	22	65	3,149		885	13	30	842
Real Estate (53)	100	5	3	92		44	5	3	36
Retail (44-45)	725	12	27	686		165	10	19	136
Wholesale Trade (42)	80	4	10	66		28	4	7	17
Transportation (48-49)	212	4	17	191		67	3	8	56
Utilities (22)	48	1	2	45		20	1	2	17
Unknown	8,411	5	5	8,401		868	3	3	862
Total	29,207	1,037	819	27,351		5,258	263	307	4,688

FIGURE 1: 2021 DBIR REPORT – INDUSTRY BREAKDOWN OF INCIDENTS AND BREACHES

For the financial services sector, over a total of 467 data breaches in 2020 we can look across the underlying actions and assets compromised to observe a significant amount of data leakage and unintended server compromises are down to human errors.



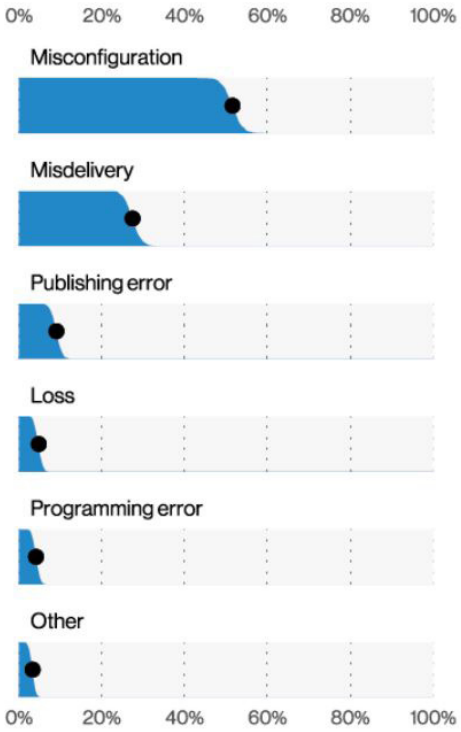


FIGURE 2: 2021 DBIR REPORT (TRUNCATED) – BREACH SUMMARY BY PATTERN, ACTION AND ASSET

How Do We Structure a Renewed Focus for Defense in Depth in the Cloud?

In a cloud runtime environment defense in depth is structured primarily by Public Cloud design, Access Management, Cloud Governance, and Operational Monitoring controls. These design elements can be organized and characterized below as:

1. Landing Zone Architecture
    a. Segmentation
    b. Environment Network Topology
    c. Cloud Resource Design
    d. Management Group Hierarchy
2. Identity and Secrets Management
    a. Identity Providers
    b. Secrets Vaults
3. Cloud Governance
    a. Adoption Framework
    b. Policy Management
4. Cloud Operations
    a. Security Posture Management
    b. Cloud Controls Monitoring

Given that the primary reason enterprises are seeking Public Cloud adoption is for agility, how do you balance iterative maturity and canary applications with a mature implementation of defense in depth in the public cloud? This short answer is that you shouldn't ignore any of the above elements if you are planning to run any critical workloads and operate in a regulated market environment. Planning from day 1 should include the above workstream stakeholders, with a view of crawl/walk/run maturity levels. If you are working too iteratively, discluding organizational teams and security blueprints, you are exposing your organization and your customers to a certainty of heightened risk.

Whilst the above all seem cloud specific, these fundamental concepts are no different and have existed in on-prem, layered infrastructure operating environments as well. You may recognize them previously through organizational structures in your ITAM system, network boundary designations & designs, and through various various legacy tools that provide hardware-based controls, software controls, written policies, operating norms/principles, and human-driven inspection. Cloud providers have encapsulated much of this complexity in their offering, exposing it as simplified, but fragmented tooling (such as AWS Control Tower, AWS Organizations, AWS CloudFormation, AWS CloudWatch, AWS CloudTrail, or other Provider tools) -- each with multiple configuration layers and guidance for how to go about designing, provisioning, auditing, and monitoring a controlled cloud footprint of resources and services. The problem is, how do we build it correctly for our organization and how do we start to understand porting our enterprise and desired cloud controls into these sets of semantics?

Landing Zone Architecture

A key design element towards cloud architecture should ensure isolation, segregation, and layered resiliency controls are ported over to cloud landing zone design that considers isolation, fault tolerance, data security, application-and-data consistency groups, failure domain and recovery objectives.

While it may be tempting to simplify management of cloud resources in a way that aligns with your technology organization (or financial chargeback structures), careful consideration should be made to isolate and segregate landing zones across End-to-End services consistent with Lines of Business (LOBs) for functionally consistent groupings of applications and data. Understanding end-to-end business system interactions and component level design will help ensure that adequate thought is put into the various environments that should be created within a given landing zone. By enlisting the help of Enterprise and LOB-aligned architects, better outcomes of landing zone design including environments (internet facing and internal-only), infrastructure and data resource requirements. A simple analogy is that organizational structures and internal financial vehicles are often volatile, with management layers shifting across human resources, whilst the core business systems and data remains unchanged unless the LOB is divested or significantly restructured. Front to back business process designs also ensure application and components' needs for realtime and batch data flow dependencies are considered in the design of landing zones, environments, and resource access.

Enterprise and LOB-oriented data architects also should play a big role in building the data container strategy across cloud resources based on application component needs, data transport layers, isolation of sensitive data and MNPI to minimize both impact of potential data loss exposure and to establish restrictive access to data containers. Cloud landing zone design and architecture should encompass an understanding of business and IT data flows across system components – whether they are batch or realtime.

Citihub Digital and our parent company Synechron have multiple partnerships in place across GCP, AWS and Azure and have been working with our clients to structure landing zones and environments that incorporate resiliency, segregation and risk management goals. While cloud providers can provide generic guidance about best practices, ultimately what is needed is experienced application and enterprise architects who understand the industry, applicable regulations, and how front->middle->back office applications and infrastructure must function to maximize the business outcomes.

Identity and Secrets Management

Managing identity, credentials, and other system secrets is an essential component to building defense in depth in the public cloud. Given that most access controls and policies will be tied to the identity in a cloud environment its critical to ensure zero-trust principles are adopted and implemented. As the usage of jump server hosts was the typical model for accessing infrastructure environments on-prem for decades, effective cloud-based access is more likely to be domain-less and zero-trust when contrasted with heritage on-prem systems and Identity models.

So what does domain-less really mean? When we consider an on-prem model where one has an established identity within a domain, for example an Active Directory domain on your intranet environment, they typically have a significant level of trust tied to resources on that domain – allowing them things like ssh access to a host and default filesystem access entitlements – even to resources they don't need access to on a regular basis. A governing principle of establishing zero-trust in cloud environments would be ensuring a fine-grained entitlement model down to the target object/asset and action level.

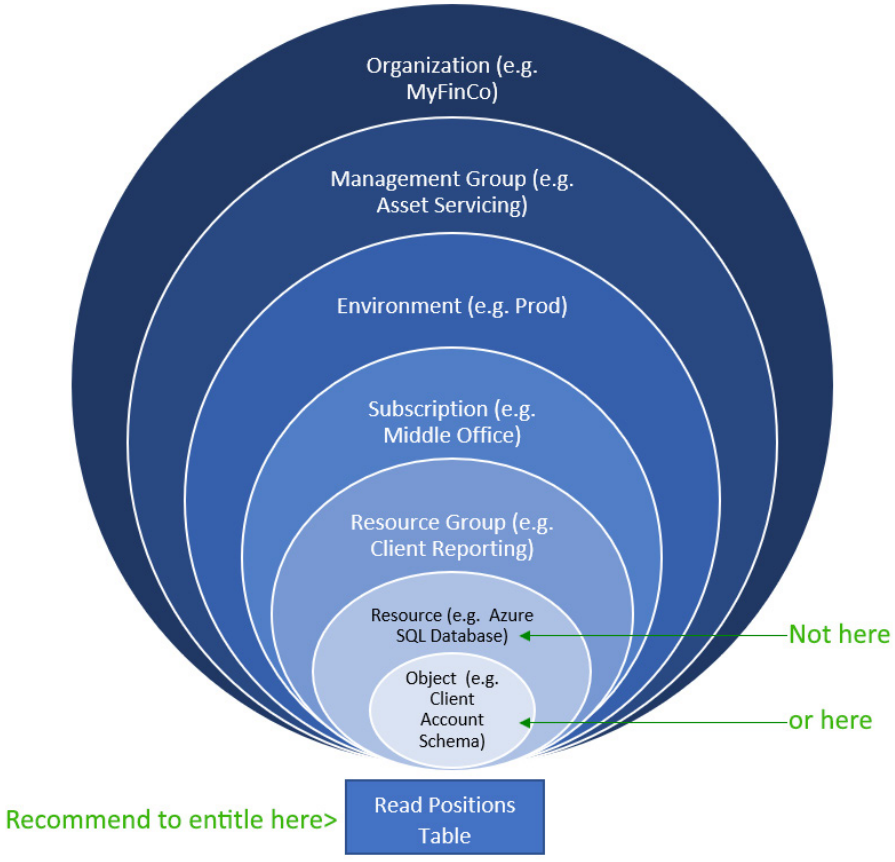


FIGURE 3:CLOUD RESOURCE HIERARCHY

There are significant number of challenges and good practices to help manage policy for access and entitlements for Cloud and on-prem solutions. The table below illustrates high level areas requiring incorporation into your Defense in Depth strategy and implementation.

Topic	Typical Pain Points
Segregation & Least Privilege	• Segmented management of secrets across critical systems deployed in several trusted and untrusted zones, with a variety of environments spanning development, QA, UAT and production • Designing for the principles of least privilege access and zero-trust
Secrets Generation & Distribution	• Acknowledgement and validation of new secrets requests • Applying repeatable and sustainable policies for the generation and maintenance of secrets across all organizational management groups & subscriptions • Support for on-demand secrets generation • Enacting global and granular policies for secret quality
Leasing & Revocation	• Enforcement of granular policies for secrets revocation - whether it be age-out, invalidation/removal, broad expiry/revocation, or termination based on types of users and roles • Management of master keys, one-time passwords, and MFA policies
Security of Secrets	• Enacting appropriate access and management controls for administrators, system users, trusted 3rd party systems and human users • Governance of controls and audit events across vaults • End-to-end encryption of secrets - in transit and at rest • Scanning for plaintext exposure of secrets during processing, development or environment automation/orchestration • Operationalizing the detection, response and recovery to cyber risks
Scaling, High Availability & Redundancy	• Supporting a high frequency of granular access requests for objects for system-to-system transactions and human users • Supporting just-in-time and dynamic secrets generation at scale • Providing both good user and developer experiences
Monitoring & Reporting	• Providing reports for both producers and receivers/users of secrets, their utilization characteristics, and administrative changes performed • Monitoring, alerting and reporting on anomalies and potential threats

FIGURE 4:STRENGTHENING IDENTITY AND ACCESS MANAGEMENT DISCIPLINES

Citihub previously has published a comprehensive paper on **building effective secrets management for the enterprise and cloud**, which is a worthwhile read on the topic covering zero trust, hardening of secrets infrastructure, and continuous monitoring considerations. Considering that Privileged Access abuse is still the predominant initial vector, zero-trust strategies are going to be increasingly critical for Public Cloud assets.

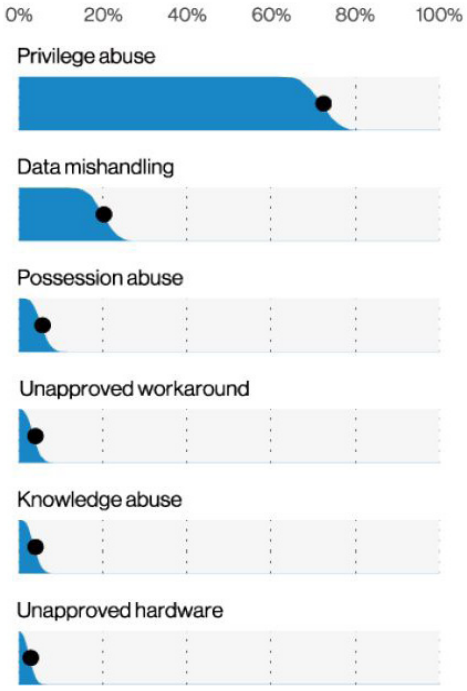


FIGURE 5: **2021 DBIR REPORT** (TRUNCATED) – INITIAL EXPLOIT VECTORS

Cloud Governance

The ability to govern both appropriate use and control of cloud resources is a fundamental pillar of defense in depth. A well thought out cloud governance program would provide a layer of operational pre-requisites and runtime guardrails that are expected of workloads and systems designed to operate in a public cloud environment. Your Policy Management scope criteria should include coverage for:

- Library of approved design blueprints
- "Permission to build" criteria
- "Permission to populate data" criteria
- "Permission to operate" criteria
- A (Cloud + Enterprise) Controls Database, with a baseline per CSP if necessary
- A set of implemented (embedded) and roadmapped (aspirational) cloud provider policy guardrails
- Financial structure and allocation vehicles

Cloud governance guardrails should seek to be embedded as Policy as Code tests that are implemented in Build, Release, and Deploy pipelines:

Build time controls are typically embedded into Static Code Analysis and Code Quality scanning tools that help 'shift left' on potential exposures and policy violations early in the development lifecycle. These could include things like:

- Scanning for OWASP 10 common exploits like SQL injection
- Use of hardcoded secrets (subscription IDs, tokens, etc.)
- Identifying unmanaged 3rd party packages or the use of prohibited package repos

Release controls are typically embedded as part of test automation coverage where test cases against compiled code can be ran pre-deployment. These could include things like:

- Unencrypted data streams
- Dynamic code calls to unauthorized services
- Jailbreaking tests
- Writing/reading to unauthorized or unencrypted persistent data stores

Deployment controls can be embedded in various environment management or orchestration toolsets such as Terraform, Cloud Resource Management tools, and Cloud Formation. These tools can ensure the creation and management of resources follow specific defined policies such as:

- Evaluating the use of public/private endpoints
- Ensuring https encrypted endpoints
- Validating infrastructure with PCI DSS compliant scanning (or suitable infrastructure compliance standard) on target infrastructure pre-deployment
- Validating package or image checksums or other immutability controls
- Validating vulnerability scoring is below acceptable thresholds

Effective cloud governance as it is outlined in the **CIS Cloud Control Companion Guide** and **NIST 800-53r5** will seek to embed as many of these controls into tooling pipelines and automation, relying less and less on human inspection and review which are fundamentally flawed for accuracy, efficiency and speed. While its unlikely that governance and policy automation will reach 100% coverage in any organization, its critical that everyone from senior leadership to development teams understand what is expected, what has been embedded in place, and what requires manual inspection still.

Those organizations that fail to establish competency in Cloud Governance practice will be the most likely to mismanage their resources on the public cloud – whether it be financial mismanagement, or at worst exploitation of services, customers and/or data.

Whether your organization is already in flight or just beginning to build a Cloud Governance structure, Citihub has practical experience in designing, building and sustaining Cloud Governance as enterprises move from small to @scale deployments on multi-cloud environments.

Cloud Operations

Continuous operation of a secure cloud runtime environment requires investment in tooling and analytics aimed at measuring and monitoring security posture across subscriptions, environments, applications, resources and identities. Most cloud providers provide their own Cloud Security Posture Management tools (CSPM) but most large enterprises will find them inadequate as standalone solutions. Careful consideration should be made to select and implement the best of breed products (for example tools like Prisma, Dome9, Fugue, and/or custom in-house tooling to covering gaps on multi-cloud environments). It's important to understand that current maturity across CSPM offerings will bring large-scale organizations to the realization that there is no clear single winner in this space – a mature implementation will involve the use of one or more commercial products *and* customized in-house analytics, security monitoring and reporting.

Some example use cases to consider for Cloud Controls Monitoring and Assurance:

- Audit trails and variance reporting for management groups, identities, access management, or resource security settings
- VPC traffic monitors
- Outbound/inbound traffic monitors for data buckets
- Object-level access reporting for critical data stores
- Account and Resource Inventory reporting
- Anomaly reporting on compute and data usage
- Step up MFA authentication requests / failed requests
- Identification of unencrypted endpoints
- Identification of publicly accessible endpoints
- Identification of non-compliant / unapproved resource creation
- Validating backup policy configurations against critical data stores (duration and frequency)
- Validating centralization of application log artifacts to a centralized collection and analysis tools
- Validation of audit and error logs across resources
- Under-and-over utilized resources
- Financial reporting and exception monitoring

Because many of the use cases required for adequate Identification of Cyber Risk will not come from commercial out-of-the-box software and services, many organizations will find the need to build custom monitoring and analytics to supplement whatever existing capabilities they have today.

Given the separation of responsibilities well documented by the Shared Responsibility Model, Citihub strongly advocates for regulated businesses to invest in proactive testing and probing of the provider's cloud controls to test the efficacy of the expected controls as configured and to test the underlying cloud service provider's implementation is working. As we have seen provider-driven issues such as DNS failures, storage system outages, storage bucket access control failures, Cloud web API service / fuzzing exploits, and Identity service failures its necessary for highly regulated and systemically important institutions to implement behavioral testing probes so that a layer of monitoring and assurance can be applied to provider-driven controls ensuring that what is configured is working as expected.

Probe-style monitoring use case examples to consider are:

- Attempted creation of non-compliant resources (e.g. unencrypted storage buckets)
- Attempted privileged access by non-privileged user
- Attempted access of a private URL via a public route
- Attempted access of an https endpoint using http protocol
- Attempted access of an unauthorized object
- Attempted access of an unauthorized subscription
- Periodic service calls to provider infrastructure APIs – for both positive outcomes and expected negative outcomes
- Periodic functional testing of resource creation / destruction

Building defense in depth will require ultimately the combination of inline testing and control and out of band 'behavioral testing' to ensure controls are working as designed, and test for both expected positive and negative outcomes. This approach is ultimately necessary to ensure that an existing, on-prem defense in depth strategy can be applied and ported to public cloud infrastructures.

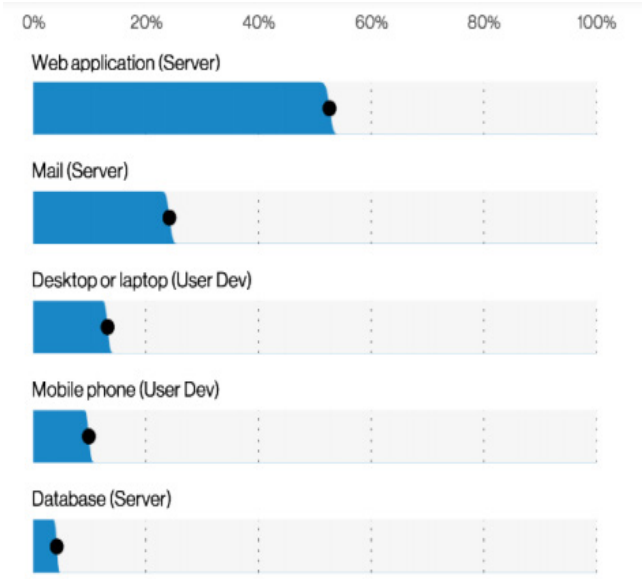


FIGURE 6: 2021 DBIR REPORT (TRUNCATED) – SYSTEMS TARGETED FOR EXPLOITS

If we look at the DBIR report for the types of systems compromised, the top targets are web applications and e-mail systems – so prioritizing Interactive and Dynamic test coverage and linting of those services for exposures remains a priority area.

Citihub Digital provides an open-source compliance probing toolkit called Probr on Github to demonstrate one such approach to building functional testing probes that operate out of band from existing vendor and commercial CSPM tools. These types of tools accelerate engagements and can be used as a mix of out-of-the-box implementations or for building net new test cases.

Citihub Digital has previously written a **whitepaper on Compliance as Code**, which goes further into approaches to building Continuous Compliance in Public Cloud. Our firm has experience designing and implementing across all of these layers of governance and control, working with global financial institutions to ensure the operation of their critical lines of business can comply with internal controls & best practices, global regulators, and the evolving landscape of foreign and domestic cyber threats. We help enterprises build and execute concrete strategies and adoption plans for cloud adoption - understanding that one size does not fit all.

Conclusion

The voracious appetite to transition large portions of IT infrastructure from on-premises to public cloud solutions when juxtaposed with the marked increase in frequency, sophistication and the deep impacts of cyber exploits presents a perfect storm for senior leadership of the enterprise. Whilst most large enterprises have taken small, calculated and experimental steps towards bringing their lines of business onto public cloud infrastructure, there is an increasing pressure to demonstrate more value out of their cloud programs – meaning tangible improvements to agility, time to market and the business return on investment. Organizational IT leaders are increasingly feeling the pressure to drive more aggressive adoption strategies, and to think larger than canary and experimental deployments.

Aligning the Cloud Adoption strategy with a layered Defense in Depth strategy will require deeper planning of the Organizational model and re-mapping of IT services to newer, cloud distributed service models and architectures. It is not enough to simply port conventional understanding to a new hybrid operating model – innovation in people, process and tooling to keep pace with cyber threats and exposures is necessary to avoid catastrophic breaches, including:

- Building cloud subscriptions and landing zone architecture that represents front-to-back Lines of Business
- Stricter access, identity and secrets management policies and enforcement, aimed towards zero trust in the most vulnerable perimeters
- Stronger governance, transparency and realtime monitoring of existing enterprise & cloud control efficacy
- Improved and enforced definitions of minimum Operational Quality, with distinct guardrails for deployment, management, and transport of data
- Comprehensive realtime cloud control monitoring to ensure the accuracy of cloud tenant configuration and expected behaviors of provider controls
- Positive and negative behavioral testing to ensure expected results from cloud provider control planes

Citihub strongly advises that enterprises strongly define and automate large portions of their existing IT Operational Quality and Compliance Controls monitoring to reduce both exposure surface area and time to identification of a breach. In the face of a persistent and growing threat of domestic and international organized crime in the cyberspace, building realtime monitoring and analytics across LOB systems that are operating in fully public and/or hybrid operating models is necessary. For those enterprises that have already established good compliance automation and quality controls internally its really a continuation of leveraging that same framework as more of a presence on public cloud is established...and for those enterprises that have not invested to that degree for their on-premises applications and infrastructure – now is a critical time to raise the organizational priorities around essential capabilities for building Defense in Depth for Public and Hybrid Cloud.

About Citihub Digital

Recoding the Digital DNA of Financial Services

Citihub Consulting is a global, independent IT advisory firm with deep domain expertise across every layer of the technology stack - from business applications and platforms down to core infrastructure. Our consultants have decades of experience helping clients promote best practice in every IT discipline.

Our Heritage: Depth in Financial Services IT

Citihub Consulting understands financial services. Our consulting teams are expert at bridging business and technology to drive digital transformation, comply with complex regulation, and secure critical systems and information.

Bridging Silos: Driving the Modernisation of IT

IT modernisation demands the ability to bridge diverse functions and technical disciplines as DevOps, Cloud, modern application architectures and cyber security blur historical organisational boundaries. Citihub Consulting's consultants span the full technology stack and can act as catalysts to maximise the value of clients' own specialists.

Success: Enduring Client Relationships

Client success is our success. That's why our clients stay with us (we've had year-on-year relationships with our top 15 clients for an average of 8 years). We're focused on building lasting relationships and clients rely on us to honour our commitments whilst giving them confidence that their most challenging goals can be achieved.

© 2021 citihub digital