# Cloud Computing

# Course plan

Learning session 4

Security

Identity and Access Management (IAM)

# Security

It is easy to spin up a new perfectly configured resource in cloud

And it is the same easy to spin up a vulnerable

# Security lesson plan

- Breach scenarios
- What is security in “cloud”
- Security areas
- Security levels: infrastructure, application, data, user
- Case studies:
  - Public Key Infrastructure (PKI)
  - Secrets management
  - Configuration management
  - Disaster recovery
  - Custom policies
  - Expect security services to fail

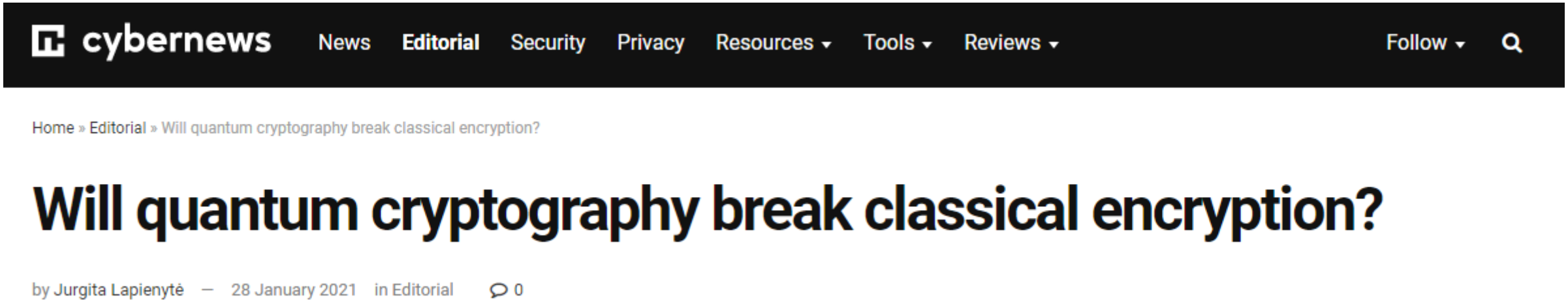
# Breach scenarios

**Ransomware**: threat to publish data or blocks access


https://www.theverge.com/2020/8/4/21353842/garmin-ransomware-attack-wearables-wastedlocker-evil-corp

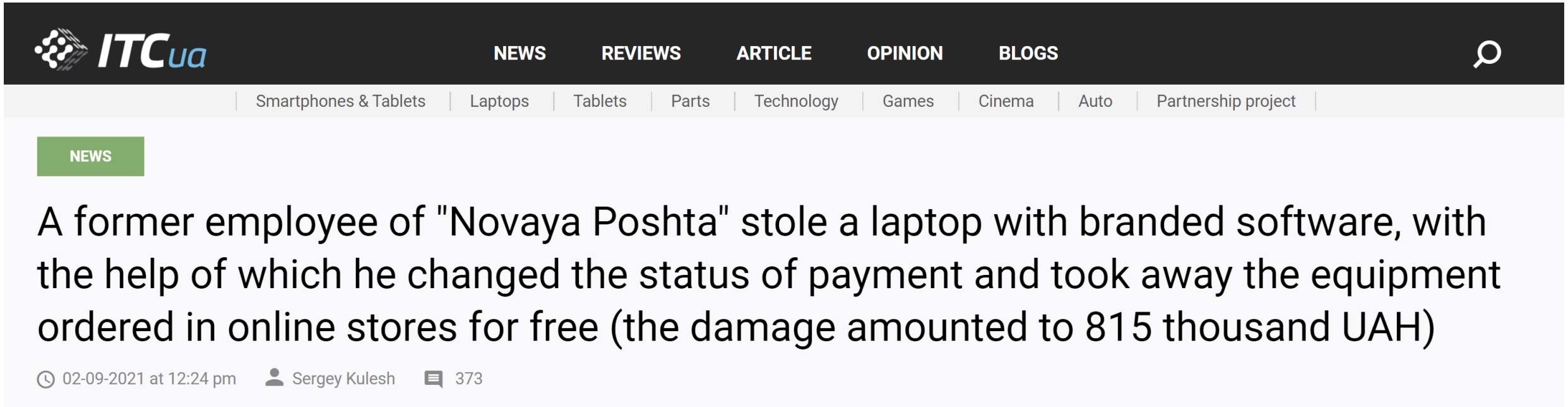
# Breach scenarios

**Encryption break**: from weak encryption algorithms and weak key generators to server-side vulnerabilities and leaked keys



# Breach scenarios

**Physical theft**: taking of another person's property or services




https://itc.ua/news/byvshij-sotrudnik-novoj-poshty-menyal...

# Breach scenarios

CVE exploitation

## Zero-Day in WordPress Plugin Exploited to Create Admin Accounts

By **Sergiu Gatlan** February 19, 2020 12:01 PM 0


A zero-day vulnerability in the ThemeREX Addons, a WordPress plugin installed on thousands of sites, is actively exploited by attackers to create user accounts with admin permissions and potentially fully taking over the vulnerable website.

https://www.bleepingcomputer.com/news/security/zero-day-in-wordpress-plugin-exploited-to-create-admin-accounts/

# Breach scenarios

## CVE exploitation

### Log4Shell

From Wikipedia, the free encyclopedia

**Log4Shell** (**CVE-2021-44228**) was a zero-day vulnerability in Log4j, a popular Java logging framework, involving arbitrary code execution.[2][3] The vulnerability has existed unnoticed since 2013 and was privately disclosed to the Apache Software Foundation, of which Log4j is a project, by Chen Zhaojun of Alibaba Cloud's security team on 24 November 2021, and was publicly disclosed on 9 December 2021.[1][4][5][6] Apache gave Log4Shell a CVSS severity rating of 10, the highest available score.[7] The exploit is simple to execute and is estimated to affect hundreds of millions of devices.[6][8]

The vulnerability takes advantage of Log4j's allowing requests to arbitrary LDAP and JNDI servers,[2][9][10] allowing attackers to execute arbitrary Java code on a server or other computer, or leak sensitive information.[5] A list of its affected software projects has been published by the Apache Security Team.[11] Affected commercial services include Amazon Web Services,[12] Cloudflare, iCloud,[13] *Minecraft: Java Edition*,[14] Steam, Tencent QQ and many others.[9][15][16] According to Wiz and EY, the vulnerability affected 93% of enterprise cloud environments.[17]

Experts described Log4Shell as the largest vulnerability ever;[8] LunaSec characterized it as "a design failure of catastrophic proportions",[5] Tenable said the exploit was "the single biggest, most critical vulnerability ever",[18] *Ars Technica* called it "arguably the most severe vulnerability ever"[19] and *The Washington Post* said that descriptions by security professionals "border on the apocalyptic".[8]

https://en.wikipedia.org/wiki/Log4Shell

# Breach scenarios

## DDOS

31

### The Pirate Bay offline following 'quite big' DDoS attack, says Anonymous is not to blame

*The Pirate Bay remains offline after a DDoS attack took the popular torrenting site down, though its operators indicate that Anonymous is not responsible for the situation.*

By Chris Welch | @chriswelch | May 16, 2012, 4:59pm EDT

*Via Ars Technica | Source The Pirate Bay (Facebook)*

SHARE



https://www.theverge.com/2012/5/16/3024861/pirate-bay-offline-ddos-attack

# Breach scenarios

Employee data theft / Social engineering

**The shocking Twitter hack this summer started with a tech support scam, New York regulators allege**

By Brian Fung, CNN Business

Updated 1717 GMT (0117 HKT) October 14, 2020

https://edition.cnn.com/2020/10/14/tech/twitter-hack-tech-support-scam/index.html

# Breach scenarios

## Supply Chain Attacks

APPLE \ MICROSOFT \ TECH

### Security researcher finds a way to run code on Apple, PayPal, and Microsoft's systems

2

*The attack is incredibly simple yet fiendishly effective*

By Mitchell Clark | Feb 10, 2021, 5:43pm EST

*If you buy something from a Verge link, Vox Media may earn a commission. See our ethics statement.*

SHARE

Illustration by Alex Castro / The Verge

verge deals

Subscribe to get the best Verge-approved tech deals of the week.

Email (required)

By signing up, you agree to our Privacy Notice and European users agree to the data transfer policy.

SUBSCRIBE

https://www.theverge.com/2021/2/10/22276857/security-researcher-repository-exploit-apple-microsoft-vulnerability

# Security

But Cloud Provider takes care about security…

# Security

Cloud Provider is responsible for protecting your data **from other tenants**.

Protecting your data from intruders/hackers - is your task.

# Security

Security is about dealing with Risk:

- Accidental deletion
- Theft
- Privacy
- Compliance

# Security

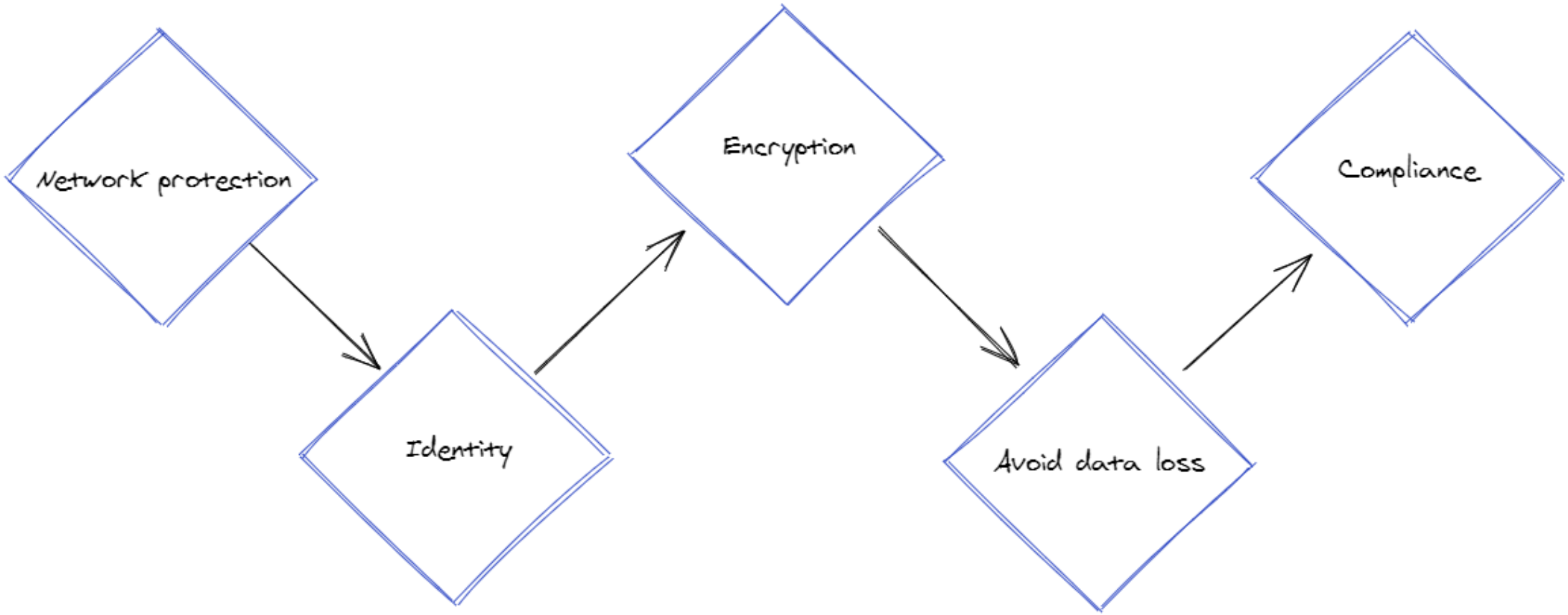
Cloud Provider often gives tools to deal with security risks

# Security

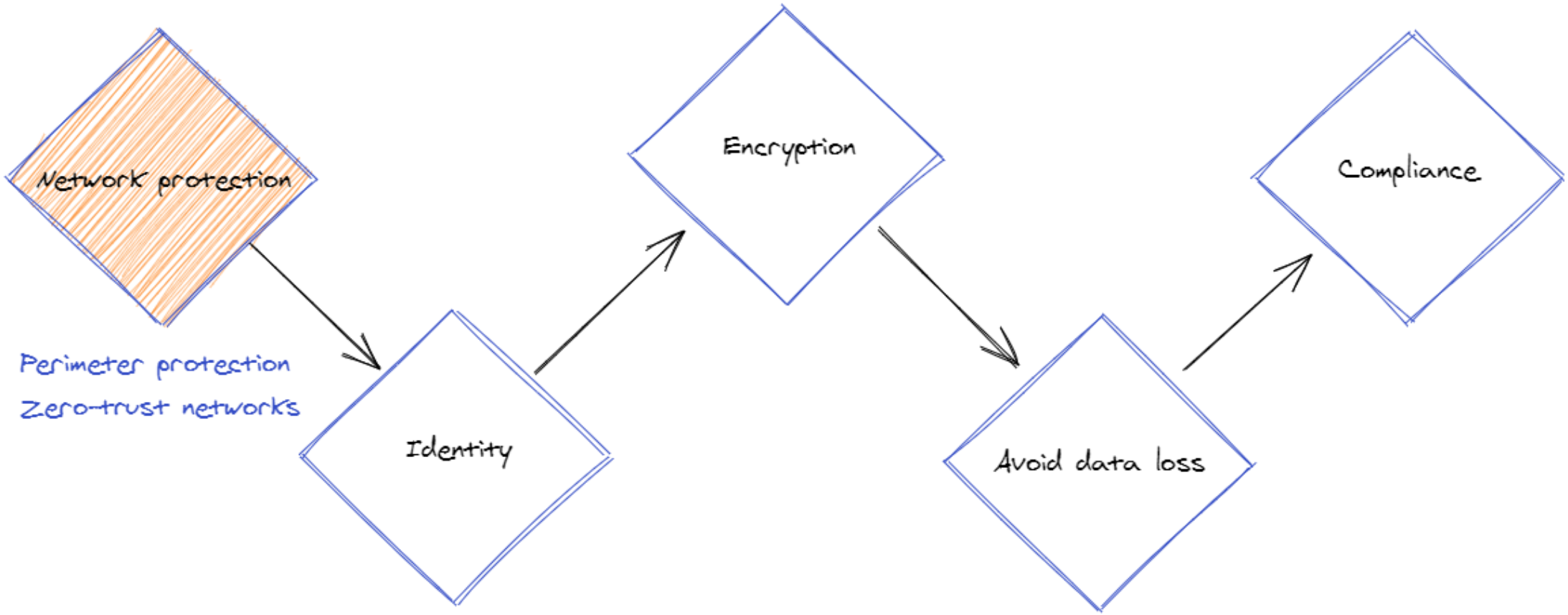
Security comes with a price:

- increased cost and complexity
- decreased maintainability

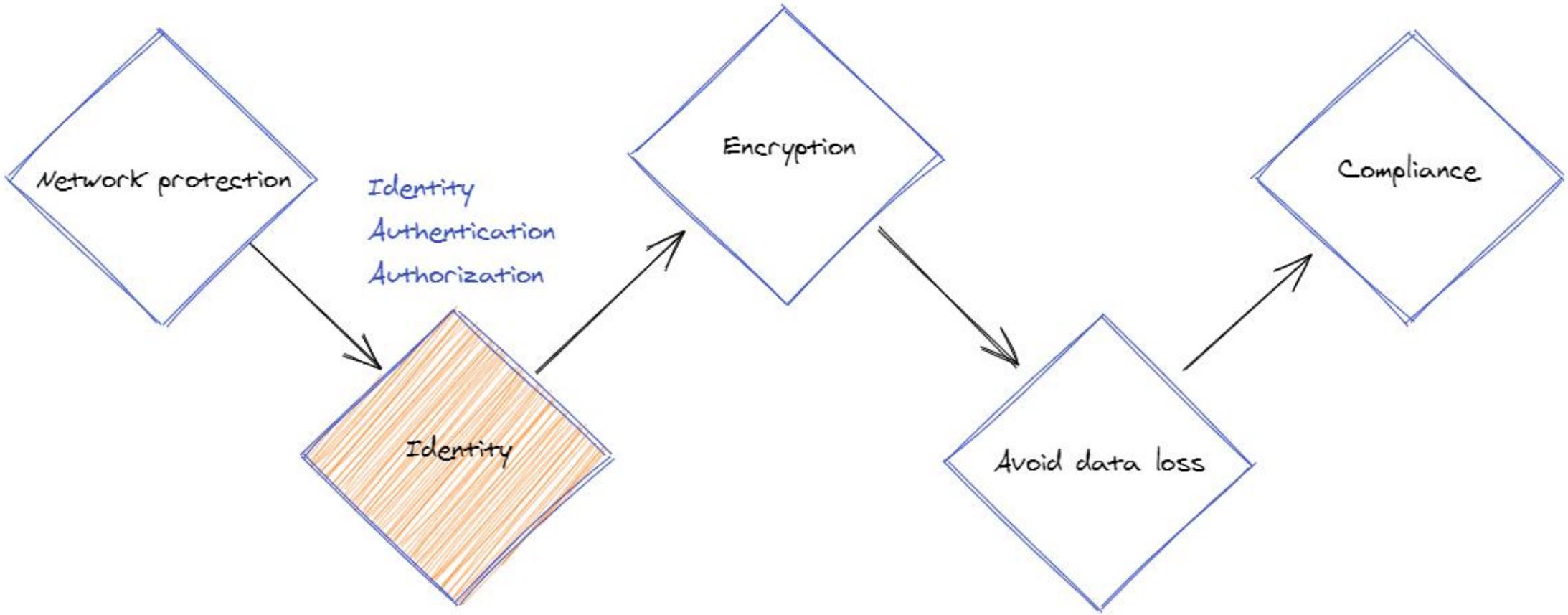
# Security Areas



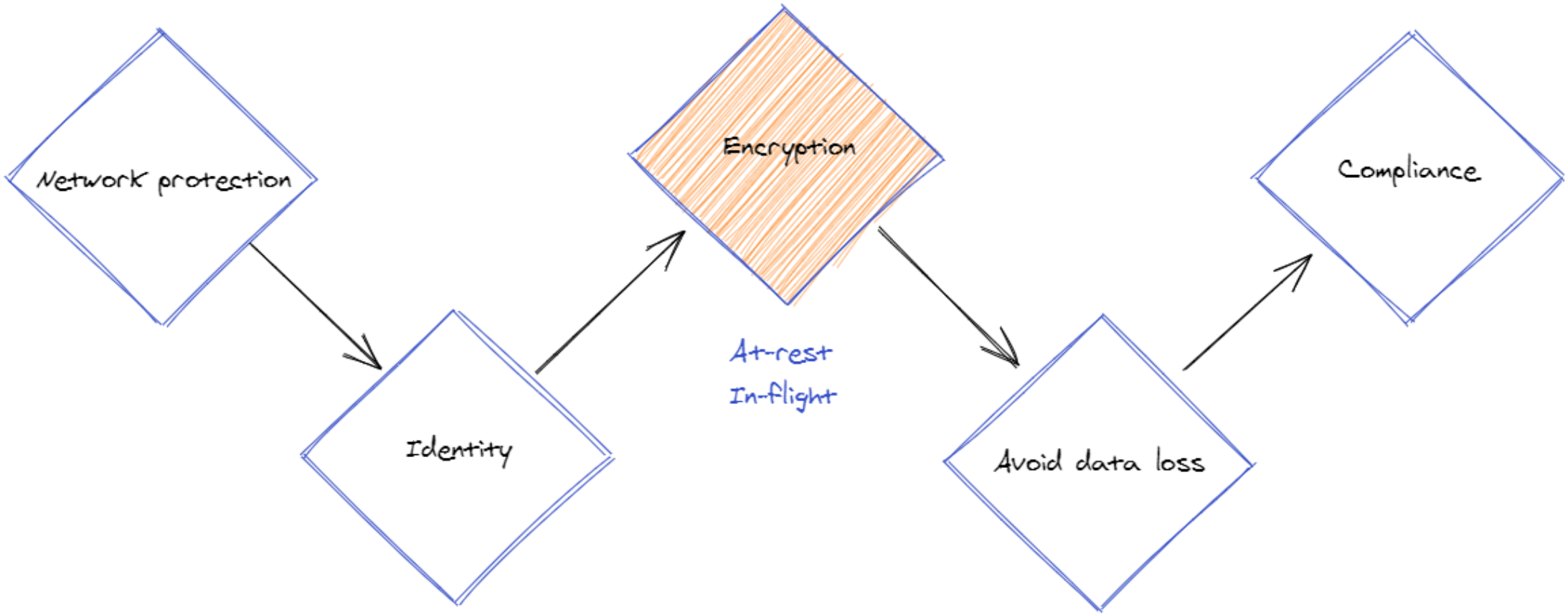
# Security Areas



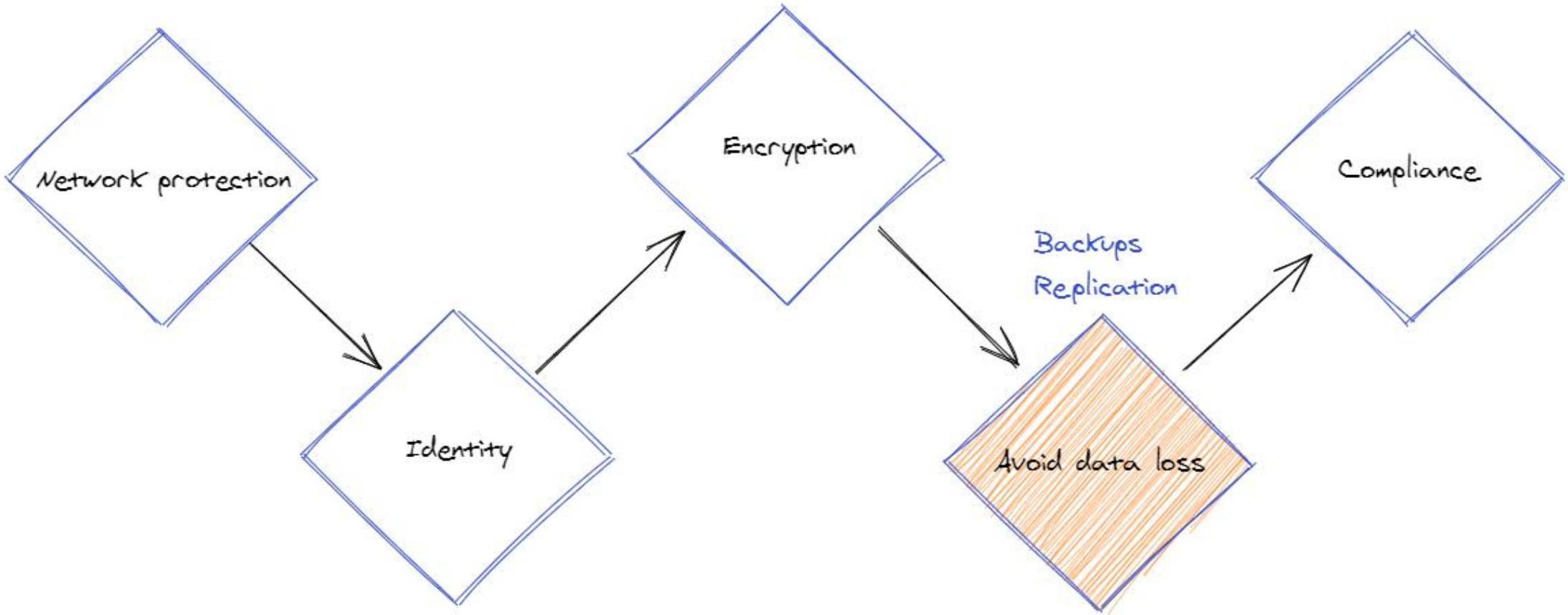
# Security Areas



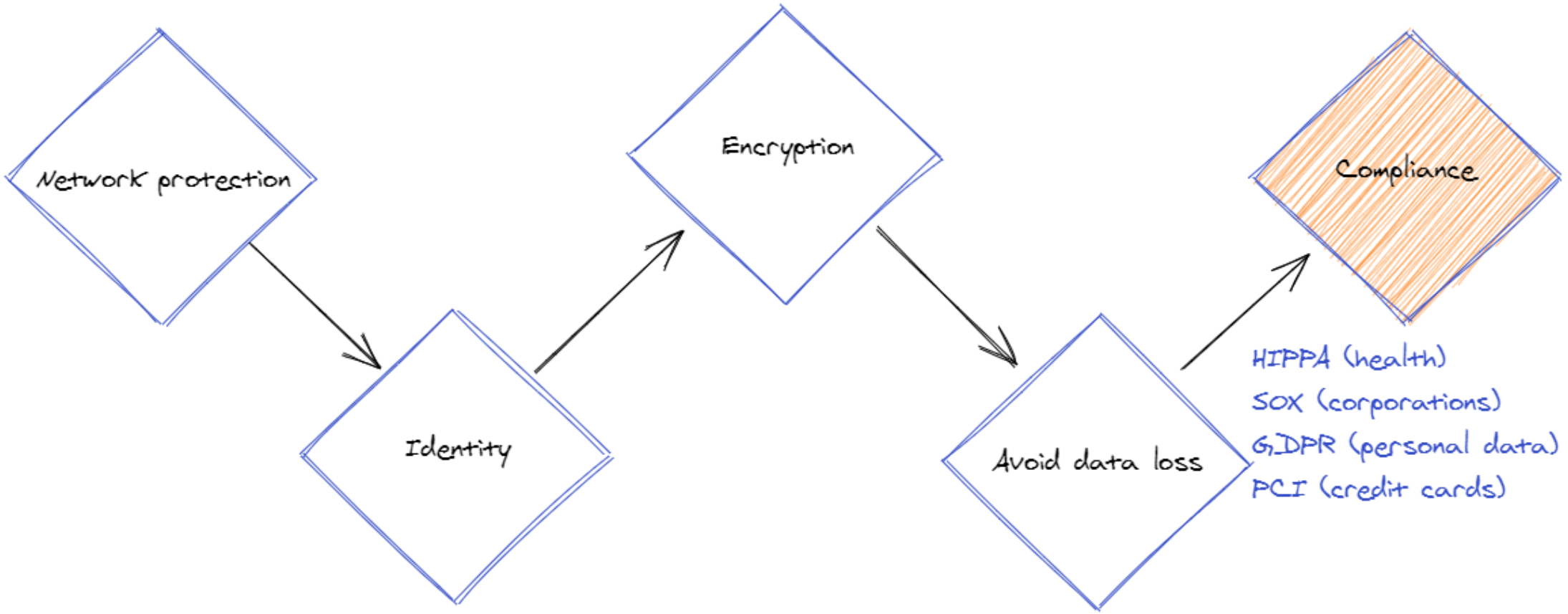
# Security Areas



# Security Areas



# Security Areas



# Security levels

Infrastructure-level security

- Server-side data encryption
- Network traffic protection (in-flight)
- OS, firewalls
- IAM/RBAC

# Security levels

HTTPs is needed even inside private network: How to contact google sre dropping a shell in cloud sql

# Security levels

Application-level security

- Client-side data encryption
- Logs: infrastructure, access-logs, OS, db, api/app
- Monitoring: metrics, notifications/alerts
- Configuration Management: patches, versioning, trusted artifacts

# Security levels

Data-level security

- DB level
- Table/object level
- Record level
- Field level (e.g. one column has more sensitive data than others)

# Security levels

User-interface level

- Least privilege
- Do not use *root*
- Strong passwords
- MFA and PIM
- Secrets rotation
- Custom policies
- Audit logging

# Security levels

Password rotation is required for machines/apps/scripts, but not for humans: The Debate about Password Rotation Policies

Regular human-password rotation causes

- weaker passwords
- work disruptions
- higher cost to maintain across the org

It’s better to use a static but strong password (and password manager)

# Case studies

Public Key Infrastructure (PKI)

# Case studies

Secrets management

- Put expiration date on a secret
- Scoped tokens instead of full-access keys
- Keep secrets out of code

# Case studies

Configuration management

- Patch dependencies
- Scan for CVE
- Sign commits, container-images, assemblies
- Immutable versions, build once

# Case studies

Disaster recovery

- Backup data
- Document restore process


MANAGE > UPTIME

## Fire Has Destroyed OVH's Strasbourg Data Center (SBG2)

OVH SBG2 data center in Strasbourg destroyed by fire on March 10 2021

No OVH, firefighting, or local government services staff members were injured, the company said. Restart of surviving data centers on campus not anticipated until Monday.

https://www.datacenterknowledge.com/uptime/fire-has-destroyed-ovh-s-strasbourg-data-center-sbg2

# Case studies

Avoid circular dependencies and be careful with a single tool combined for unrelated use-cases

- Roblox was down for 73 hours partially because everything relied on a single Consul instance (including monitoring)

- Google wifi-password reset caused the whole company unable to use central password-manager

# Case studies

Custom policies

- Codify rules
- Verify adherence to rules at deployment time
- Monitor/enforce rules at runtime

# Case studies

Expect security services to fail

For example, Parler content was dumped because twilio integration faded away

# Case studies

Note *who* uses your product

- Google is regularly under attack because of Gmail accounts (even in 2010)
- Strava leaked US army bases because of location tracking

# Course plan

Learning session 4

Security

Identity and Access Management (IAM)

# Identity Access Management Lesson Plan

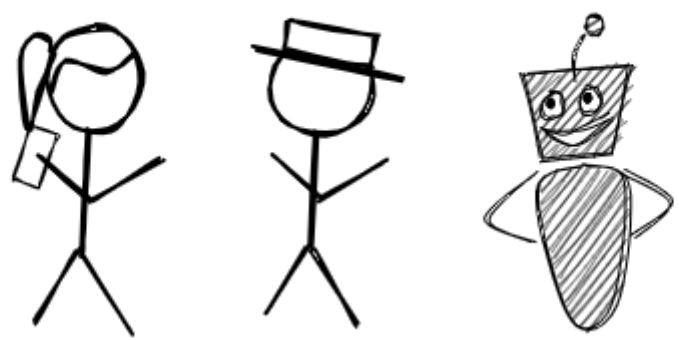
- Common Terminology:
  - Identities, Groups
  - Permissions, Roles
  - Scopes
  - Role-based Access Control (RBAC)
  - Access Control Lists (ACL)
- Authentication
- Authorization
- OAuth, OpenID, SAML Protocols
- Clouds: AWS/GCP IAM, AAD

# Identity

- Digital representation of an actor
- can be authenticated
- user, application, server

# Identity

- Digital representation of an actor
- can be authenticated
- user, application, server

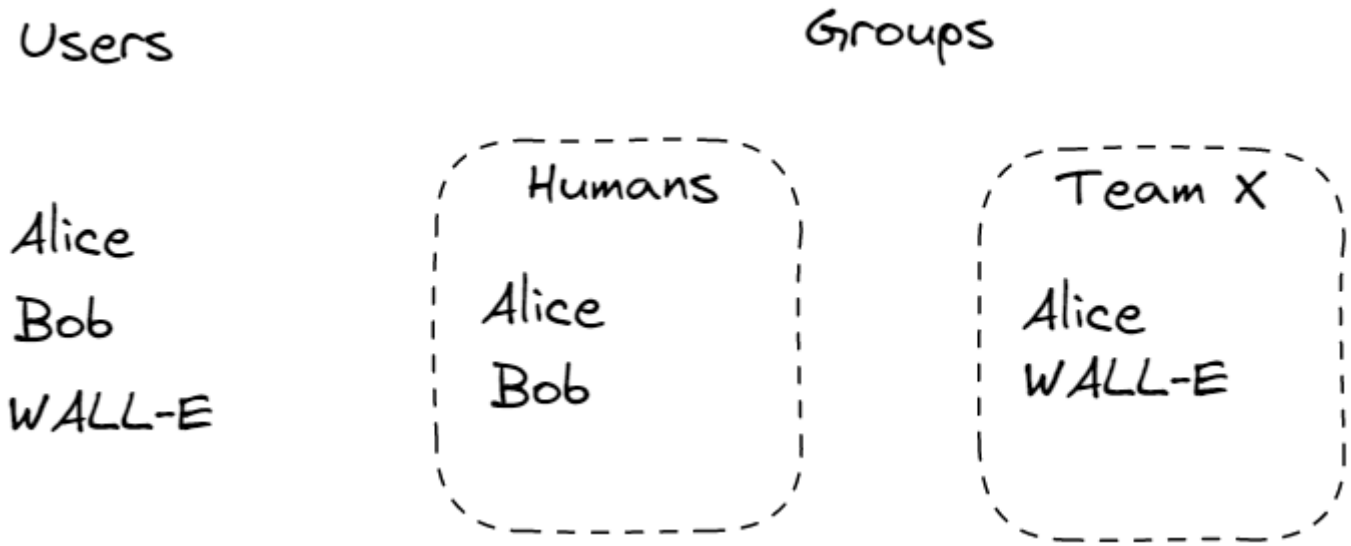


Users

Alice

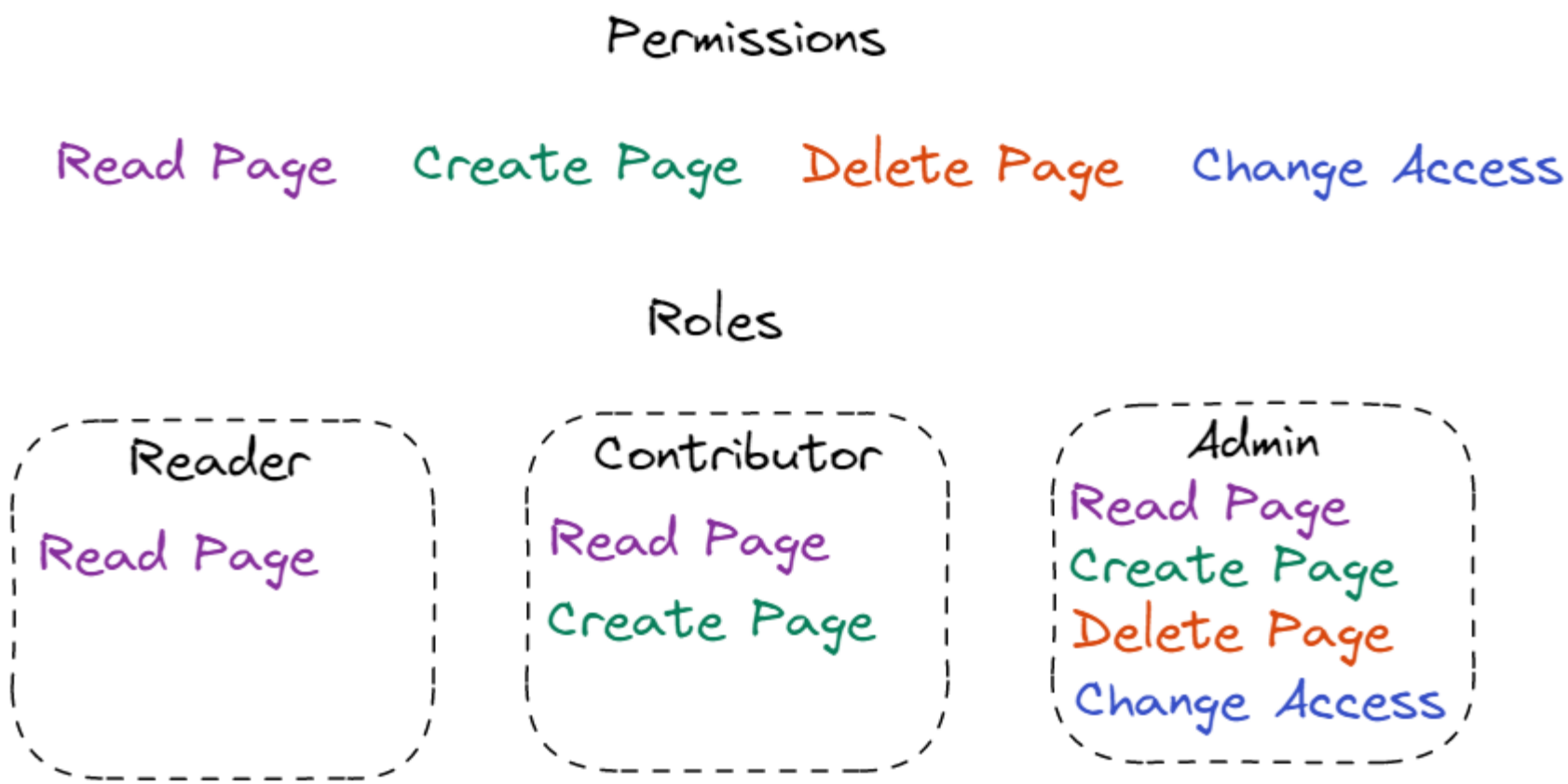
Bob

WALL-E

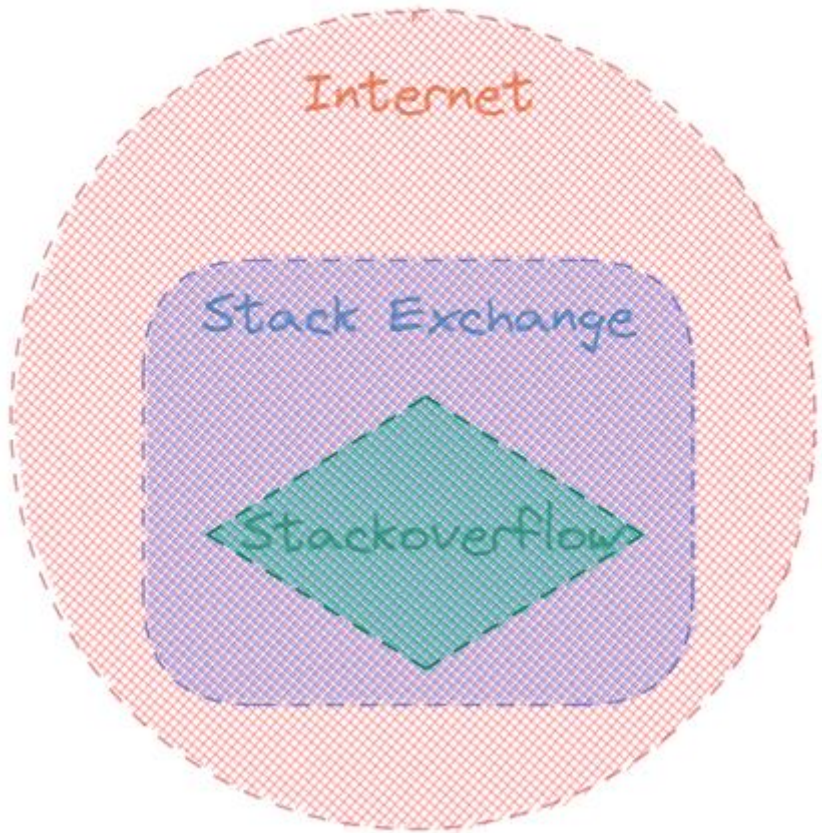

Users
Alice
Bob
WALL-E
Groups
Humans
Alice
Bob
Team X
Alice
WALL-E

Permissions

Read Page  Create Page  Delete Page  Change Access


Permissions
Read Page
Create Page
Delete Page
Change Access
Roles
Reader
Read Page
Contributor
Read Page
Create Page
Admin
Read Page
Create Page
Delete Page
Change Access

# Scope



# Role-based Access Control (RBAC)

Identity is Role in Scope

# Role-based Access Control (RBAC)

| Identity | is | Role | in | Scope |
|---|---|---|---|---|
| Bob | is | Reader | in | Internet |
| Humans | is | Contributor | in | Stack Exchange |
| Team X | is | Admin | in | Stackoverflow |

# Identity Access Management

Azure RBAC explained

## Access-control list (ACL)

List of permissions for a given user on a given resource:

Resource: Identity can Permissions

# Access-control list (ACL)

List of permissions for a given user on a given resource:

| Resource: | Identity | can | Permissions |
|---|---|---|---|
| /my_photos: | Humans | can | Read |
| /my_photos: | Bob | can | Read, Write |

# Identity Access Management

ACLs in Azure Data Lake

# Identity Access Management

Authentication – verification that an identity is who/what they claims

# Identity Access Management

Authentication could be based on

- Password
- Certificate
- Token
- Biometrics (fingerprint, face identification, etc)

# Identity Access Management

Authorization – verify that exact identity is permitted to perform an operation

# Identity Access Management

*SAML*

- Open standard to exchange authentication and authorization data.
- First published in 2001, SAML 2.0 in 2005
- XML-based markup + protocol

# Identity Access Management

*OAuth*

- Open standard to delegate access [authorization]
- First published in 2006
- OAuth 2.0 published in 2012

# Identity Access Management

*OpenID* – authentication protocol first published in 2006.

*OpenID Connect (OIDC)* – the third version of OpenID protocol, published in 2014

# Identity Access Management

OAuth 2.0 is only for authorization

OpenID Connect (OIDC) is a layer on top of OAuth 2.0 and **adds login and profile information** about the person who is logged in

OIDC enables single-sign-on (SSO) and uses id-token (e.g. JWT)

# Identity Access Management

An Illustrated Guide to OAuth and OpenID Connect

# Identity Access Management

AWS IAM

GCP IAM

Azure Active Directory (AAD)

# Identity Access Management

All of them covers authentication and authorization:

- Verifies *Identities*
- Manage *Identities* access to *Resources* via *Permissions*
- Aggregate *Identities* into *Groups*
- Aggregate *Permissions* into *Roles*

# Identity Access Management

Plus

- Identity management
- Auditing – logs to answer the question “who did what, where and when?”
- Policies – enforce rules

# Identity Access Management

Demo

- Kubernetes RBAC
- Azure Active Directory

# Additional resources

- (article) What is DDOS attack
- (article) How to break encryption
- (article) Public Key Infrastructure
- (article) What is good Runbook
- Password generator and common password approaches with **negative** impact