Cloud Service Provider Security Posture

Ensuring Security in Cloud Computing

Madyan Makki

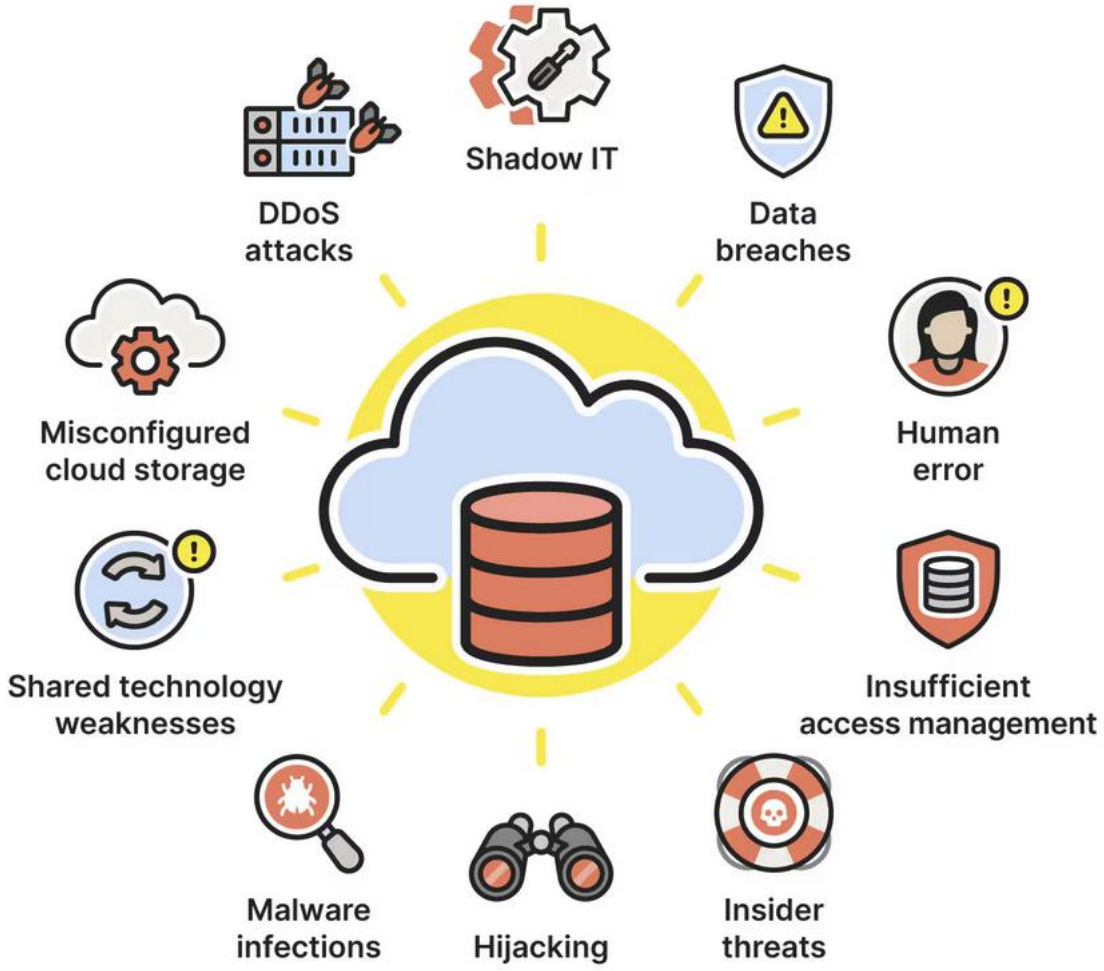
Challenges and Risks

Common Security Risks and threats:

Data breaches
Insider threats
Misconfigurations
Lack of compliance

How CSPs Address These Risks:

Continuous monitoring and threat intelligence
Security training and best practices for users
Regular security audits and compliance checks



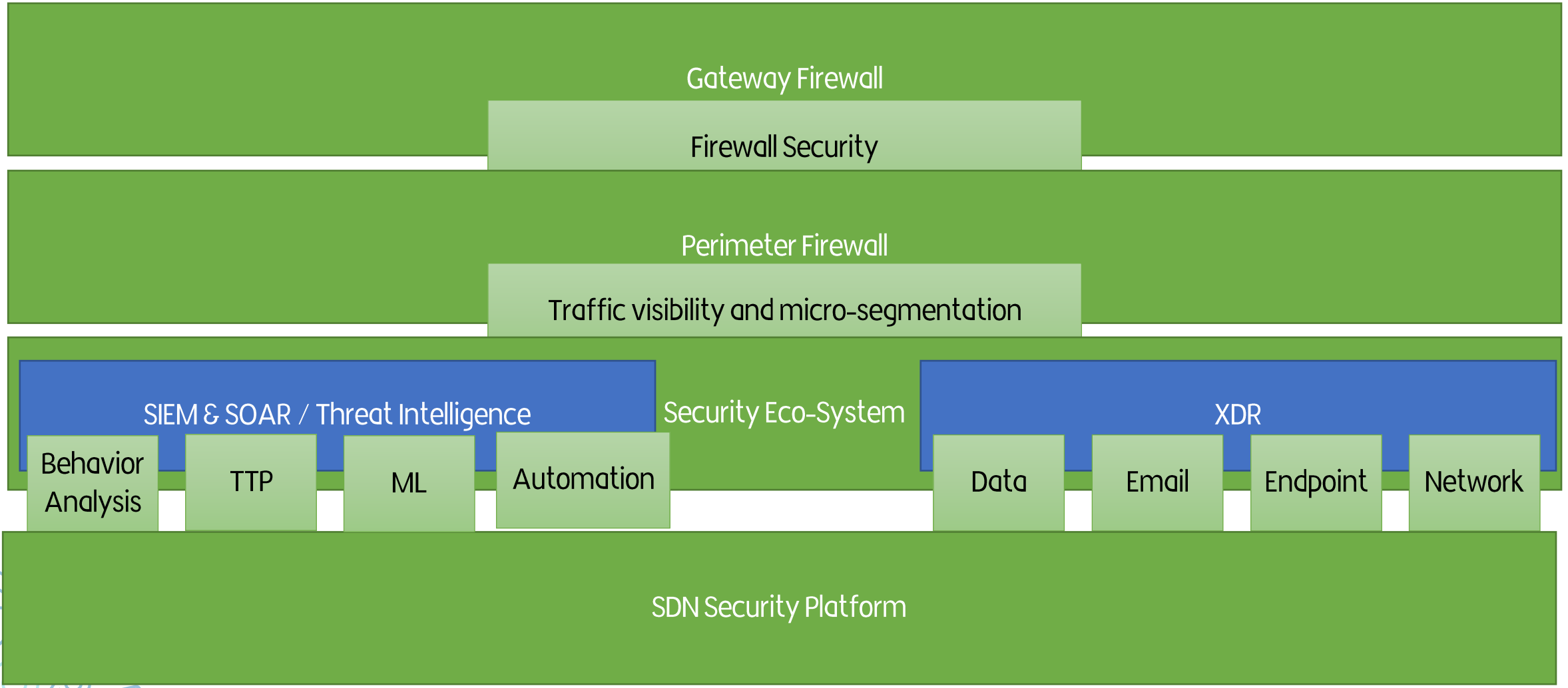
CSP Security Stack

Cloud Service Providers (CSPs) offer a comprehensive security stack to ensure the protection of data, applications, and infrastructure within the cloud. This stack includes various components that work together to provide robust security.

Components

- Identity and Access Management (IAM): Manages user identities and controls access to resources.
- Data Protection: Ensures data is encrypted both at rest and in transit.
- Network Security: Protects against network-based threats through firewalls, DDoS protection, and secure configurations.
- Security Monitoring and Incident Response: Continuously monitors the cloud environment for threats and provides tools for incident response.
- Compliance and Governance: Ensures adherence to industry standards and regulatory requirements.
- Application Security: Protects applications from vulnerabilities and attacks through secure development practices and runtime protection.

Sohobcom Security Stack



Identity and Access Management (IAM)

Key Features:

- User Authentication: Ensures users are who they claim to be through passwords, biometrics, or multi-factor authentication (MFA).
- Access Controls: Assigns permissions to users and roles to control access to resources.
- Single Sign-On (SSO): Allows users to log in once and gain access to multiple systems without re-authenticating.

Benefits:

- Reduces risk of unauthorized access.
- Simplifies user management and improves user productivity.

Security Analytics

Key Features:

- Threat Detection: Identifies and responds to threats in real-time.
- Data Correlation: Correlates data from various sources to detect complex attacks.
- Incident Response: Provides tools for investigating and mitigating security incidents.

Benefits:

- Enhances visibility into security threats.
- Reduces response time to security incidents.

Unified Threat Protection

Key Features:

- Firewall: Controls incoming and outgoing network traffic.
- Antivirus: Scans for and removes malware.
- Intrusion Prevention System (IPS): Detects and blocks network-based attacks.

Benefits:

- Provides comprehensive protection against a wide range of threats.
- Simplifies security management with an all-in-one solution.

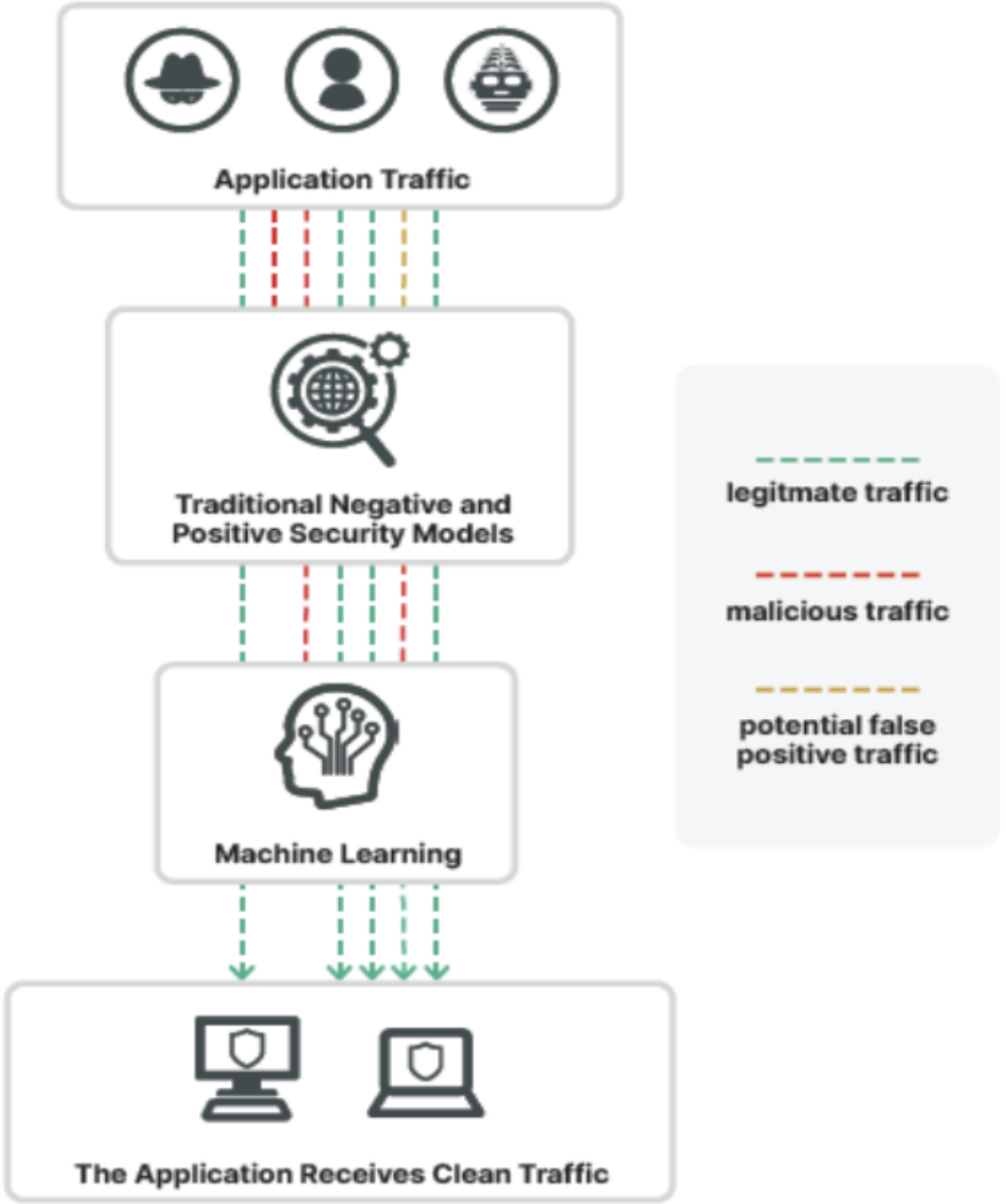
Web Application Firewall

Key Features:

- Web Application Security: Protects web applications from attacks like SQL injection and cross-site scripting (XSS).
- Bot Mitigation: Detects and blocks malicious bots.
- API Security: Protects APIs from abuse and attacks.

Benefits:

- Ensures the security and integrity of web applications.
- Enhances protection against automated threats.



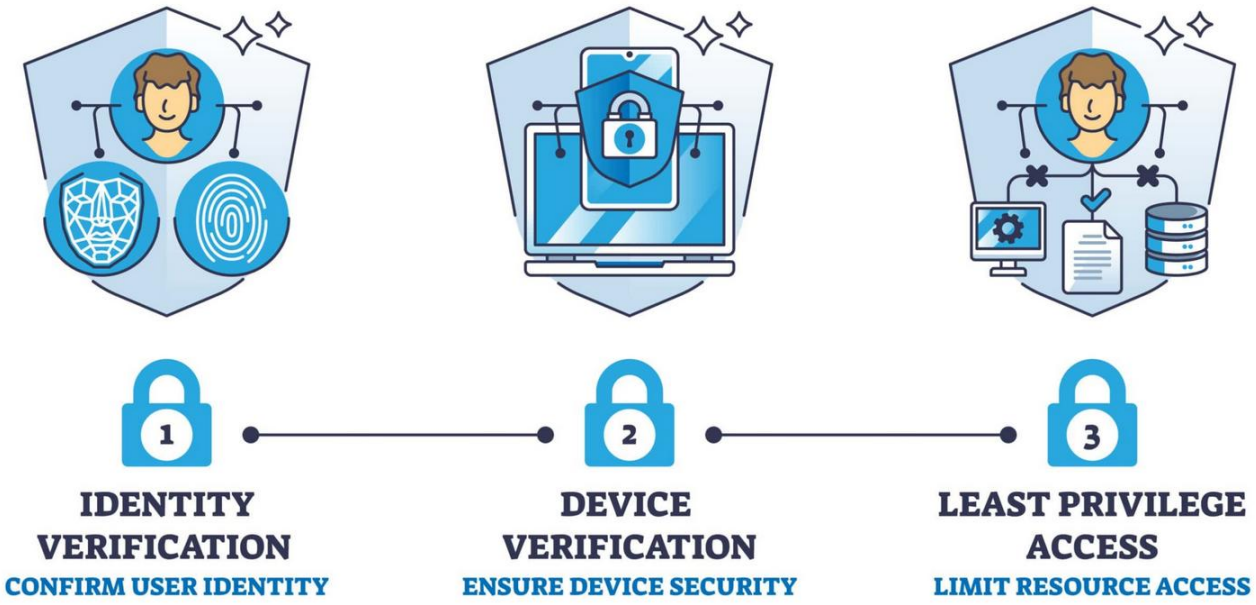
ZTNA

Key Features:

- Micro-Segmentation: Divides networks into smaller, isolated segments.
- Access Control: Grants access based on user identity and context.
- Continuous Monitoring: Continuously verifies trust before granting access.

Benefits:

- Enhances security by limiting access to only what is necessary.
- Reduces the risk of lateral movement within the network.



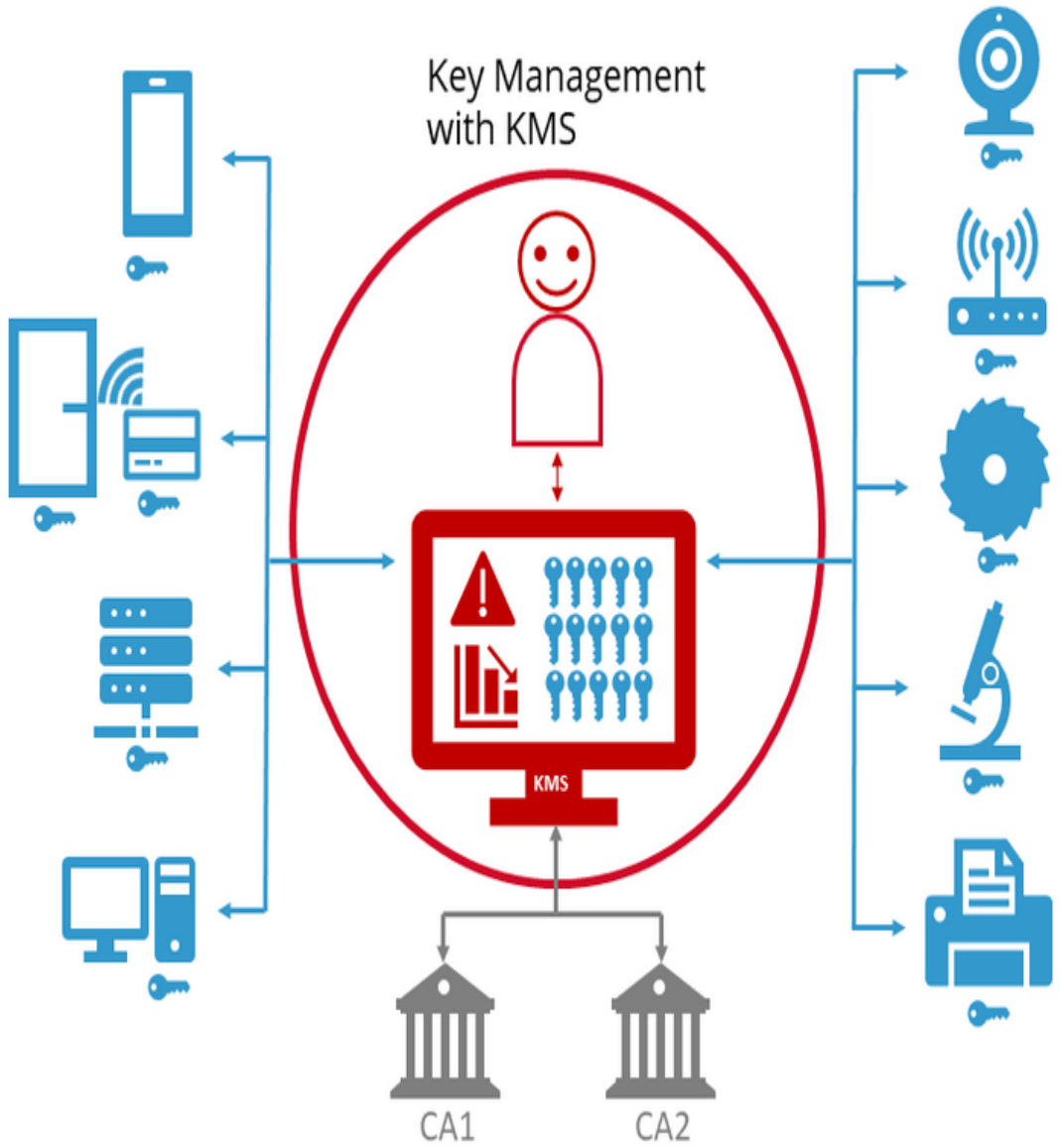
Key Management Service (KMS)

Key Features:

- Key Creation and Rotation: Creates and rotates encryption keys securely
- Access Control: Manages access to encryption keys.
- Auditing: Provides logs of key usage for auditing.

Benefits:

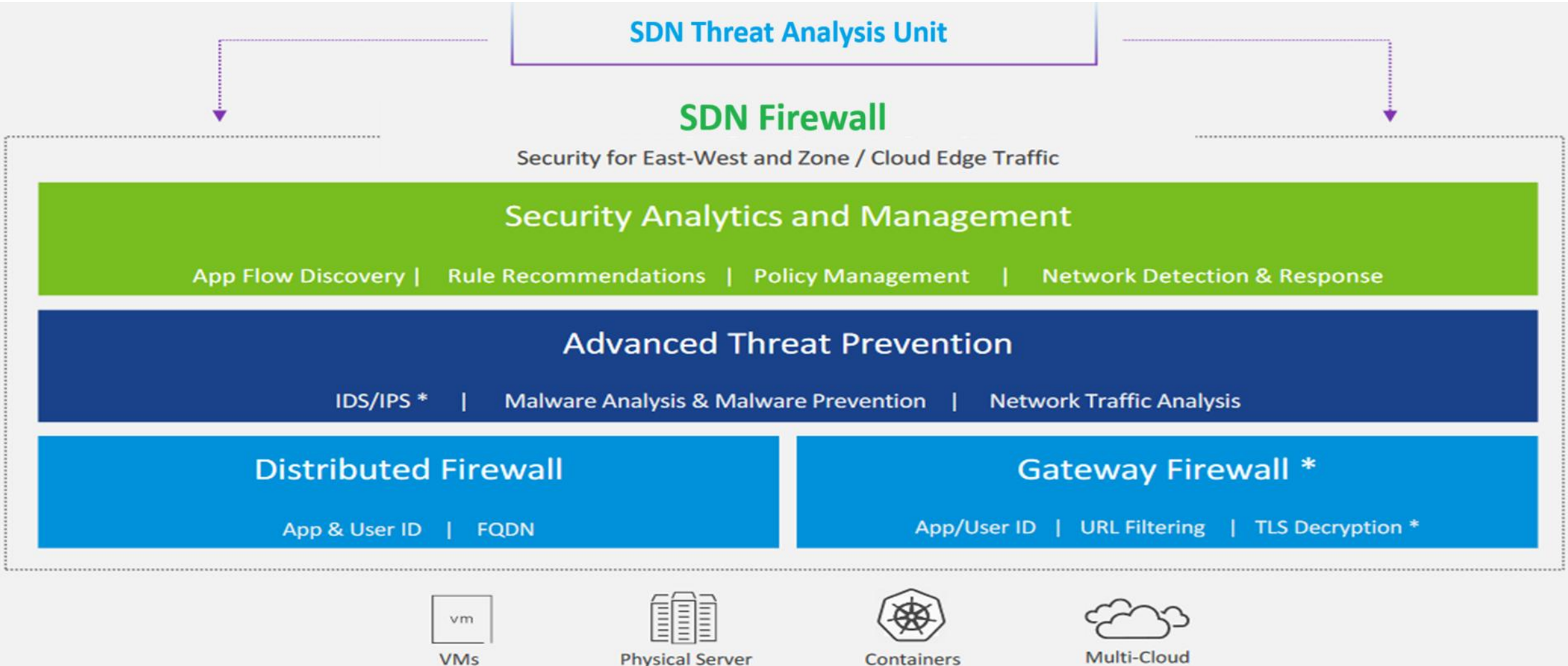
- Enhances data security through effective key management.
- Simplifies compliance with data protection regulations.



SDN Advanced threat protection

SDN Firewall

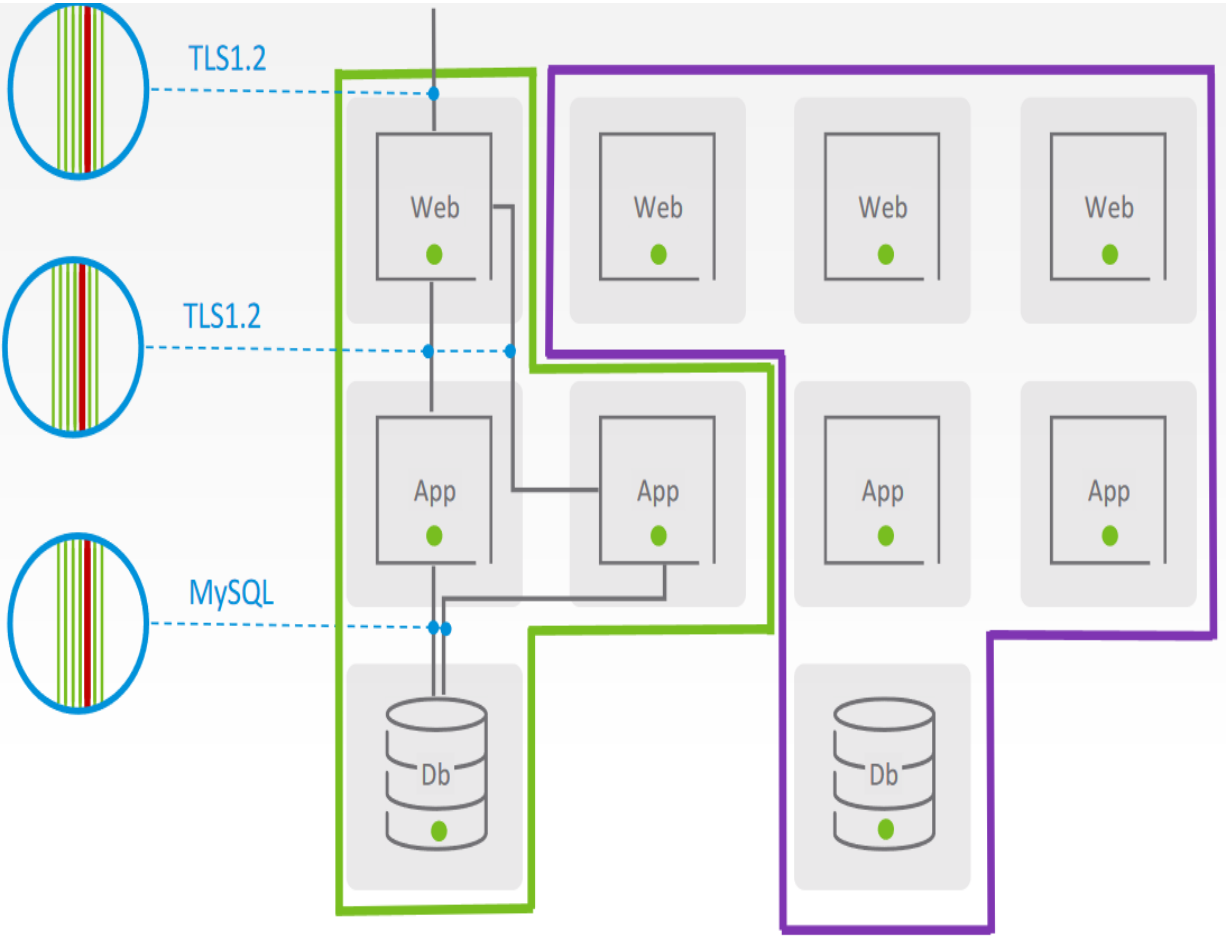
- Access Control + ATP + Analytics and Management



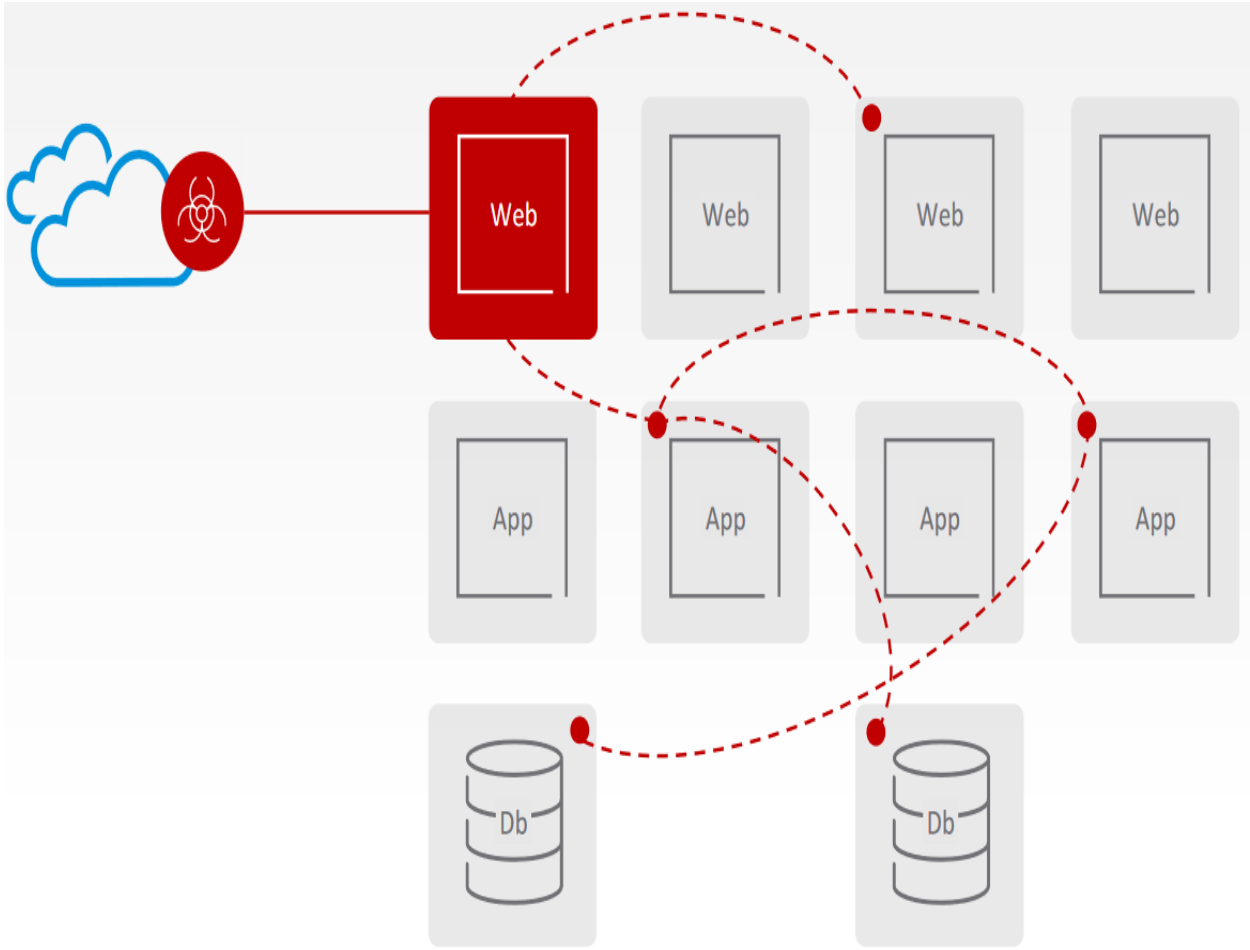
SDN Advanced threat protection

SDN Firewall

Segmentation

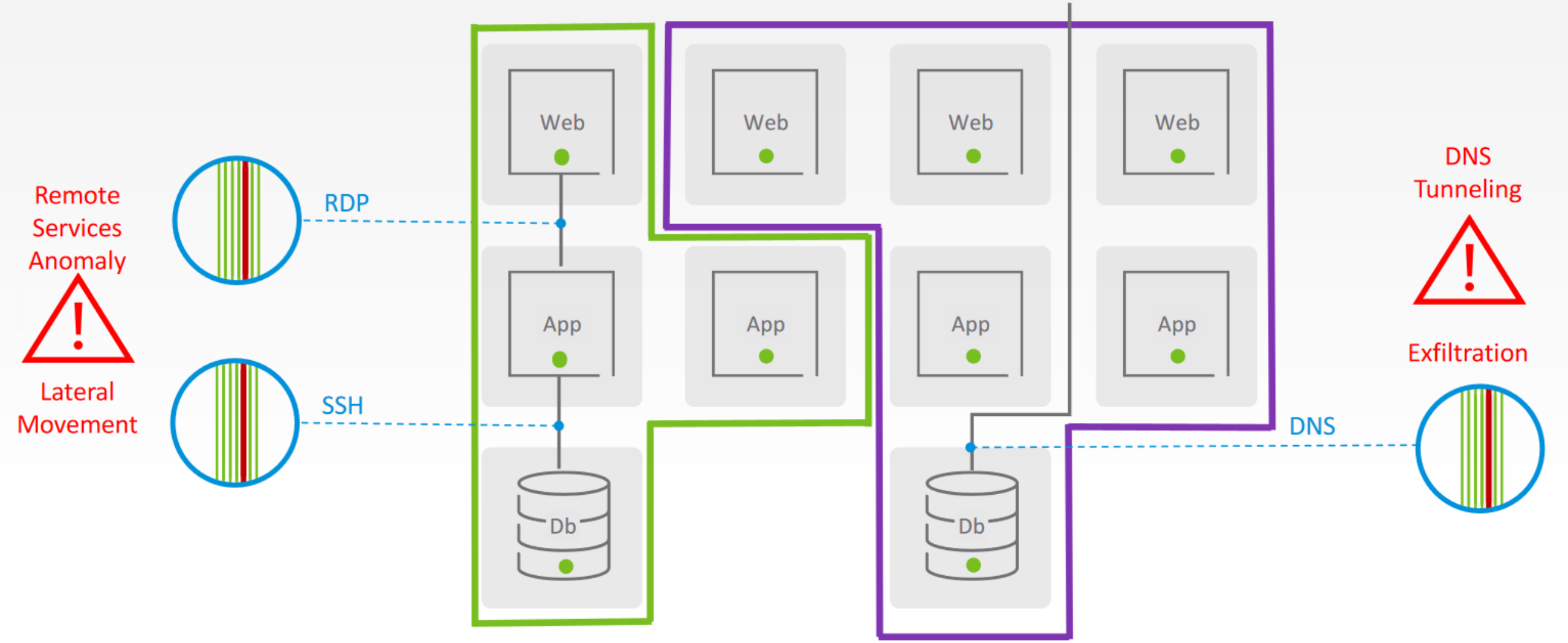


Perimeter



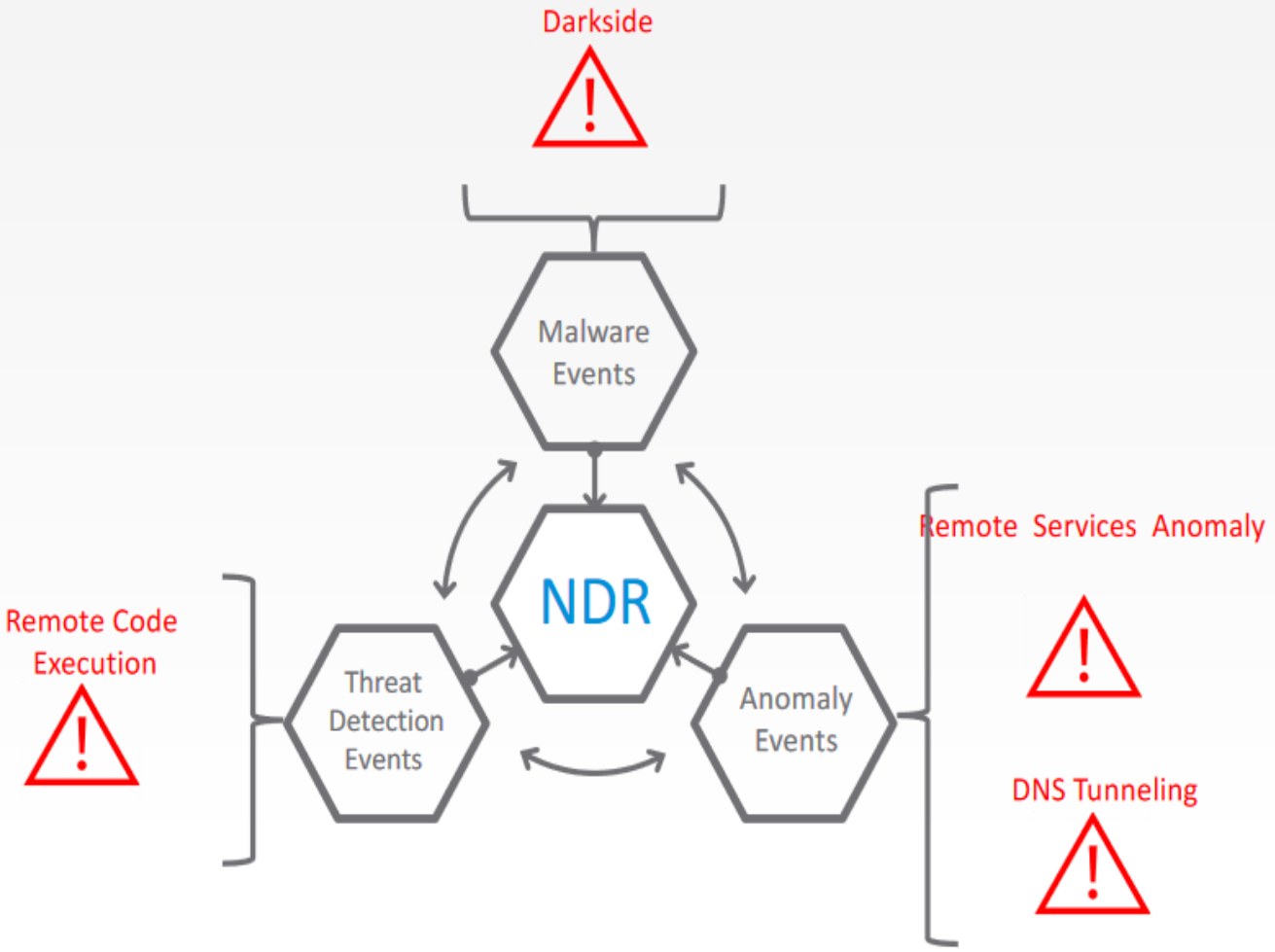
SDN Advanced threat protection

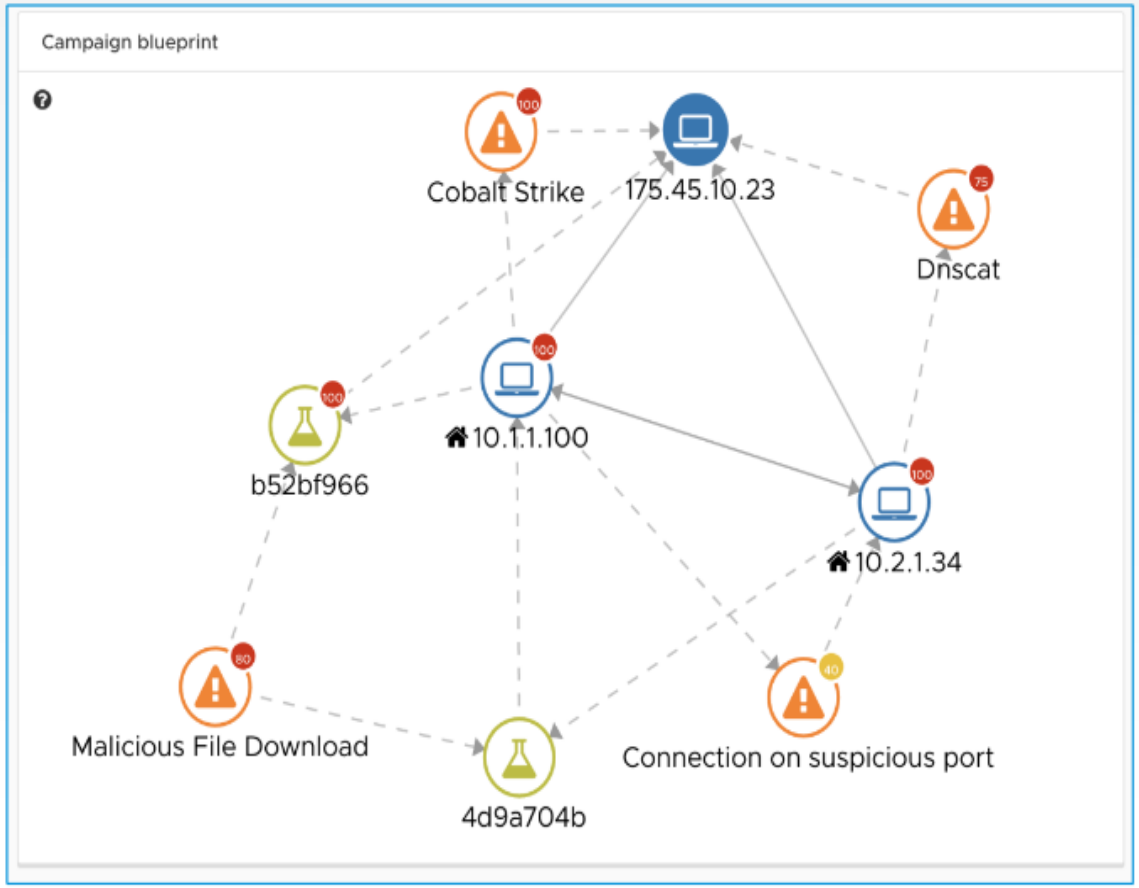
Network traffic Analysis



SDN Advanced threat protection

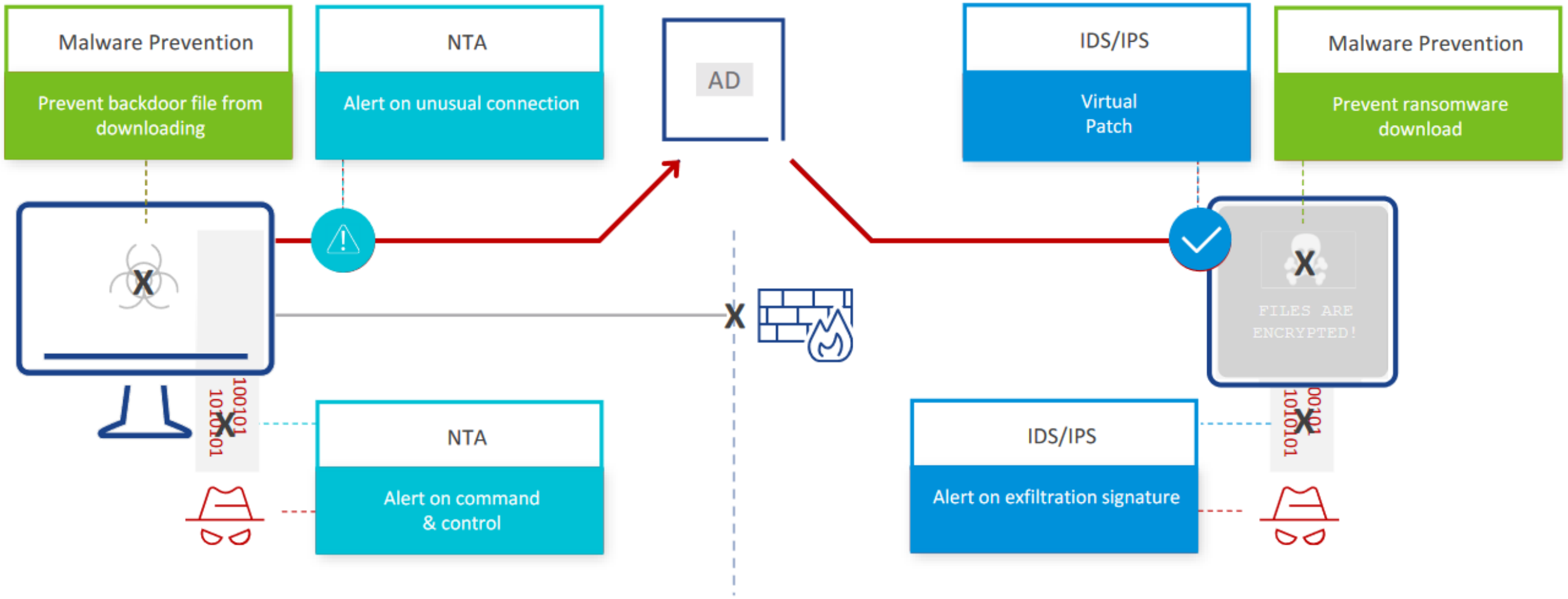
Network Detection & Response





SDN Advanced threat protection

Visibility & Enforcement across the Attack Chain



SDN Advanced threat protection

Example: post exploit tools detection

Firewall

<Block>

Unneeded communication to/between zones/apps/tiers/shared services

RDP/SMB where not needed

Use of insecure protocols

L7 protocol tunneling

IDPS

<Detect/Prevent>

Kerberos Auth. Compromises

Brute Force Login Attempts

Service/Vulnerability Scanning

Exploitation of Services

SSH connections on unusual ports

RDP Anomalies

Cobalt Strike/ Metasploit on the network

NTA

<Detect>

Suspicious LLMNR/NBT-NS Responses

Port scanning & sweeping

Suspicious remote connections like RDP

Unusual connections/ports on other internal hosts

Unusual volume of traffic dropped by FW

Malware Prevention

<Detect/Prevent>

Internal malicious file transfers

SDN Advanced threat protection

Example: Ransomware protection

Firewall

<Block>

Unneeded outbound access

Access to known bad domains

IDPS

<Detect/Prevent>

Ransomware C2/Beacon Traffic

Hostile Domain Lookup

Malicious SSL Certificate

Ransomware sending encryption key

Ransomware File Request

NTA

<Detect>

Unusual network traffic patterns

Data Download Anomalies

Beaconing

Malware Prevention

<Detect/Prevent>

Download of known malicious files

Download of unknown malicious files through static and Dynamic Analysis of File Behaviors

Analyze network behavior of ransomware to create IDPS signatures

Thank You

www.sohobcom.ye

سُحبكم sohobcom

سُحبكم لتقنية المعلومات والحلول الرقمية

Sohobcom for Information Technology and Digital Solutions