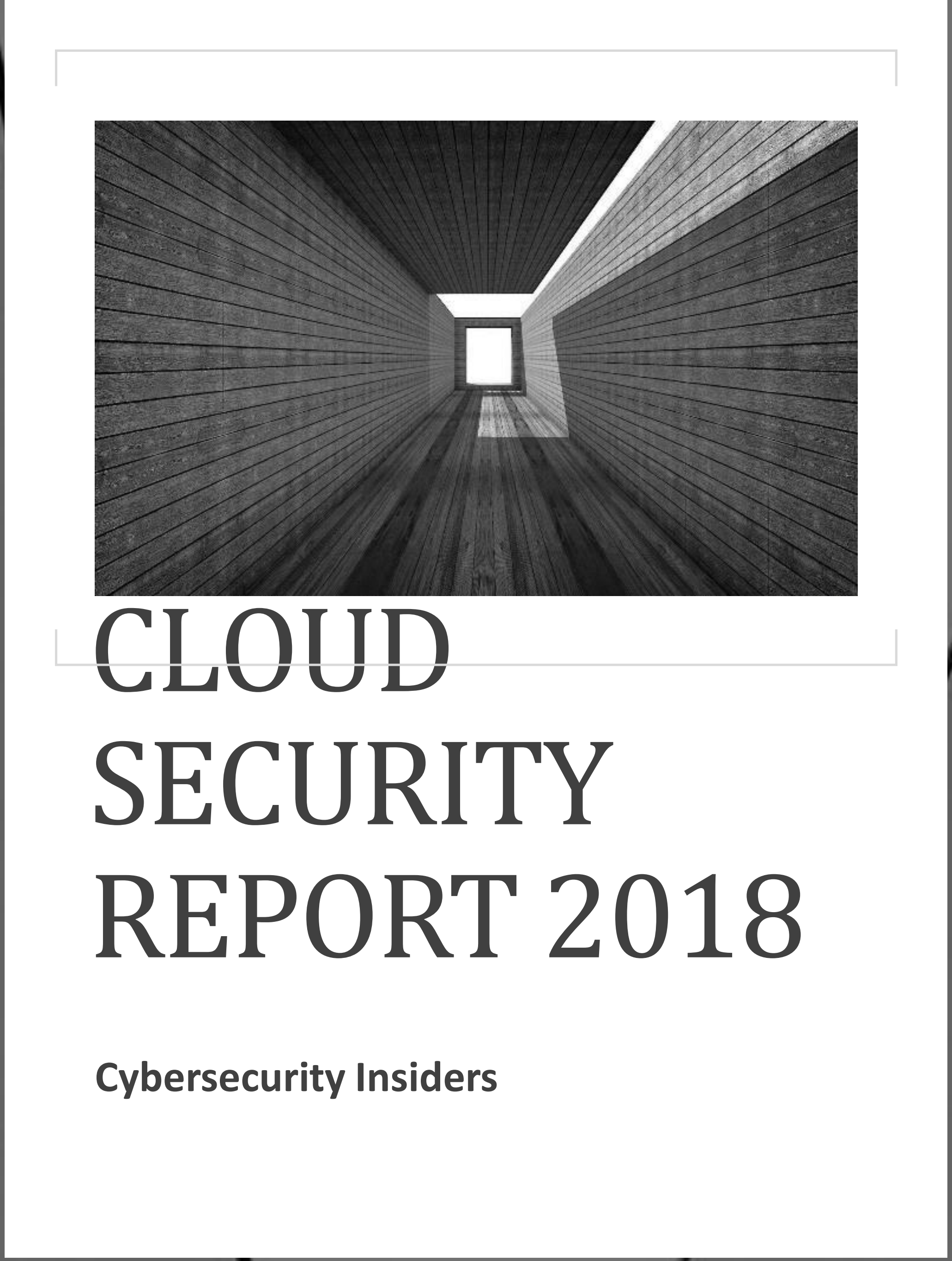
Cloud
Security, Threat & Privacy

Dr. Syed Imtiyaz Hassan
Assistant Professor, Deptt. of CSE,
Jamia Hamdard
(Deemed to be University),
New Delhi, India.
https://syedimtiyazhassan.org
s.imtiyaz@jamiahamdard.ac.in



CLOUD SECURITY REPORT 2018

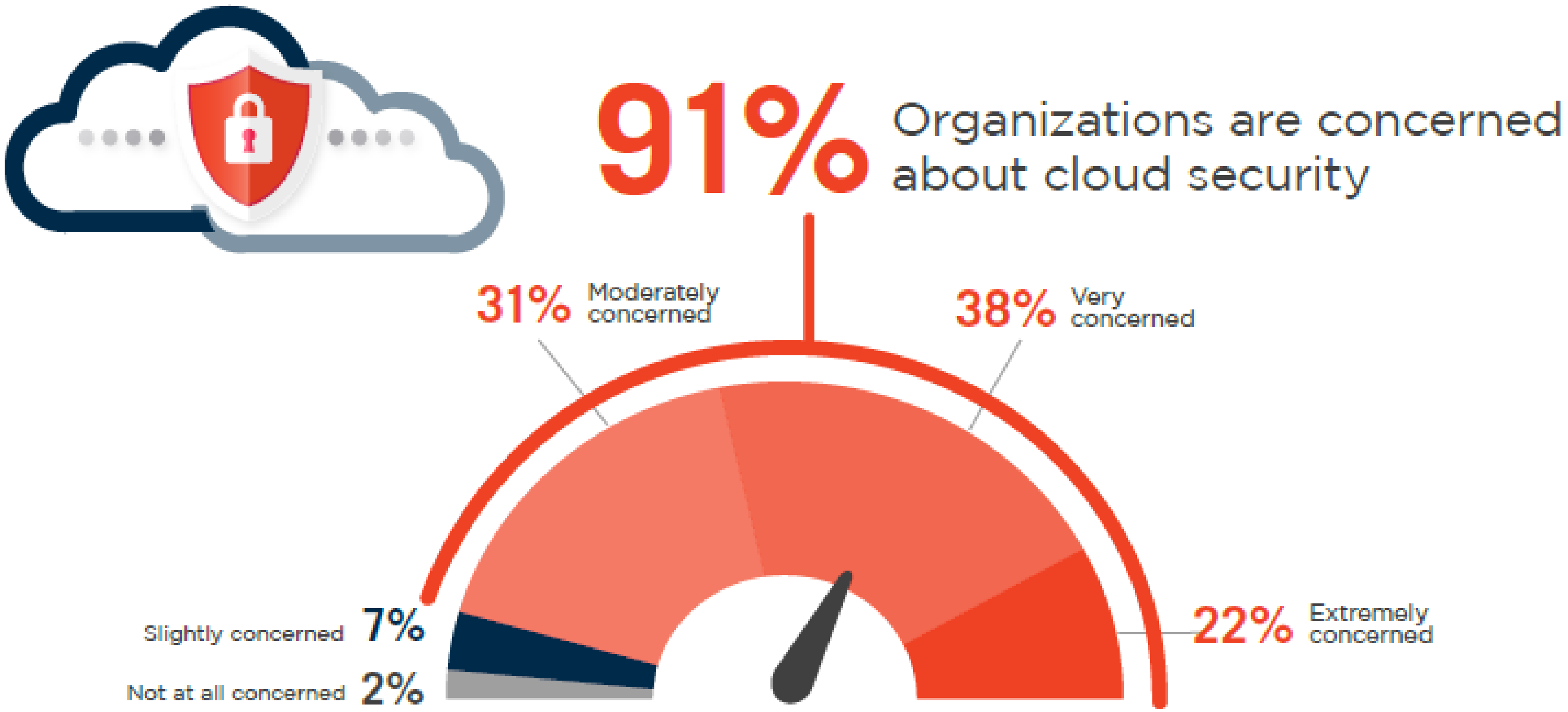
Cybersecurity Insiders

Produced by

- 400,000 member Information Security Community on LinkedIn
- In partnership with Cybersecurity Insiders
- Available Online: https://pages.cloudpassage.com/rs/857-FXQ-213/images/2018-Cloud-Security-Report%20%281%29.pdf

CLOUD SECURITY REPORT 2018 (Cybersecurity Insiders)

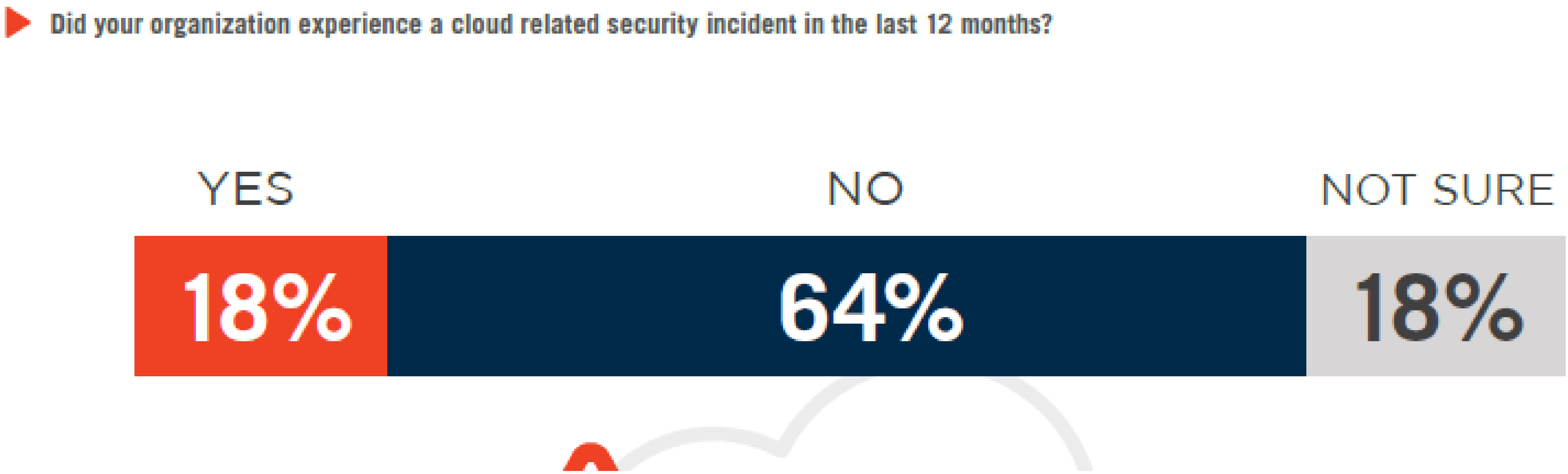
Please rate your level of overall security concern related to adopting public cloud computing.



91% Organizations are concerned about cloud security

https://pages.cloudpassage.com/rs/857-FXQ-213/images/2018-Cloud-Security-Report%20%281%29.pdf

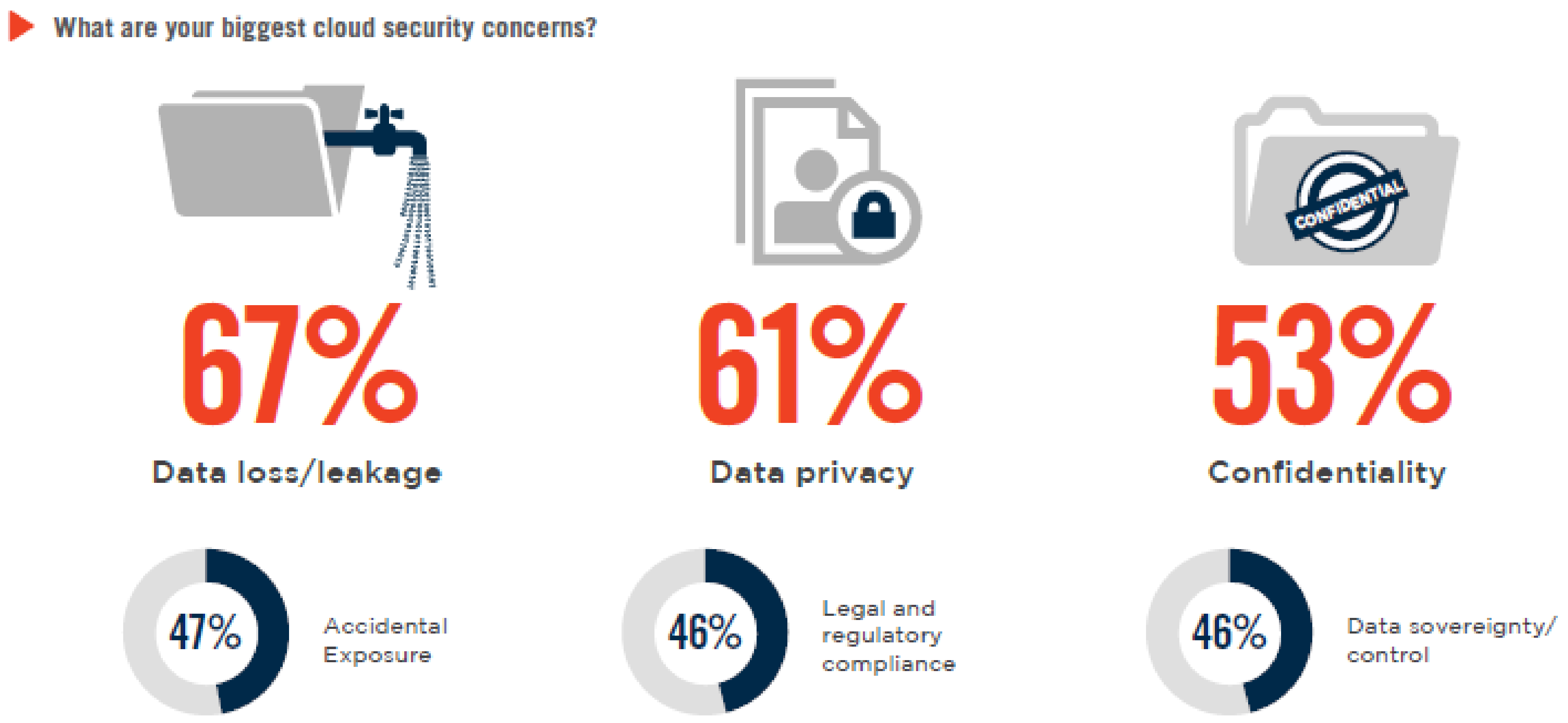
CLOUD SECURITY REPORT 2018 (Cybersecurity Insiders)



Did your organization experience a cloud related security incident in the last 12 months?

https://pages.cloudpassage.com/rs/857-FXQ-213/images/2018-Cloud-Security-Report%20%281%29.pdf

CLOUD SECURITY REPORT 2018 (Cybersecurity Insiders)



What are your biggest cloud security concerns?

67% Data loss/leakage

61% Data privacy

53% Confidentiality

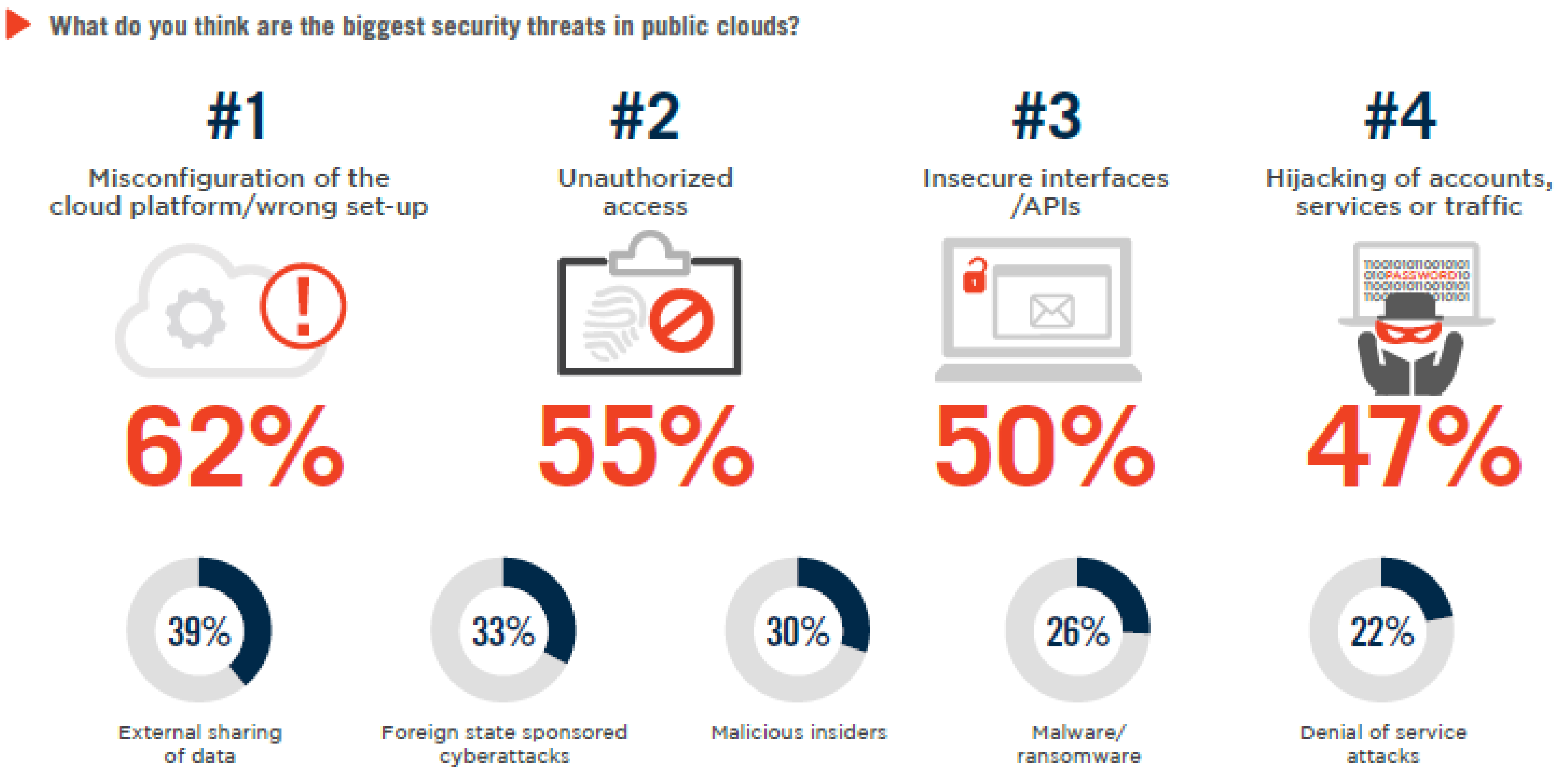
47% Accidental Exposure

46% Legal and regulatory compliance

46% Data sovereignty/ control

https://pages.cloudpassage.com/rs/857-FXQ-213/images/2018-Cloud-Security-Report%20%281%29.pdf

CLOUD SECURITY REPORT 2018 (Cybersecurity Insiders)



What do you think are the biggest security threats in public clouds?

#1
Misconfiguration of the cloud platform/wrong set-up
62%

#2
Unauthorized access
55%

#3
Insecure interfaces /APIs
50%

#4
Hijacking of accounts, services or traffic
47%

39% External sharing of data

33% Foreign state sponsored cyberattacks

30% Malicious insiders

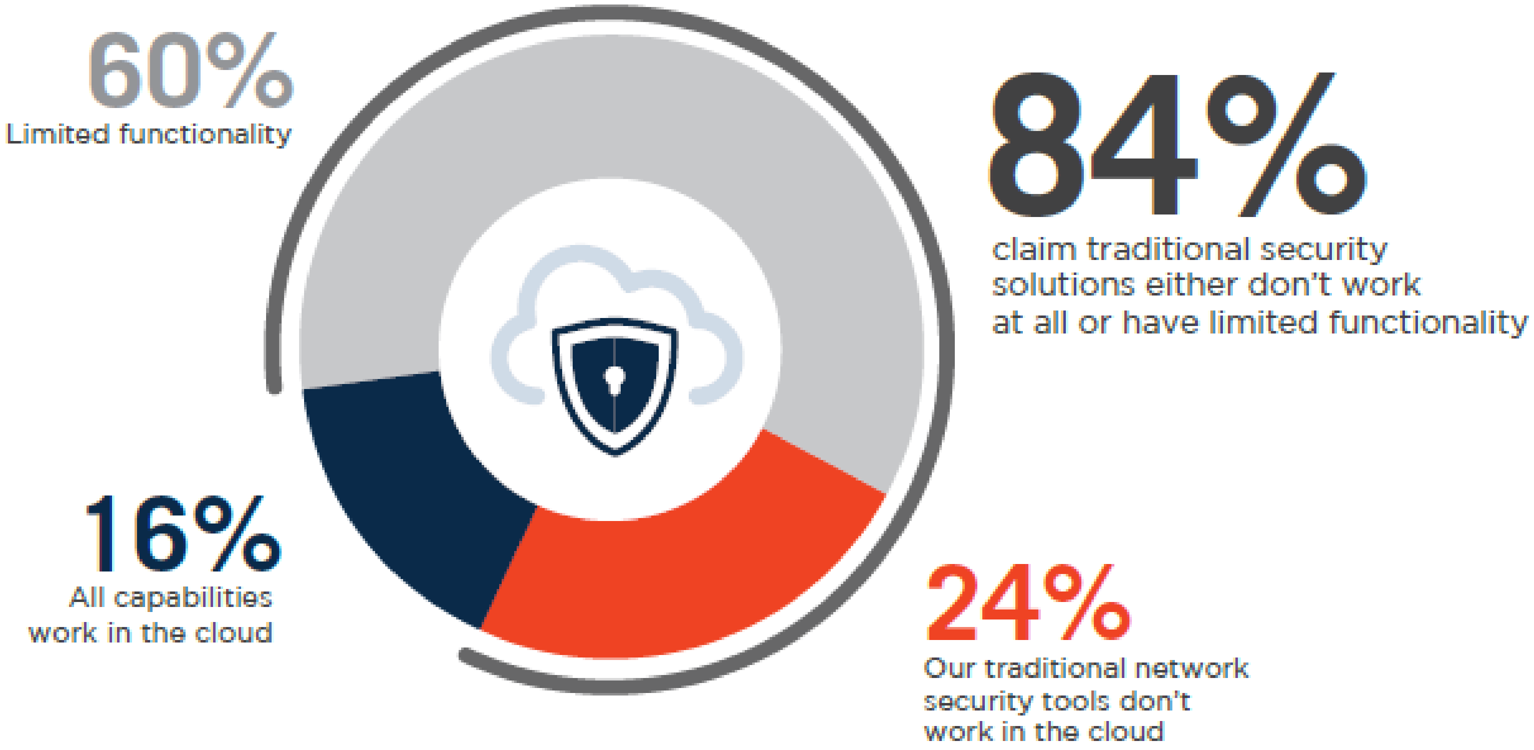
26% Malware/ ransomware

22% Denial of service attacks

https://pages.cloudpassage.com/rs/857-FXQ-213/images/2018-Cloud-Security-Report%20%281%29.pdf

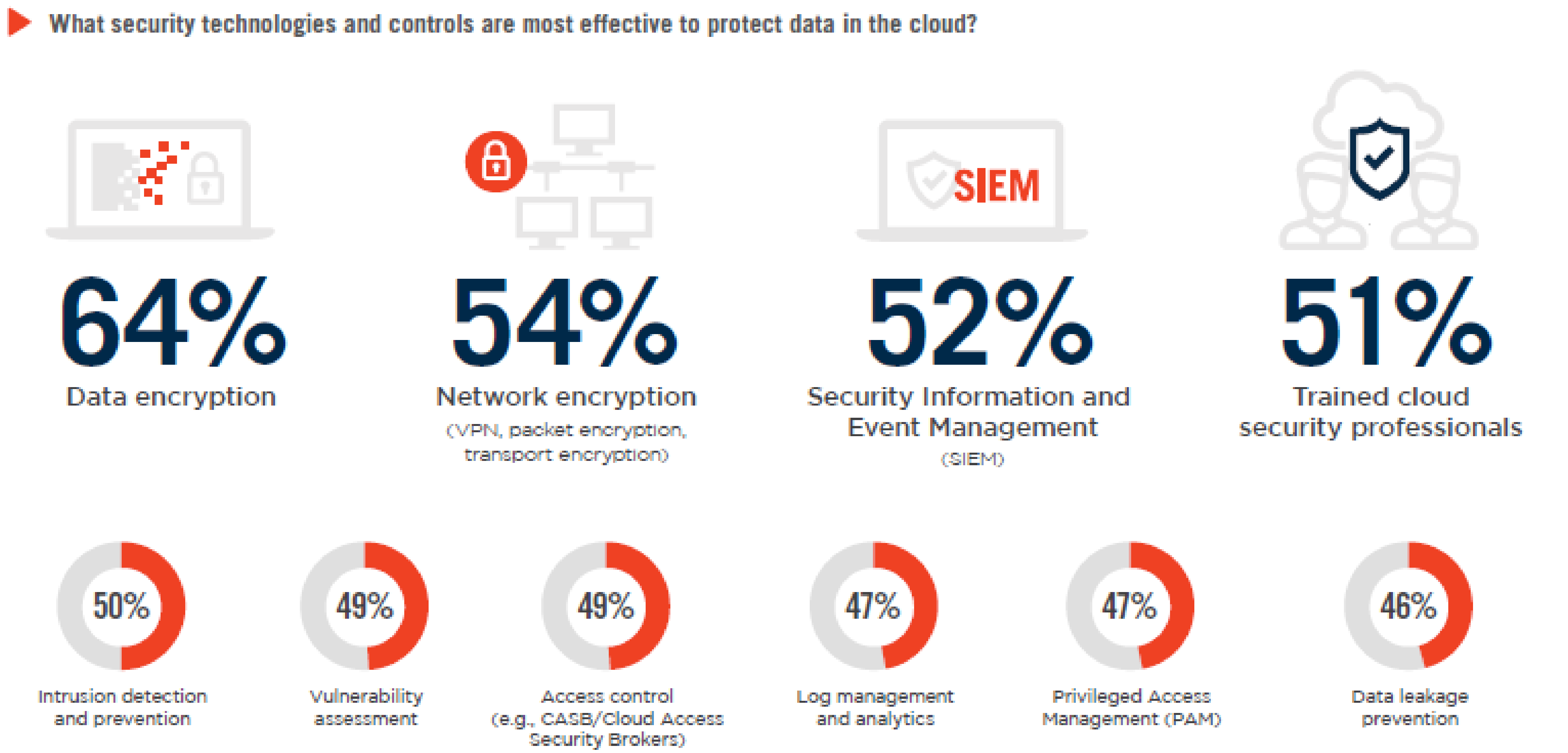
CLOUD SECURITY REPORT 2018 (Cybersecurity Insiders)

How well do your traditional network security tools/appliances work in cloud environments?



https://pages.cloudpassage.com/rs/857-FXQ-213/images/2018-Cloud-Security-Report%20%281%29.pdf

CLOUD SECURITY REPORT 2018 (Cybersecurity Insiders)



What security technologies and controls are most effective to protect data in the cloud?

64% Data encryption

54% Network encryption (VPN, packet encryption, transport encryption)

52% Security Information and Event Management (SIEM)

51% Trained cloud security professionals

50% Intrusion detection and prevention

49% Vulnerability assessment

49% Access control (e.g., CASB/Cloud Access Security Brokers)

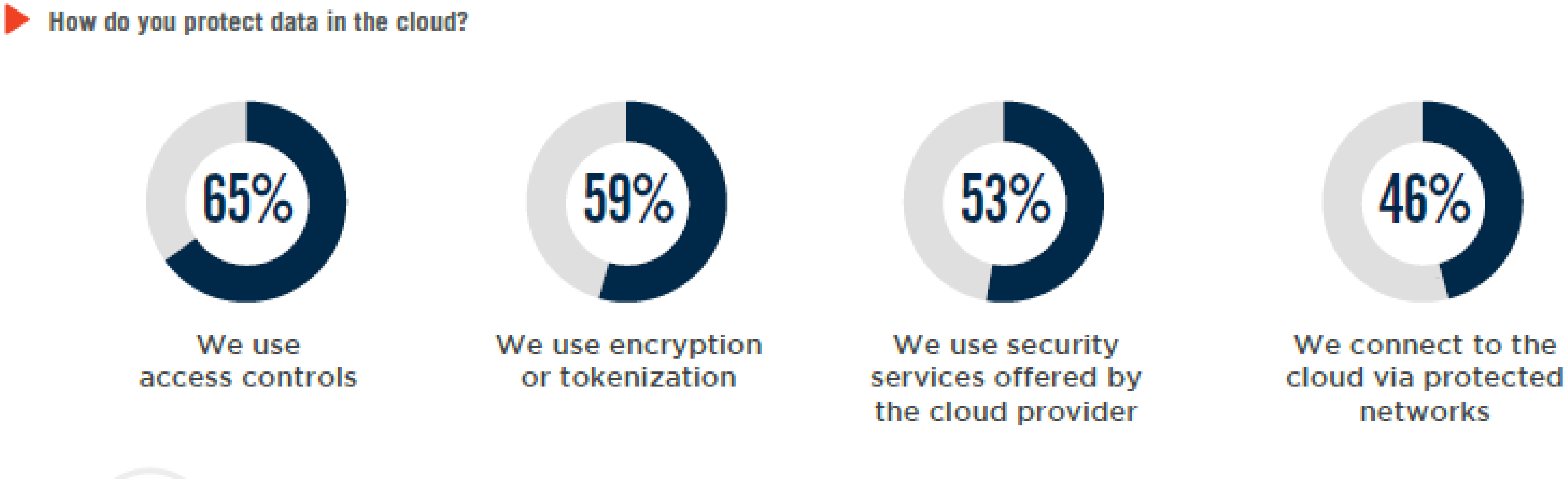
47% Log management and analytics

47% Privileged Access Management (PAM)

46% Data leakage prevention

https://pages.cloudpassage.com/rs/857-FXQ-213/images/2018-Cloud-Security-Report%20%281%29.pdf

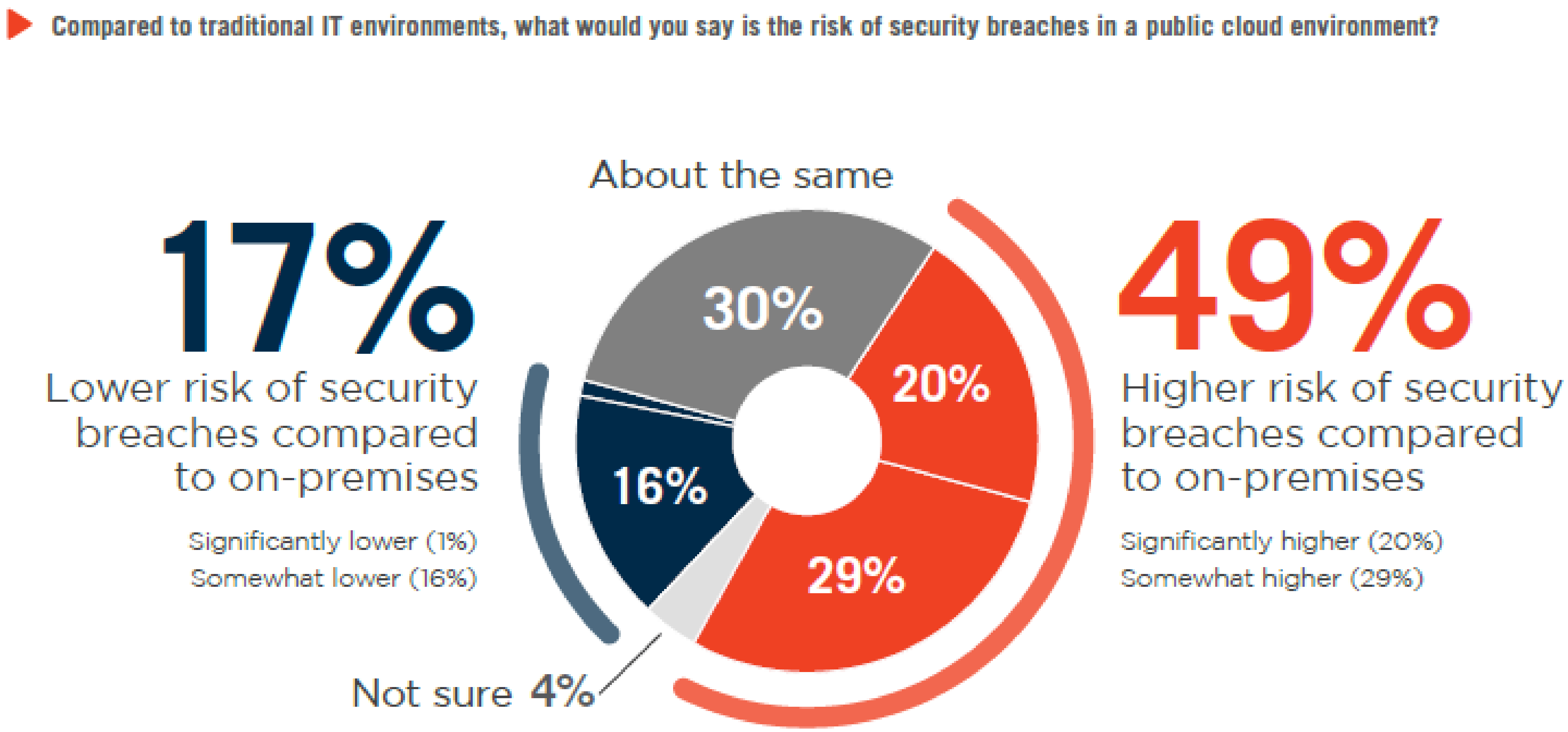
CLOUD SECURITY REPORT 2018 (Cybersecurity Insiders)



How do you protect data in the cloud?

https://pages.cloudpassage.com/rs/857-FXQ-213/images/2018-Cloud-Security-Report%20%281%29.pdf

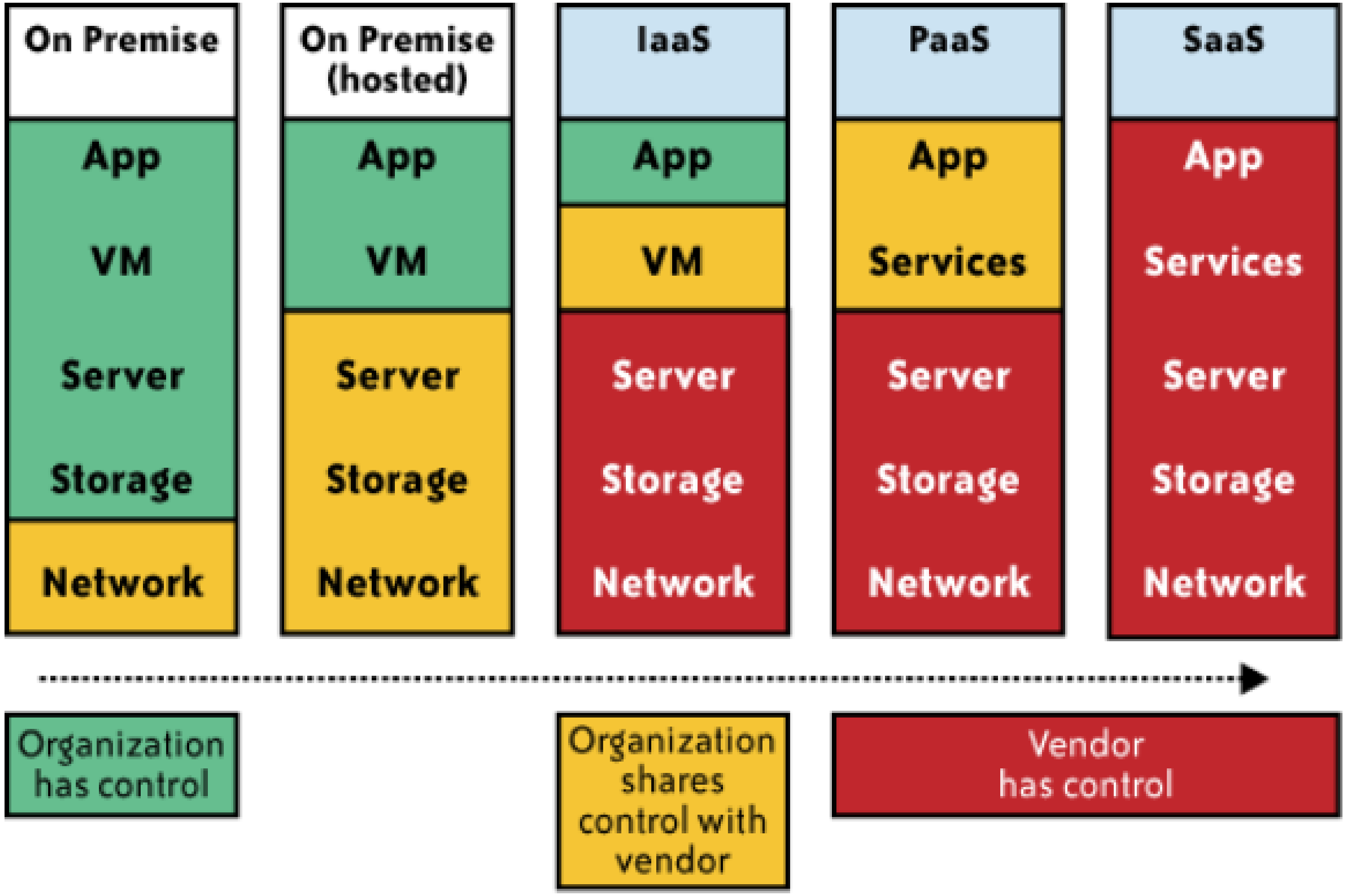
CLOUD SECURITY REPORT 2018 (Cybersecurity Insiders)



Compared to traditional IT environments, what would you say is the risk of security breaches in a public cloud environment?

https://pages.cloudpassage.com/rs/857-FXQ-213/images/2018-Cloud-Security-Report%20%281%29.pdf

Traditional IT infrastructure and Cloud Security



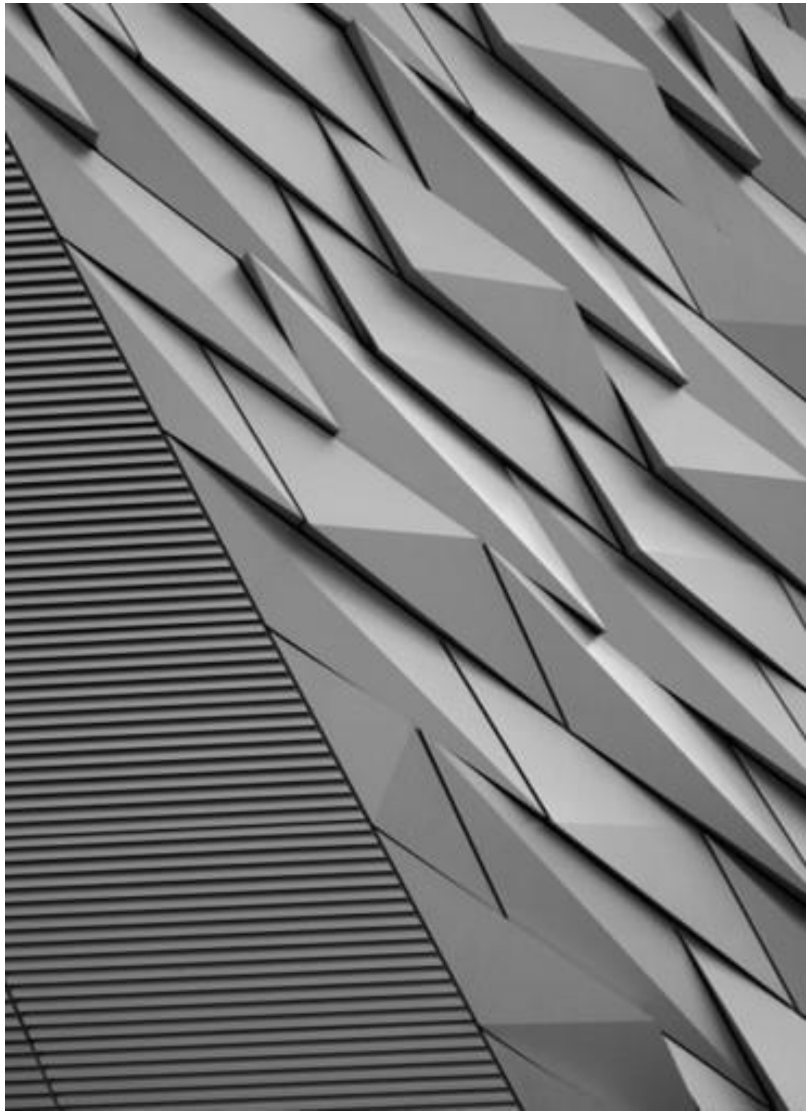
On Premise	On Premise (hosted)	IaaS	PaaS	SaaS
🟩 App	🟩 App	🟩 App	🟨 App	🟥 App
🟩 VM	🟩 VM	🟨 VM	🟨 Services	🟥 Services
🟩 Server	🟨 Server	🟥 Server	🟥 Server	🟥 Server
🟩 Storage	🟨 Storage	🟥 Storage	🟥 Storage	🟥 Storage
🟨 Network	🟨 Network	🟥 Network	🟥 Network	🟥 Network

🟩 Organization has control

🟨 Organization shares control with vendor

🟥 Vendor has control

Cloud Security Reasons



Most security problems stem from:

- Loss of control
- Multi-tenancy

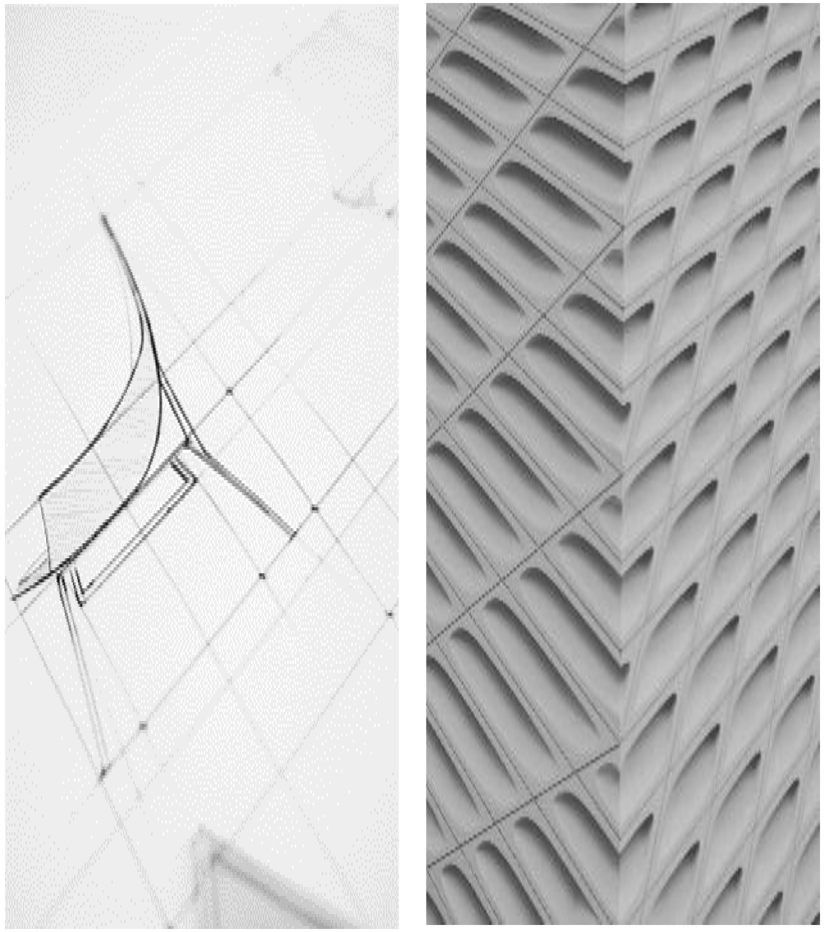
Threat, Vulnerability, and Risk

- **Threats** refer to circumstances or events with the potential to cause harm by way of their outcome. A threat is **what we're trying to protect against**.

- **Vulnerabilities** simply refer to weaknesses in a system. Vulnerabilities make threats possible.

- **Risk** refers the potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability.

- Risk = Threat probability x Potential loss

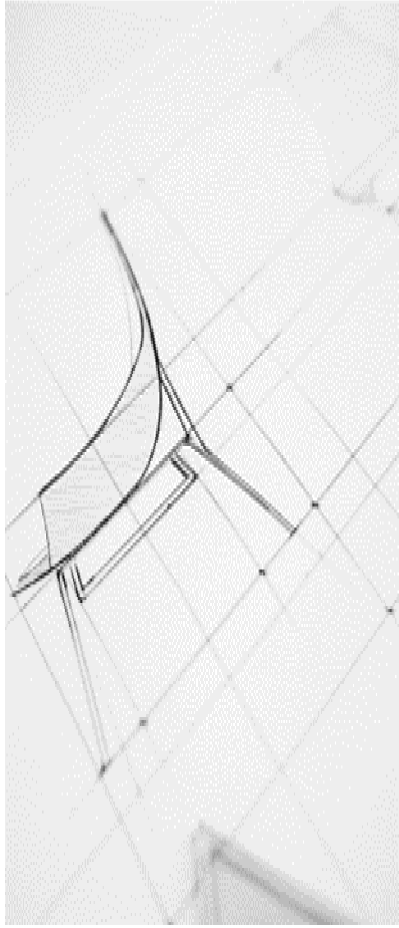


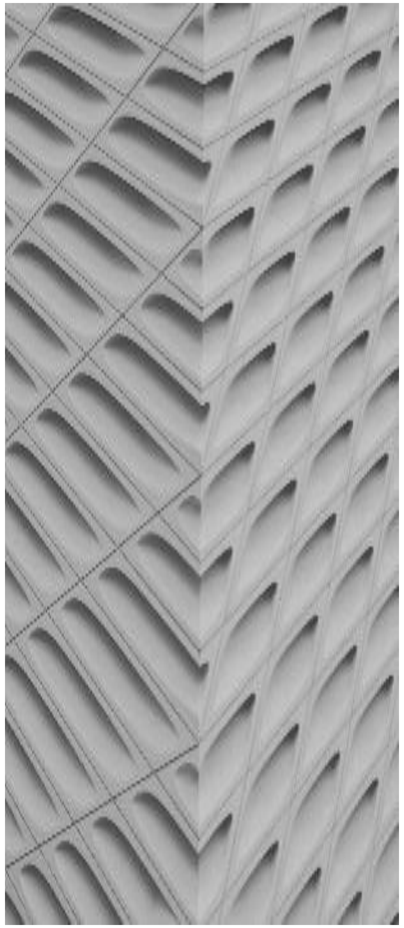
Security

- Measures that are taken to **protect** a place, or to ensure that only people with permission enter it or leave it. *(Collins)*

- The state of being **free** from danger or **threat**.

- A **feeling** of security is a feeling of being safe and free from worry.



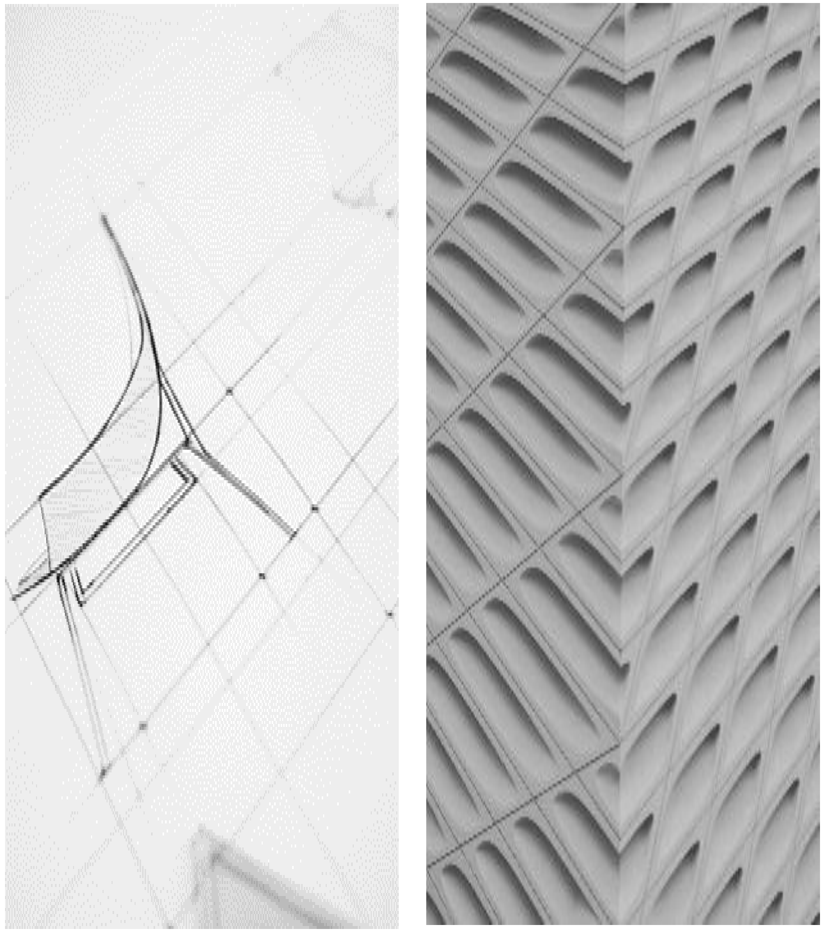


Threat to Cloud Security

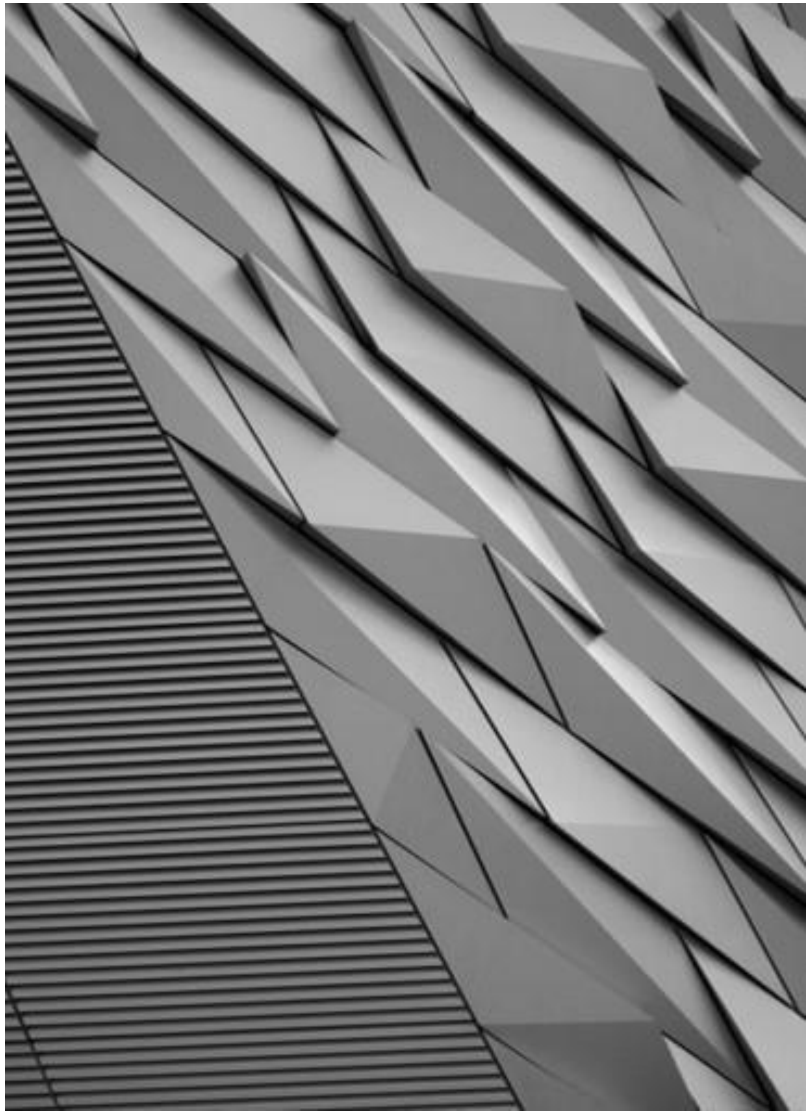
- Threat to Infrastructure
  - *Application Level*
  - *Host Level*
  - *Network Level*

- Threat to Information

- Threat to Access Control



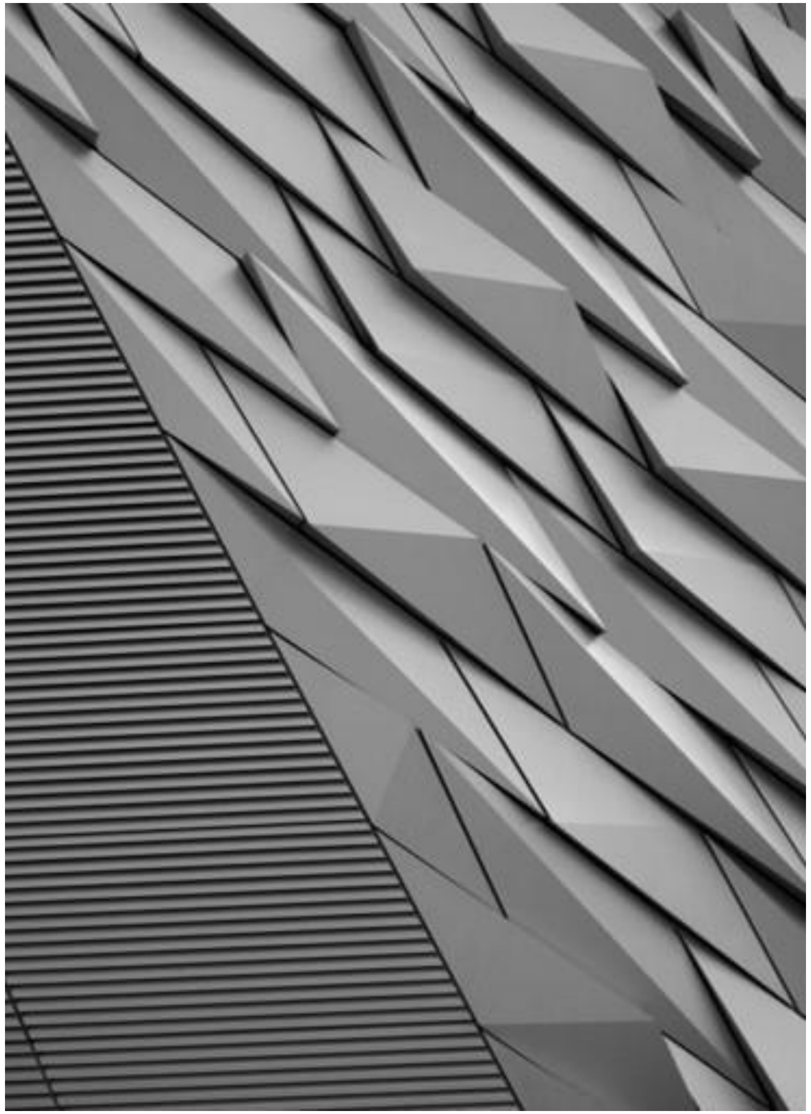
Application Level



- Cloud malware injection
  - A **malicious virtual machine** or a **service implementation** is injected.
  - **Solution**: Perform the **integrity check** to the **service** instance.

- Cookie poisoning
  - An **unauthorized access** is made into the application by modifying the contents of the cookie.
  - **Solution**: **Clean up** the cookie or **encrypt** the **cookie** data.

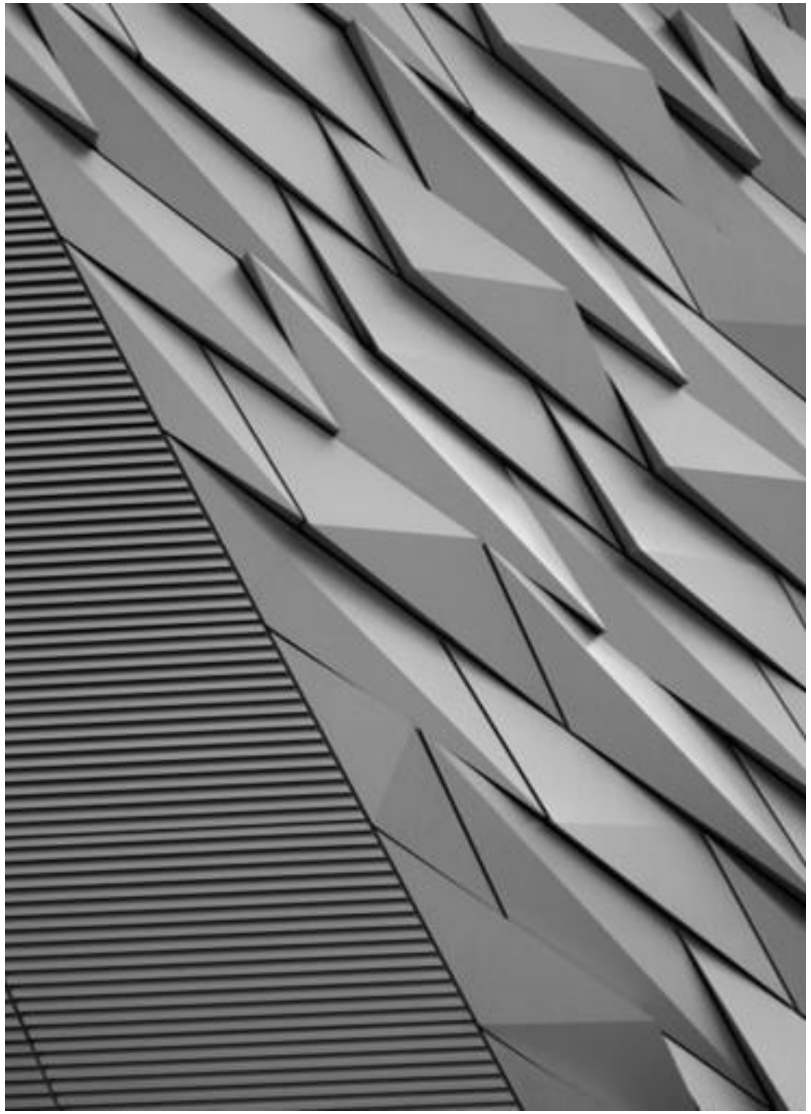
Application Level



- Backdoor and Debug Option
  - Debug option provides back entry for the developers.
  - If **left enabled** unnoticed, may provide easy **access to the hackers** and allow them to make changes in the website.

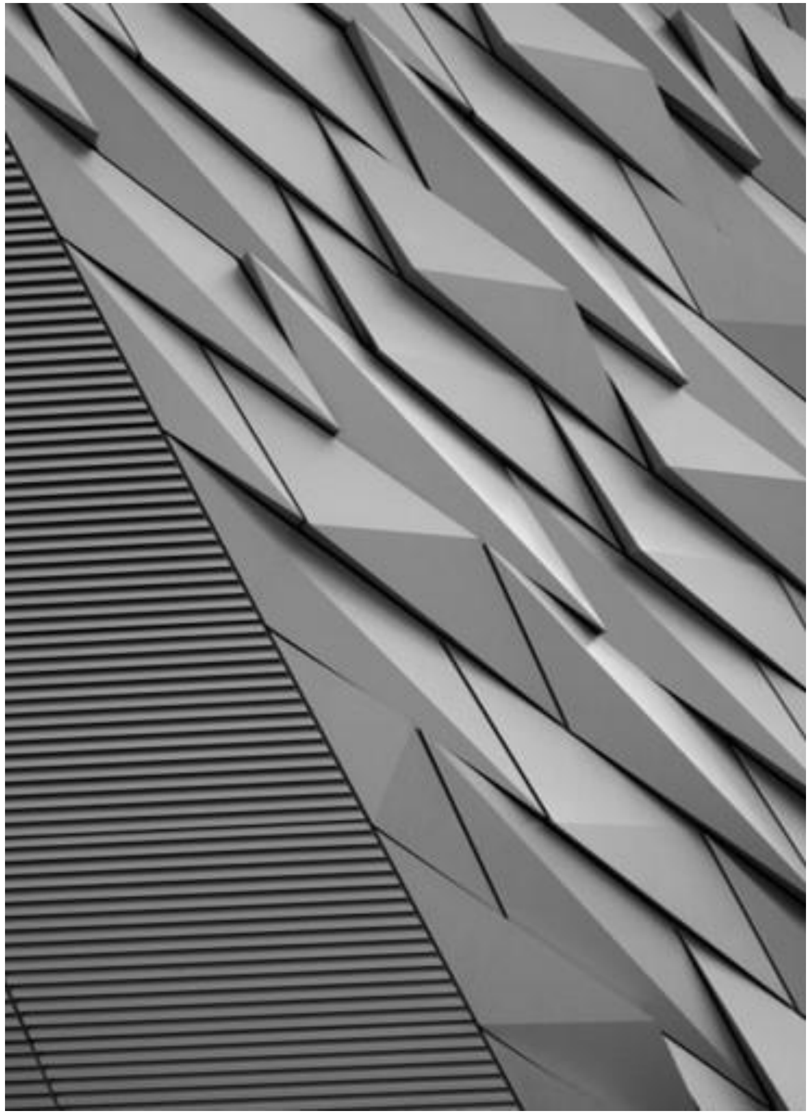
- Hidden Field Manipulation
  - Certain fields are hidden in the web-site and is used by the developers.
  - Hacker can easily modify on the web page.
- SQL Injection
  - Inserting a malicious code into a standard SQL code

Host Level



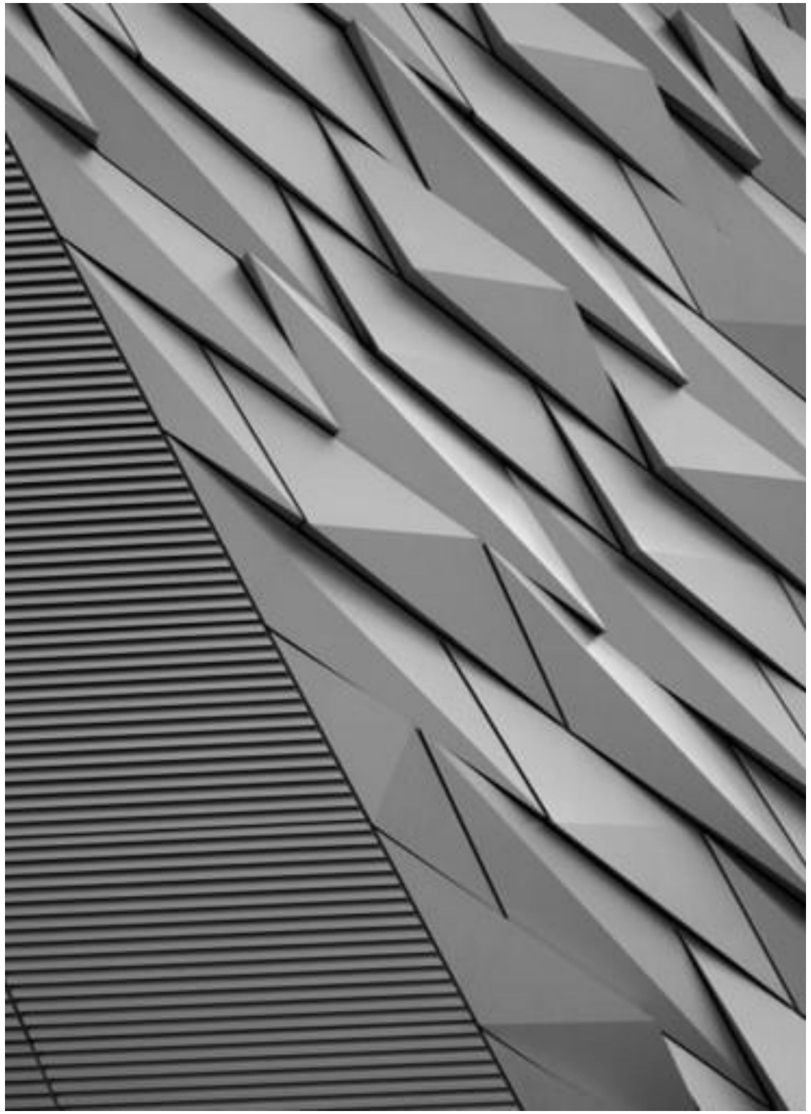
- Virtualization software security
- Customer guest OS or virtual server security
- Security threats:
  - **Stealing keys** used to access and manage hosts
  - **Attacking unpatched**, vulnerable services listening on standard ports (e.g., FTP, NetBIOS, SSH)
  - **Hijacking accounts** that are not properly secured
  - **Attacking systems** that are not properly secured by host firewalls
  - **Deploying Trojans** embedded in the software component in the VM or within the VM image (the OS) itself

Network Level



- DNS: Sender and a receiver get rerouted through some evil connection.
  - Domain hijacking
  - Cross site scripting
- Eavesdropping
  - Attacker monitor network traffic in transit then interprets all unprotected data.
- Denial-of-service (DOS)
  - Overflows a server with frequent request of services to damage the network.
  - Server could not serve client regular requests.

Network Level



- Network Sniffing
  - As data flows across the network, the sniffer **captures each packet** and, if necessary, decode the packet's raw data.
- Man-in-the-Middle
  - A type of eavesdropping attack.
  - A malicious actor inserts himself as a relay/proxy into a communication session between people or systems.

Threat to Information

- Confidentiality
  - Is the property that data contents are **not** made available or **disclosed** to **illegal users**.
- Integrity
  - Demands maintaining and assuring the **accuracy** and **completeness** of data.
- Availability
  - Refers to **remain accessible at all times**.

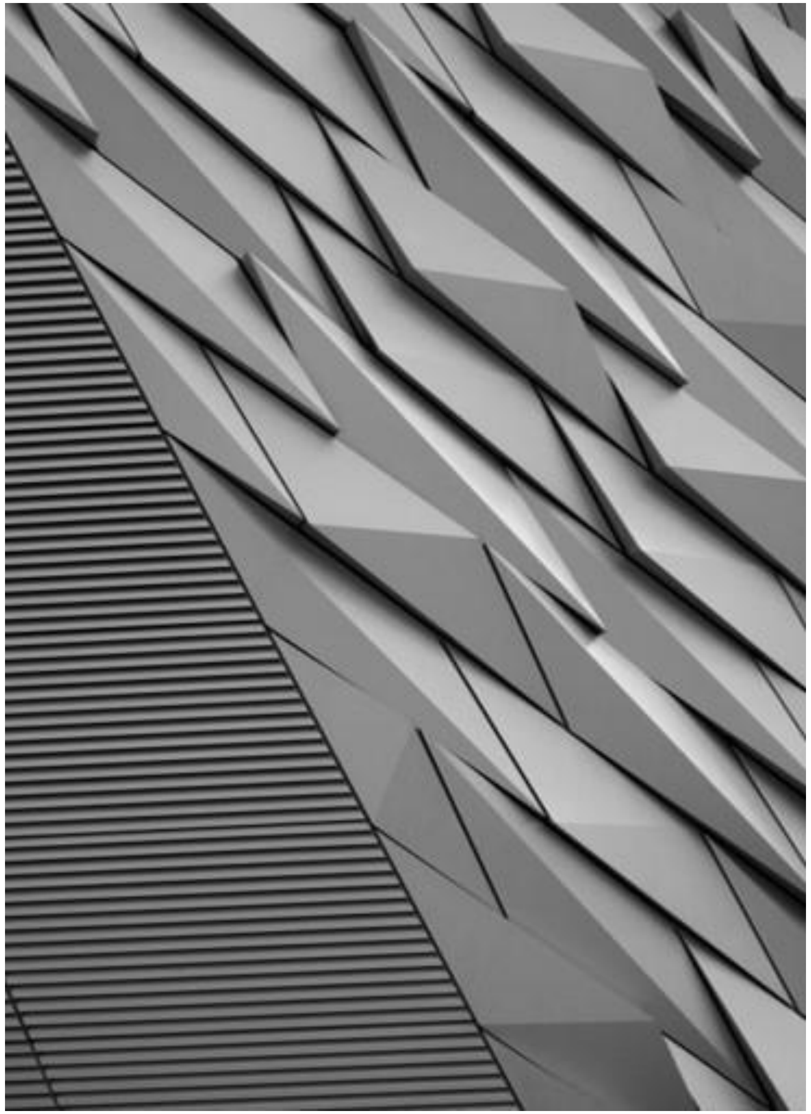
Threat to Access Control

- Identity, Authenticity & Authorization
  - **Identity management** is the organizational process for identifying, authenticating and authorizing individuals or groups of people to **have access** to applications, systems or networks by associating user **rights and restrictions** with established identities.
  - Single Sign-on or Federated Identity Management

Threat to Access Control

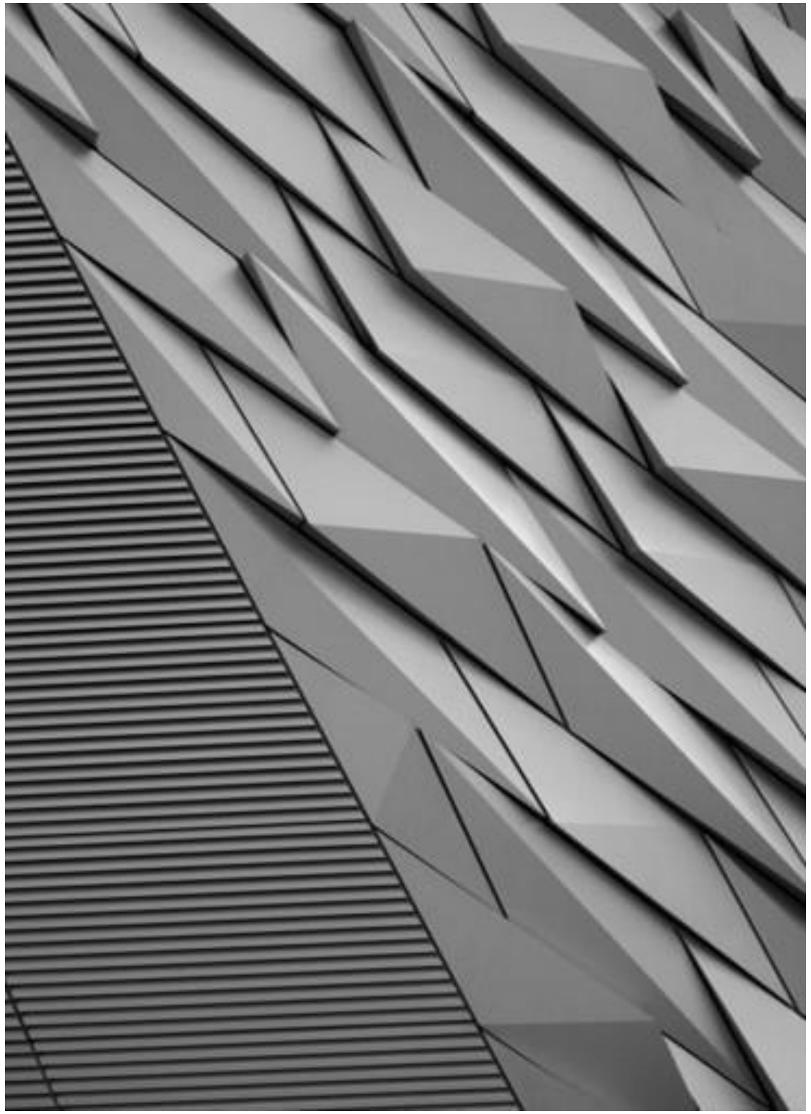
- Non-repudiation
  - Nonrepudiation refers to the ability to ensure that a party to a contract or a communication **cannot deny the authenticity** of their signature on a document or the sending of a message that they originated.

Privacy



- Privacy is the ability of an individual or group to **seclude** themselves or information about themselves and thereby **reveal** them **selectively**.

Cloud GRC



- Cloud Governance Risk management and Compliance
  - **GRC** (governance, risk management, and compliance) refers to a capability that **helps an organization** achieve its objectives, with responsibility running right across the organization.
  - GRC is a **set of processes and practices** that runs across departments and functions.
  - GRC might be enabled by a dedicated platform and other **tools**, although this is not mandatory.

Thank You