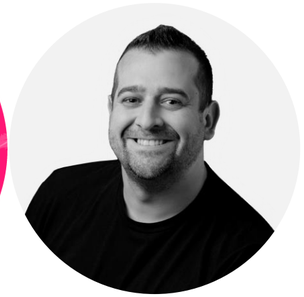
Security Concepts and Methodologies in the Microsoft Cloud



Vlad Catrinescu

Microsoft MVP | Independent Consultant

@vladcatrinescu | VladTalksTech.com | YouTube.com/@VladTalksTech

Overview

Common security threats

Zero Trust methodology

Defense in depth

Encryption

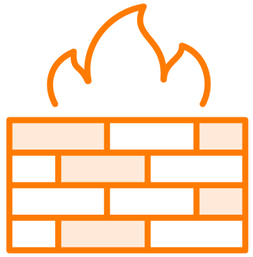
Hashing

Digital signatures

Common Security Threats

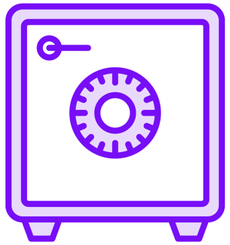
Common Security Threats

Data breach

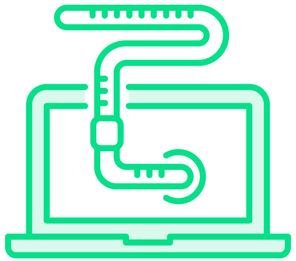


Disruptive attacks

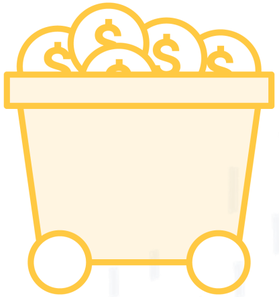
Dictionary attack
aka Brute Force Attack



Ransomware



Worms



Coin miners
aka Cryptojacking

Data Breach

A data breach is when data is stolen

- Personal data

Can result in identity attacks

- Phishing / Spear phishing

Phishing

Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

https://www.phishing.org/what-is-phishing

Phishing vs. Spear Phishing

Phishing	VS	Spear Phishing
Sent to hundreds or thousands of recipients with the same message		Highly targeted – usually a specific individual The hacker researches the target beforehand Boss / Colleagues E-mail comes from someone you know for a task you usually do

Dictionary Attacks

Also called *Brute Force Attack*

Common identity attack

Hacker attempts by trying a large number of known passwords

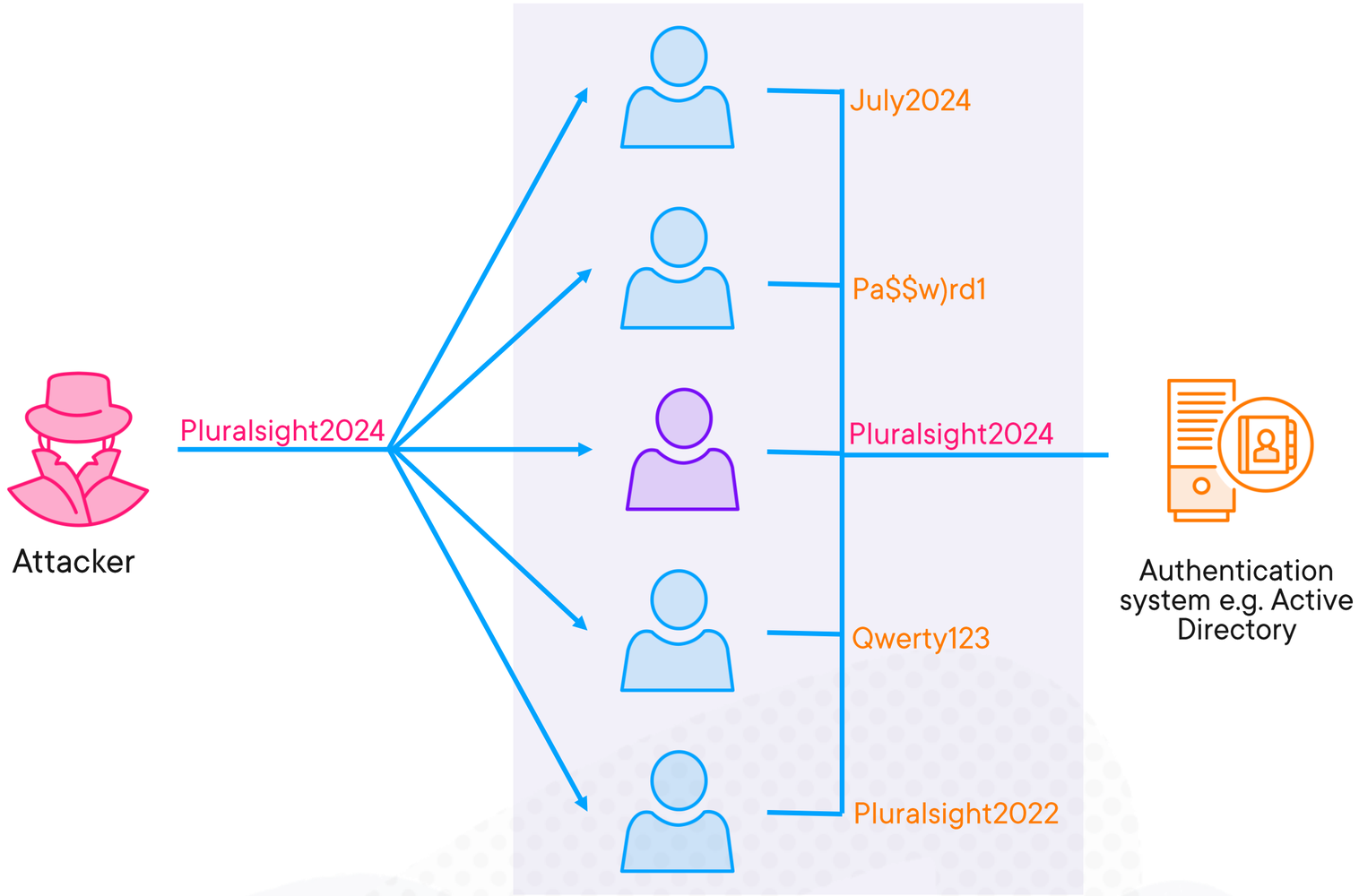
- Each password is automatically tested against a known username

Password Spray

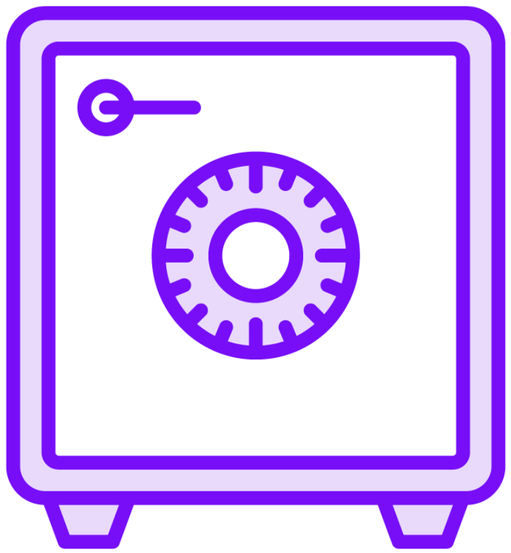
Identity attack

Submit a small number of known weakest password to all accounts in an organization

Limited number of tries to avoid detection thresholds



Ransomware



Type of malware that encrypts files and folders

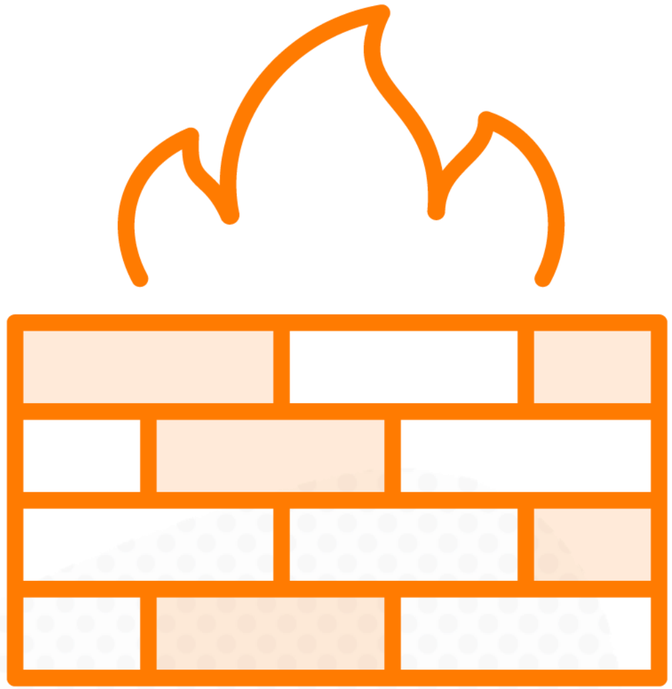
Ransomware attempts to extort money from victims in exchange for the decryption key

- Usually in cryptocurrency

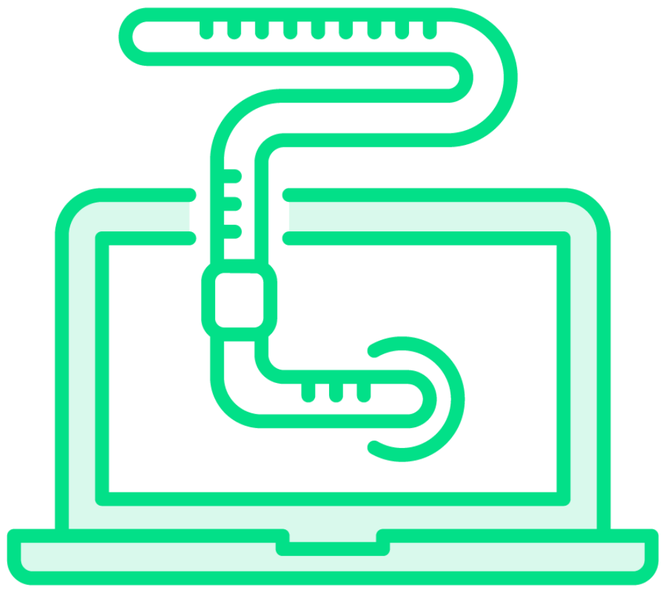
Disruptive Attacks

Distributed Denial of Service (DDoS) attack

- Exhaust an application / server / service resources by flooding it with traffic
- Renders the target unavailable to legitimate users



Worms



Type of malware that can copy itself

Spreads through a network by exploiting vulnerabilities

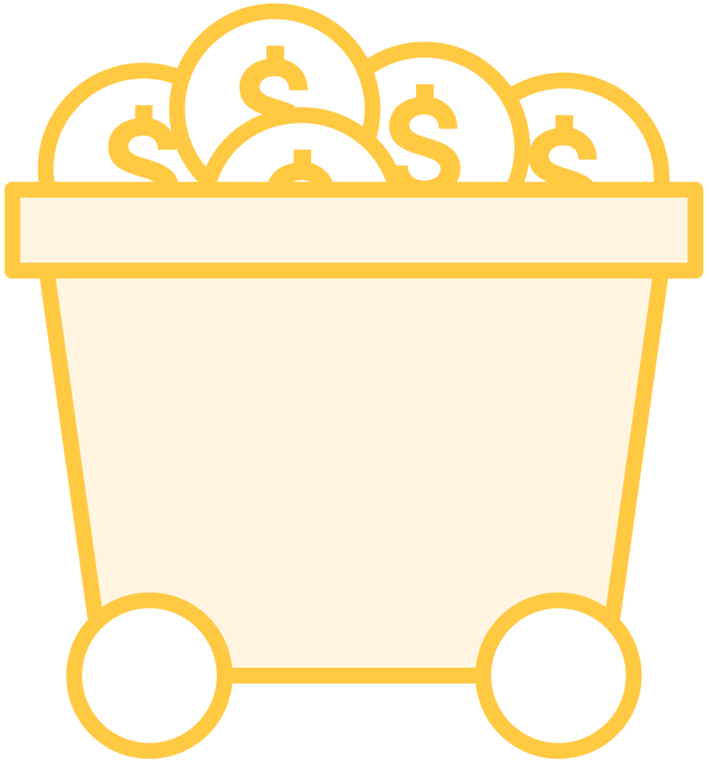
Can spread trough multiple ways

- E-mail attachments
- Text messages
- Removable drives

Coin Miners (Cryptojacking)

Affected computer mines for Cryptocurrency currency for the hacker

Affected computers only notice a decrease in performance



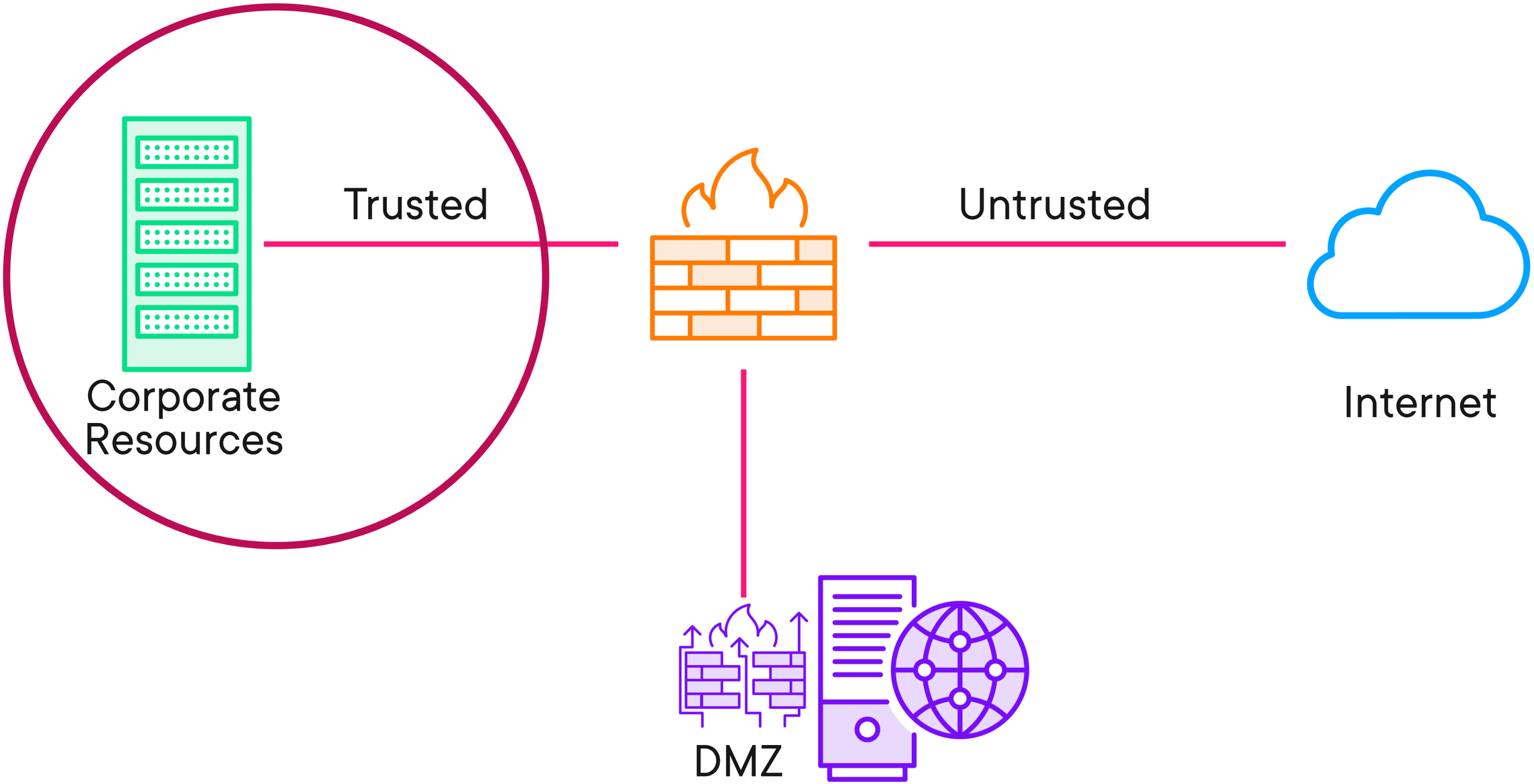
Zero Trust Methodology

Zero Trust

Zero Trust is a cybersecurity model with a very simple premise: eliminate the concept of “trust” from your network.

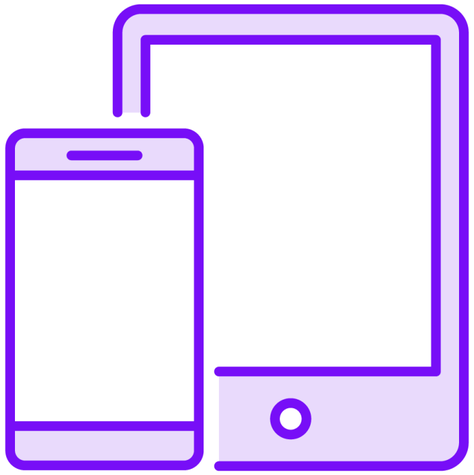
https://www.techradar.com/features/zero-trust-the-strategic-approach-to-stop-data-breaches

Traditional Network Design

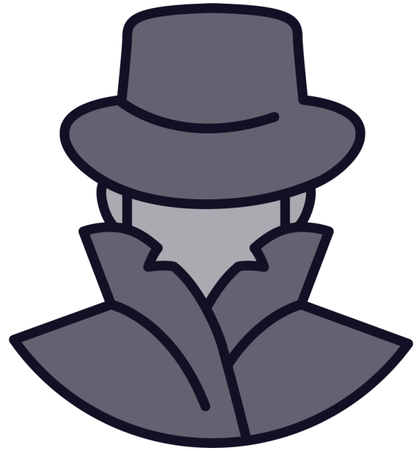


The Corporate Perimeter Has Changed

Cloud technology



Mobile workforce

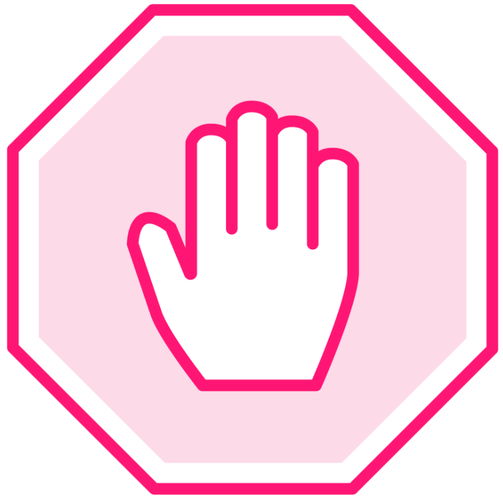


Bad actors and threats have evolved

NIST SP 800-207

Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned).

Zero Trust Guiding Principles



Verify Explicitly

Least Privileged Access

Assume Breach

Verify Explicitly

Authenticate and authorize based on available data points

- User identity
- Location
- Device
- Service
- Data anomalies

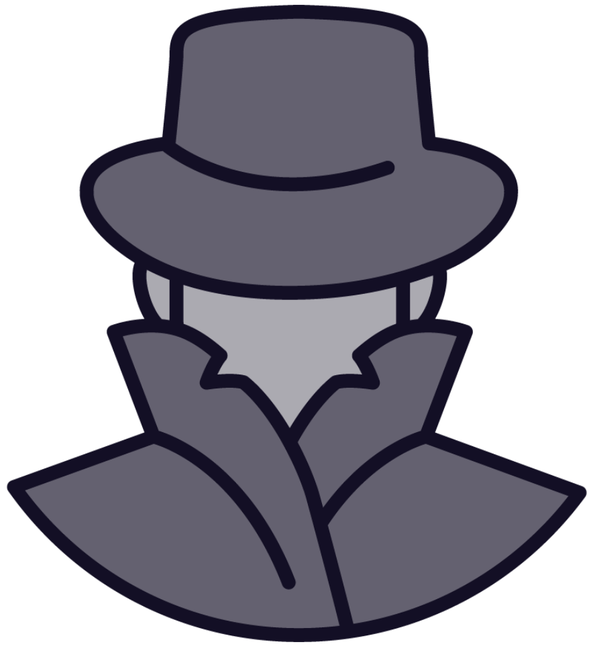
Least Privileged Access

Limit users with Just-in-time and just-enough access

JIT/JEA

Risk-based adaptive policies

Assume Breach



Segment access by network, user, devices, and application

Use encryption to protect data

Use analytics to get visibility

Zero Trust Foundational Pillars

Identities

Identities must be verified with strong authentication, and follow least privilege access principles

Devices

Monitoring devices for health and compliance is an important aspect of security

Applications

Discovering all applications being used, sometimes called Shadow IT because not all applications are managed centrally

Data

Should be classified, labeled, and encrypted based on its attributes

Infrastructure

To improve security, you assess for version, configuration, and JIT access, and use telemetry to detect attacks and anomalies

Networks

Should be segmented, including deeper in-network micro segmentation

Learn more about it on Pluralsight

Zero Trust Architecture (ZTA)

Learning Path

Defense in Depth

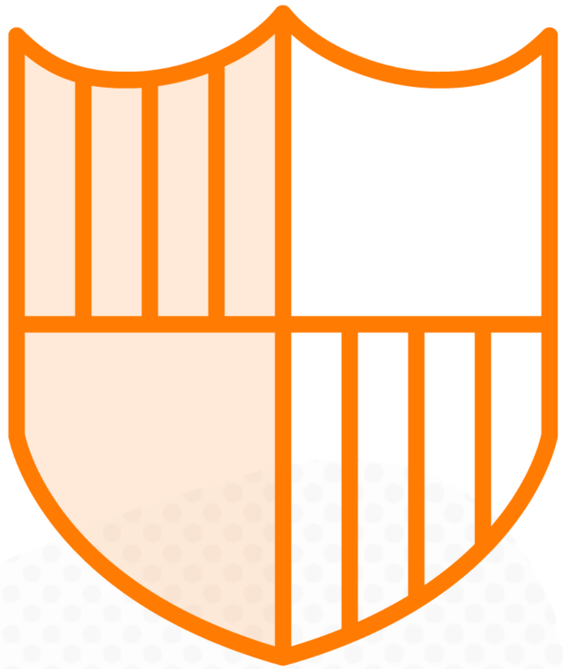
Center for Internet Security (CIS)

Defense in Depth (DiD) refers to an information security approach in which a series of security mechanisms and controls are thoughtfully layered throughout a computer network to protect the confidentiality, integrity, and availability of the network and the data within.

Defense in Depth

Use a layered approach, rather than relying on a single perimeter

If one layer is breached – a subsequent layer will prevent an attacker getting access to the data



Layers of Security

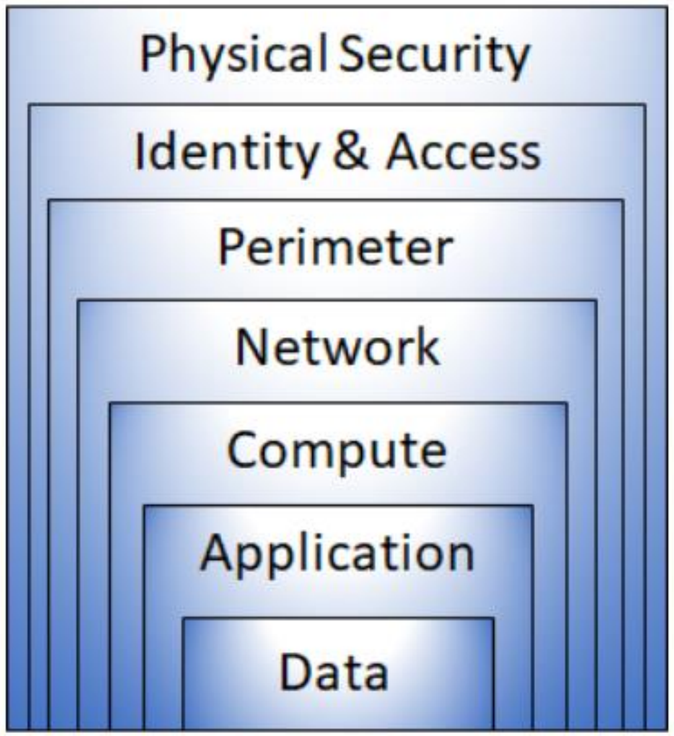


Image Source: Microsoft©

Physical

- Limiting access to a datacenter

Identity & Access

- Security controlling access to infrastructure

Perimeter

- Denial of Service protection

Network

- Limit communication between resources with segmentation

Layers of Security (Continued)

Compute

Secure access to VMs by closing certain ports

Application

Ensure that applications are secure and free of security vulnerabilities

Data

Encryption to protect data

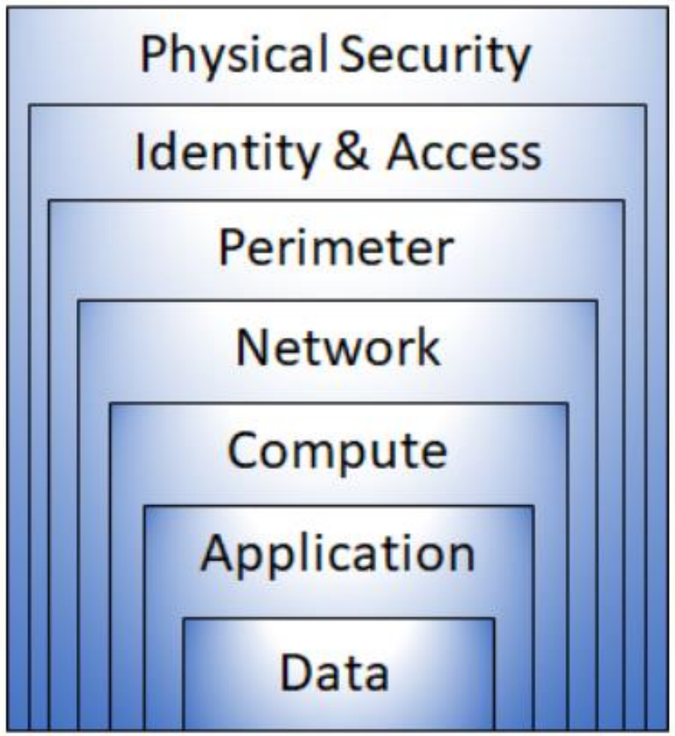
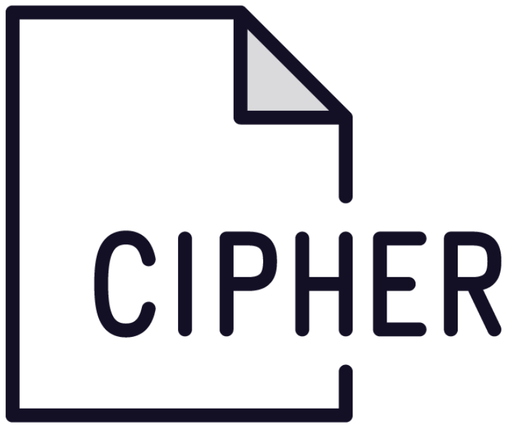


Image Source: Microsoft©

Encryption

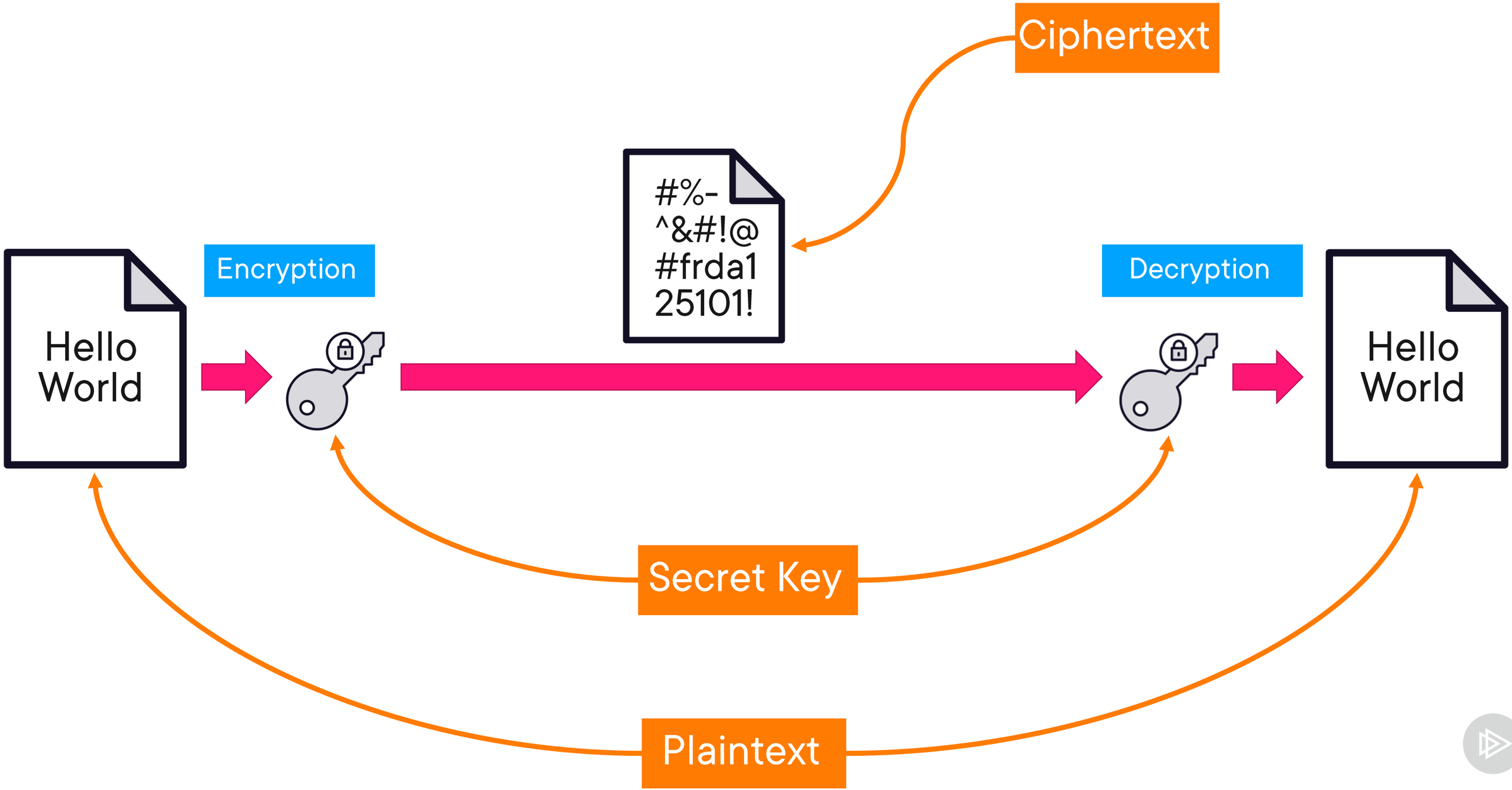
Encryption



The process of making data unreadable and unusable to unauthorized viewers

Data must be decrypted using a secret key to be used

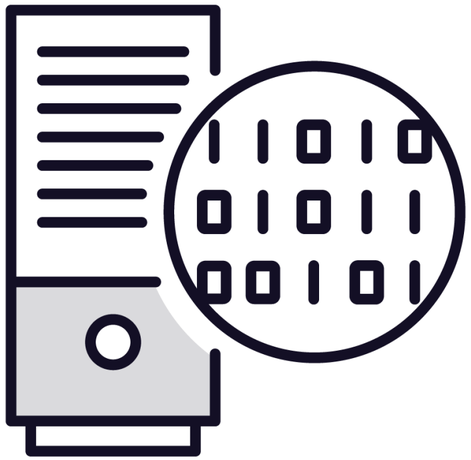
Encryption Basics



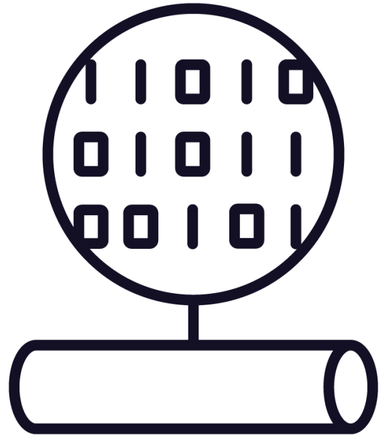
Types of Encryption Methods

Symmetric Cryptography	VS	Asymmetric Cryptography
Single key to encrypt and decrypt the data		Two keys instead of one - A public key - A private key Used for Transport Layer Security (TLS) - Such as the HTTPS protocol

Data Encryption

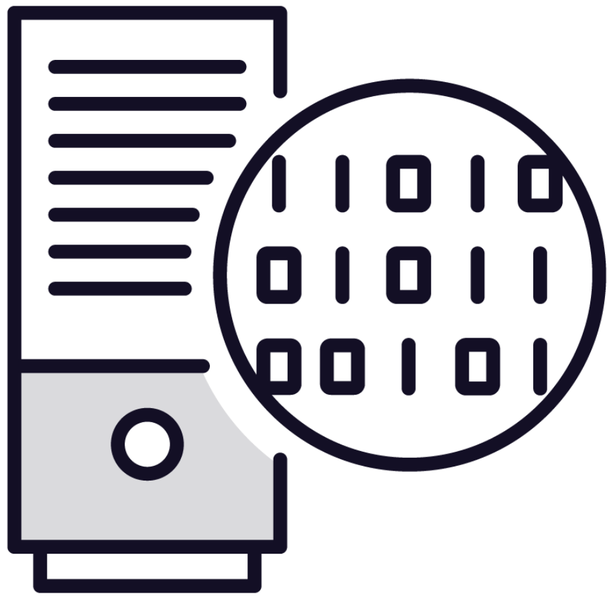


Data at Rest



Data in Transit

Encryption at Rest



Data that's stored on a physical device

- Server
- Hard drive
- Database
- Storage account

Data is unreadable without the keys needed to decrypt it

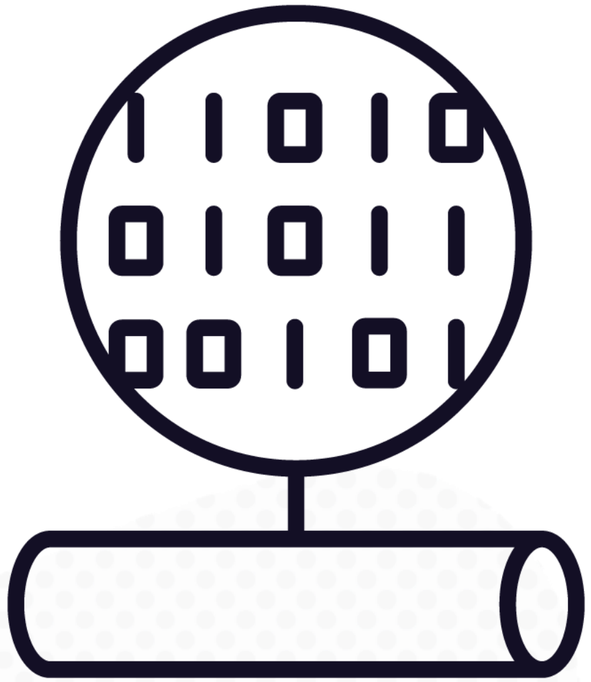
- Even if physical storage is stolen

Encryption in Transit

Data moving from one location to another

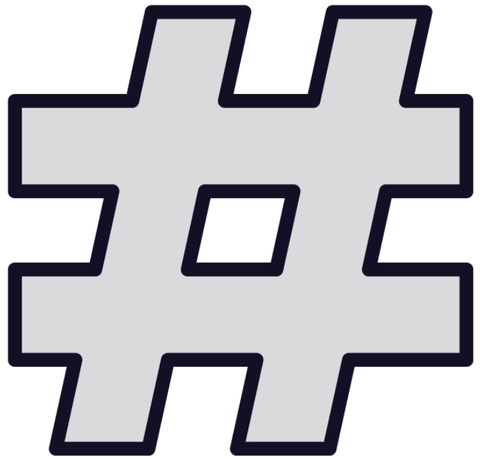
Protects data from outside observers

HTTPS is an example of encryption in transit



Hashing

Hashing



Using an algorithm to map data of any size to a *unique* fixed length value

The hash can be used as a unique identifier of its associated data

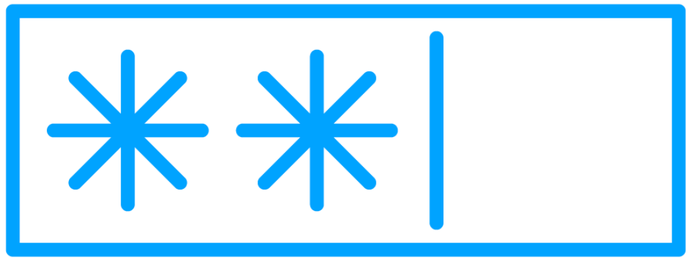
Hashing is deterministic

- Same input produces the same output
- Changing anything in the input will produce a different hash

Encryption vs. Hashing

Encryption	VS	Hashing
Protect data at rest or in transit Encrypted data needs to be decrypted to be used		Hashing is meant to verify that a file or piece of data hasn't been altered Hashing is a one-way function

Password Hashing



Hashing is often used to store passwords

When you enter a password

- Same algorithm is used to create a hash of the password
- The hash is compared to the stored hash version of the password
- If they match – password is correct

Salting

Hash functions are deterministic

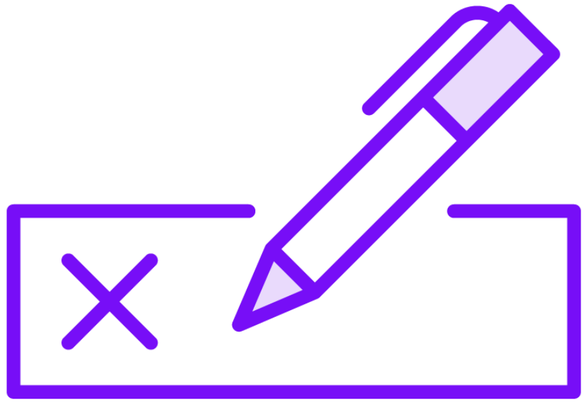
- Hackers can use brute-force attack by hashing the password
  - For a matched hash – they can know the actual password

Salting means adding a random value known only to you to the input

- User password: Plur@ls!ght
- Add your SALT before hashing: Plur@ls!ghtSALT

Digital Signatures

Digital Signatures



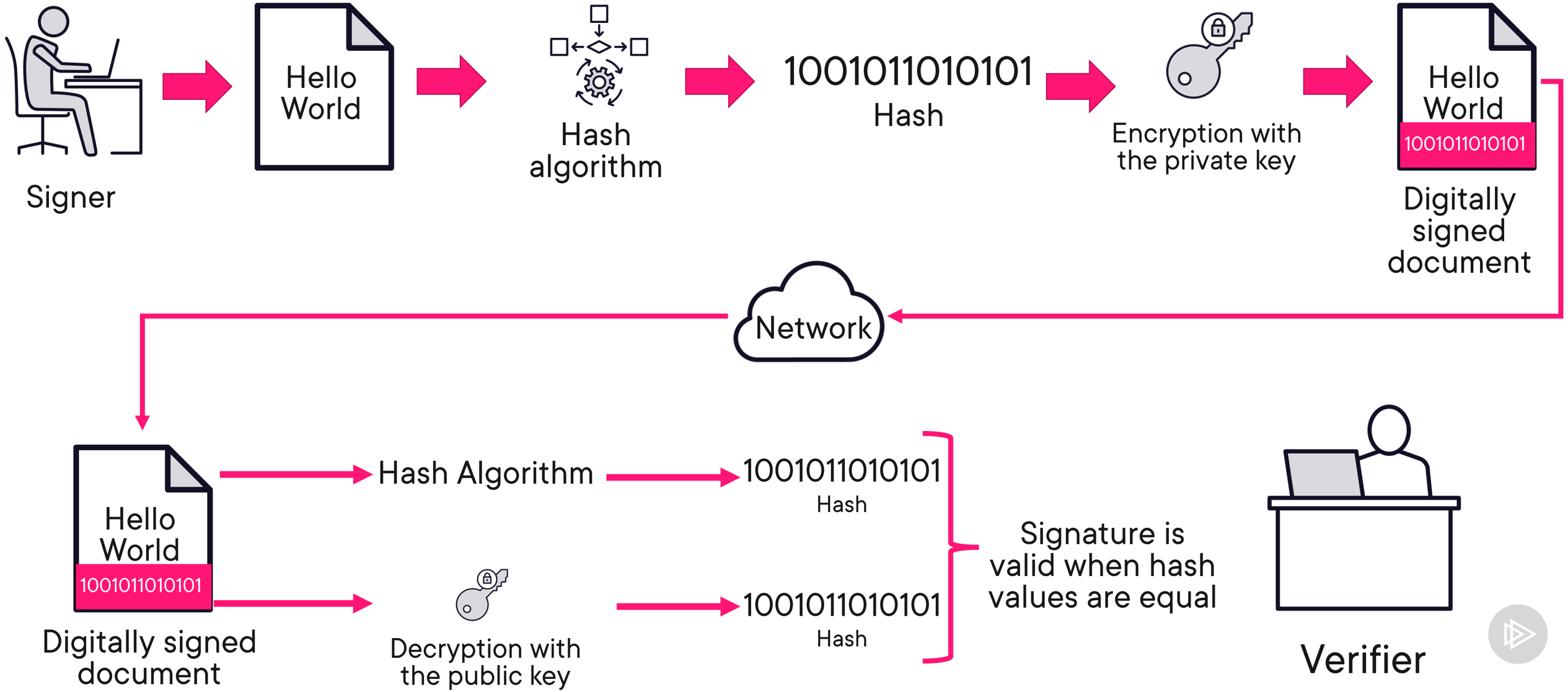
Digital signatures prove that a document was not modified from the time it was signed

- Intentionally or unintentionally

Digital signatures use both encryption keys and hashing

- But do not necessarily encrypt the content of the message
- Asymmetric cryptography is used to encrypt the hash

Digital Signatures Overview



Module Conclusion

Common threats for enterprises today

Zero Trust methodology

- Never trust, always verify
  - Verify explicitly
  - Least privileged access
  - Assume breach

Defense in depth

- Layered approach

Encryption

Hashing

Digital signatures

Up Next:

Identity Concepts in the Microsoft Cloud