HUAWEI

HUAWEI CLOUD TechWave APAC 2024

Huawei Cloud Security Services

Benjamin Lee

Senior Cloud Security Architect

APAC CTO Office

HUAWEI CLOUD EVERYTHING AS A SERVICE

Contents

Cybersecurity Threats Are On the Rise

Attack trends

2006	2010	2015	2020	2022
Cyber attacks mainly affected infrastructure.	PRISM aroused global attention to data and privacy security.	Data has become the attack target.	Many supply chain security risks broke out.	
➢ Technologies such as web attacks, DoS attacks, and data packet spoofing were growing mature.	➢ In 2013, disclosure of ***PRISM*** (interception and backdoor implant) shocked the world.	➢ In 2017, **WannaCry** ransomware spread around the world. The virus encrypted victims' files for ransoms.	➢ **Log4J** vulnerabilities affected tens of millions of applications.	
➢ In 2009, a virus called ***Stuxnet*** severely crippled Iran's nuclear program.	➢ Occasional data breaches (**Google Street View**) raised privacy concerns.	➢ Data breaches were on the rise. In 2017, **1.5 TB** of HBO data was stolen by hackers, and data about **143 million** consumers from the largest credit investigation organization in the US was leaked. In the same year, **3 billion** Yahoo accounts were leaked, DiDi was fined **CNY8 billion** for a data breach, and SHGA Database was breached.	➢ **SolarWinds** infrastructure platform supply chain was hacked.	

Countries/Regions All Over the World Are Enacting Legislation to Improve Cyber Security

EU
EU General Data Protection Regulation (GDPR)

Russia
Information, Information Technologies and Information Protection Act

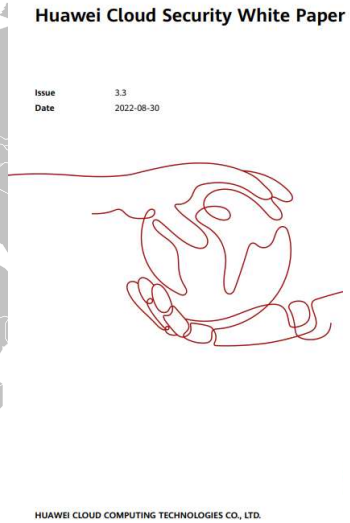
China
Cybersecurity Law

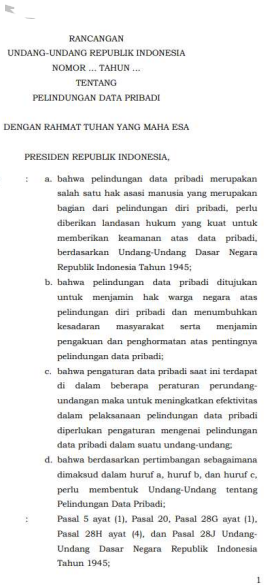
Japan
Basic Law for Cyber Security

South Korea
Personal Information Protection Act (PIPA)

Canada
Personal Information Protection and Electronic Documents Act (PIPEDA), Freedom of Information and Protection of Privacy Act (FOIPPA), and Personal Information Protection Act (PIPA)

U.S.
California Consumer Privacy Act (CCPA), Financial Services Modernization Act (Gramm–Leach–Bliley Act, GLBA), Health Insurance Portability and Accountability Act (HIPAA), Children's Online Privacy Protection Rule (COPPA), and the Clarifying Lawful Overseas Use of Data (CLOUD) Act





RANCANGAN
UNDANG-UNDANG REPUBLIK INDONESIA
NOMOR ... TAHUN ...
TENTANG
PELINDUNGAN DATA PRIBADI

DENGAN RAHMAT TUHAN YANG MAHA ESA

PRESIDEN REPUBLIK INDONESIA,

Menimbang :
a. bahwa pelindungan data pribadi merupakan salah satu hak asasi manusia yang merupakan bagian dari pelindungan diri pribadi, perlu diberikan landasan hukum yang kuat untuk memberikan keamanan atas data pribadi, berdasarkan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;
b. bahwa pelindungan data pribadi ditujukan untuk menjamin hak warga negara atas pelindungan diri pribadi dan menumbuhkan kesadaran masyarakat serta menjamin pengakuan dan penghormatan atas pentingnya pelindungan data pribadi;
c. bahwa pengaturan data pribadi saat ini terdapat di dalam beberapa peraturan perundang-undangan maka untuk meningkatkan efektivitas dalam pelaksanaan pelindungan data pribadi diperlukan pengaturan mengenai pelindungan data pribadi dalam suatu undang-undang;
d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, dan huruf c, perlu membentuk Undang-Undang tentang Pelindungan Data Pribadi;

Mengingat : Pasal 5 ayat (1), Pasal 20, Pasal 28G ayat (1), Pasal 28H ayat (4), dan Pasal 28J Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;

1

Argentina
Personal Data Protection Law (PDPL) and Confidentiality of Information Law

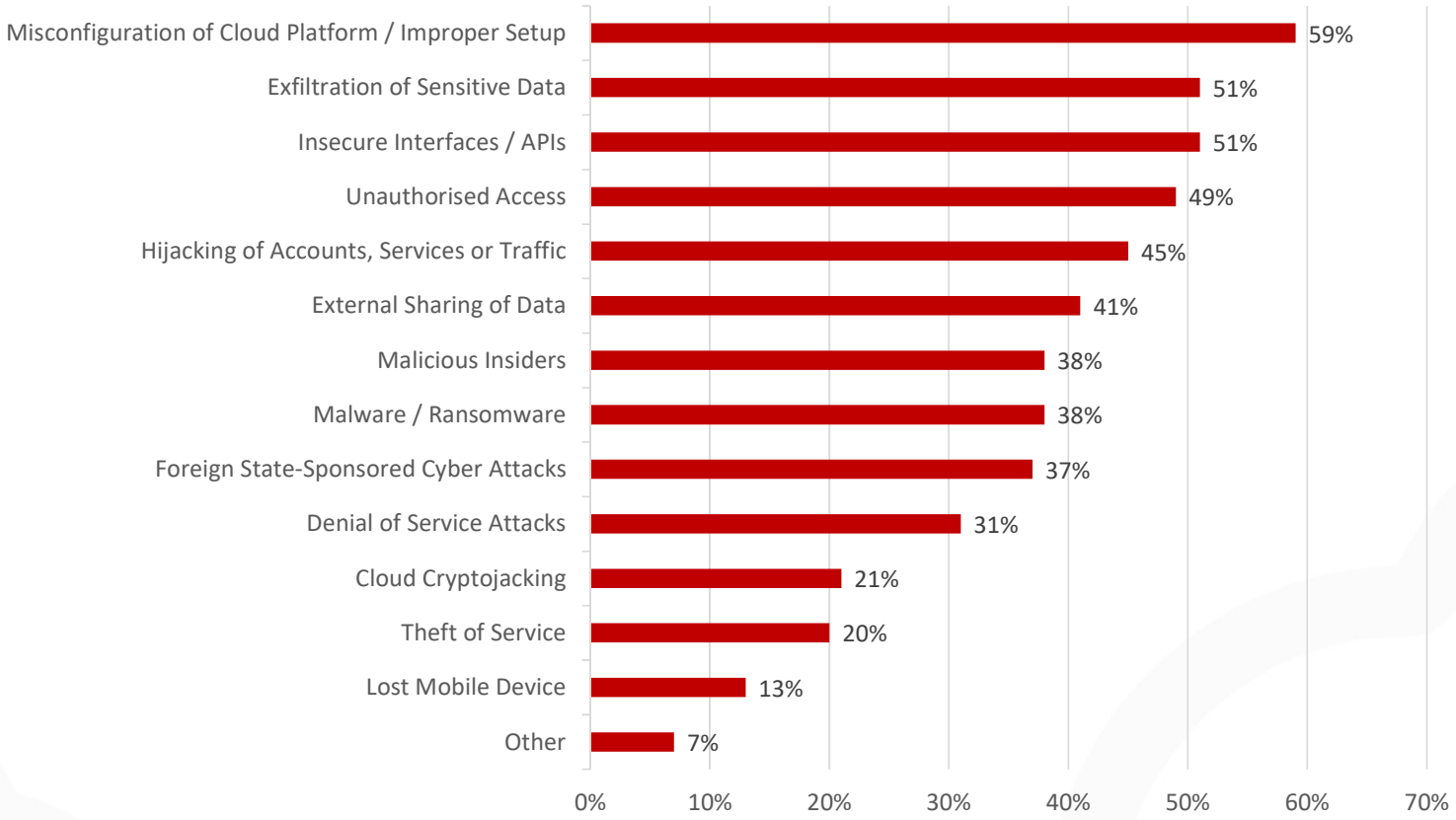
Singapore
Personal Data Protection Act (PDPA)

Thailand
Personal Data Protection Act (PDPA)

India
Digital Personal Data Protection Act

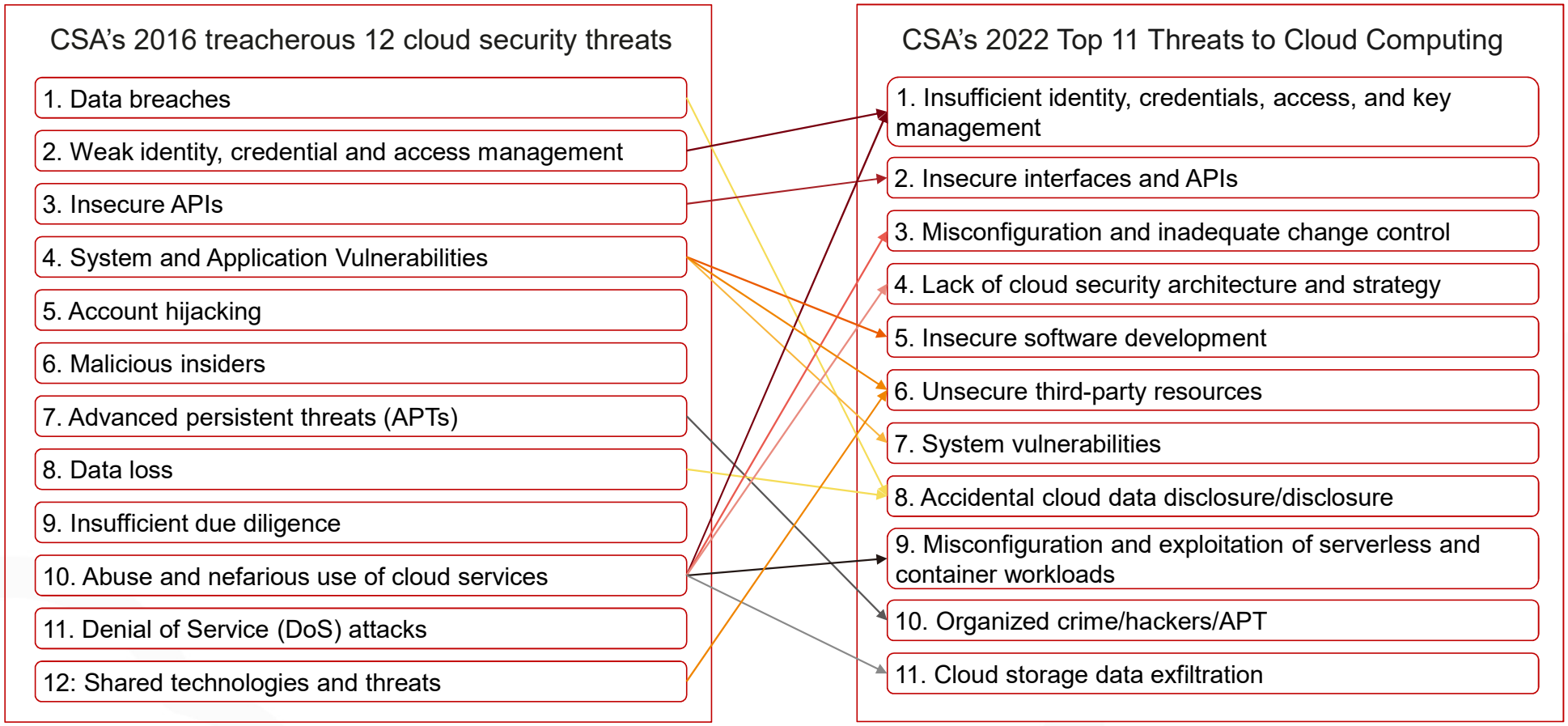
Indonesia
Personal Data Protection (PDP Law)

Cloud Security Trends



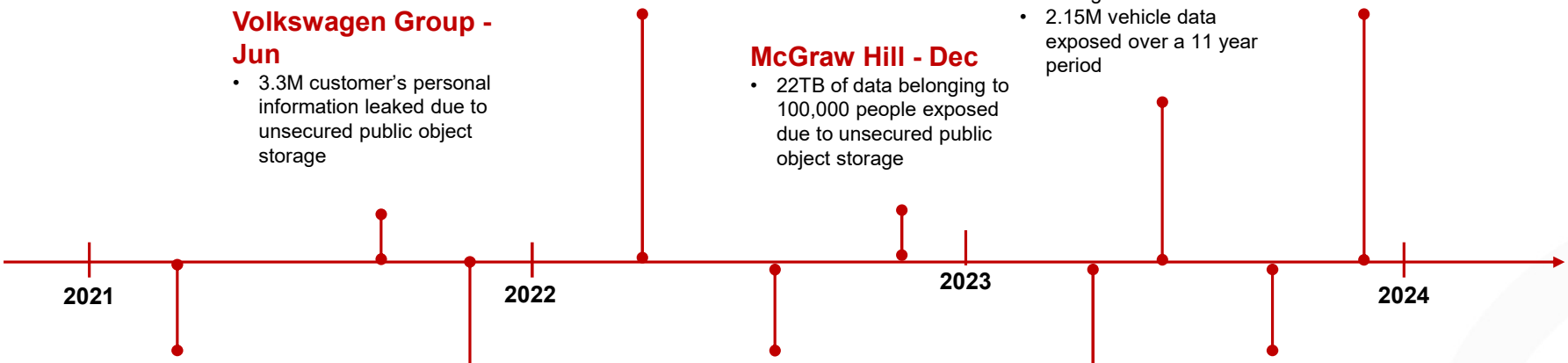
https://resources.checkpoint.com/cyber-security-resources/2023-cloud-security-report

Shift from Traditional Cloud Security Issues



https://cloudsecurityalliance.org/artifacts/the-treacherous-twelve-cloud-computing-top-threats-in-2016/
https://cloudsecurityalliance.org/press-releases/2022/06/07/cloud-security-alliance-s-top-threats-to-cloud-computing-pandemic-11-report-finds-traditional-cloud-security-issues-becoming-less-concerning/

Data Breaches Due to Cloud Misconfiguration



European Volleyball Confederation - Feb
- Images passports and identity documents belonging to journalists and volleyball players from around the world exposed due to unsecured public object storage

Volkswagen Group - Jun
- 3.3M customer's personal information leaked due to unsecured public object storage

Ghana's National Service Secretariate - Dec
- 55GB of citizen data belonging to 700,000 citizens exposed due to unsecured public object storage

Shanghai Police - Jul
- 23TB of personal information for 1 billion Chinese citizens leaked due to unsecured system

Microsoft - Oct
- 2.4TB of data belonging to 65,000 companies from 111 countries exposed due to misconfigured data bucket.

McGraw Hill - Dec
- 22TB of data belonging to 100,000 people exposed due to unsecured public object storage

Indiana University - May
- 1.3M files containing student data was exposed due to unsecured public object storage

Toyota - June
- 260,000 Customer's information exposed over a 8 year period due to unprotected public object storage
- 2.15M vehicle data exposed over a 11 year period

Microsoft - Sept
- 38TB of personal and corporate data exposed due to misconfigured access link granted full access to storage account

San Francisco's Transport Agency - Oct
- 26,000 personal information exposed due to unsecured public object storage

Contents

Huawei Cloud Has Won 130+ Security Compliance Certifications Worldwide

Security and compliance

- ISO 27001
- ISO 27017
- CSA STAR Certification
- ISO 20000
- ISO 22301
- Singapore MTCS
- SOC1 Type2
- SOC2 Type2
- SOC3

Privacy compliance

- ISO 27701
- ISO 27018
- ISO 29151
- BS 10012
- SOC2 Type1 Privacy
- Singapore PDPA
- PDPO of Hong Kong (China)
- Malaysia PDPA
- Thailand PDPA
- Indonesia PDP

Financial compliance

- PCI DSS
- PCI 3DS
- Singapore OSPAR
- PCI DSS Practice Guide
- Singapore MAS & ABS
- HKMA & SFC in Hong Kong (China)
- Malaysia BNM&SC
- Thailand BoT & OSEC
- Indonesia POJK 4, 38 & SEOJK 21

Healthcare compliance

- ISO 27799

Compliance in China

DJCP

- Public cloud O&M system (level 3)
- Public cloud operations system (level 3)
- Public cloud service system (level 3)
- Public cloud PaaS system (level 3)
- Public cloud SaaS system (level 3)

DJCP

- Public cloud high-level protection service system (level 4)
- Public cloud high-level protection PaaS system (level 4)
- Public cloud high-level protection SaaS system (level 4)

CAC www.cac.gov.cn

- Cloud computing service security assessment

ITSS®

- ITSS Cloud Computing Service Capability Assessment by the MIIT

CUDPCA

- Certification for the Capability of Protecting Cloud Service User Data

- TRUCS Gold O&M Assessment

Trusted cloud in China

TRUCS 可信云服务评估

- Trusted cloud service assessment

- Cloud server
- RDS
- Cloud cache
- OBS
- Block storage
- Cloud distribution
- Workspace
- Cloud backup
- Direct Connect
- Content security
- Message queue
- Card OCR
- GPU cloud servers
- Physical cloud server
- Cloud server security
- Local load balancing
- Security operation center
- Situational awareness platform
- Cloud-native databases
- Distributed database middleware

TRUSTED CLOUD 可信云

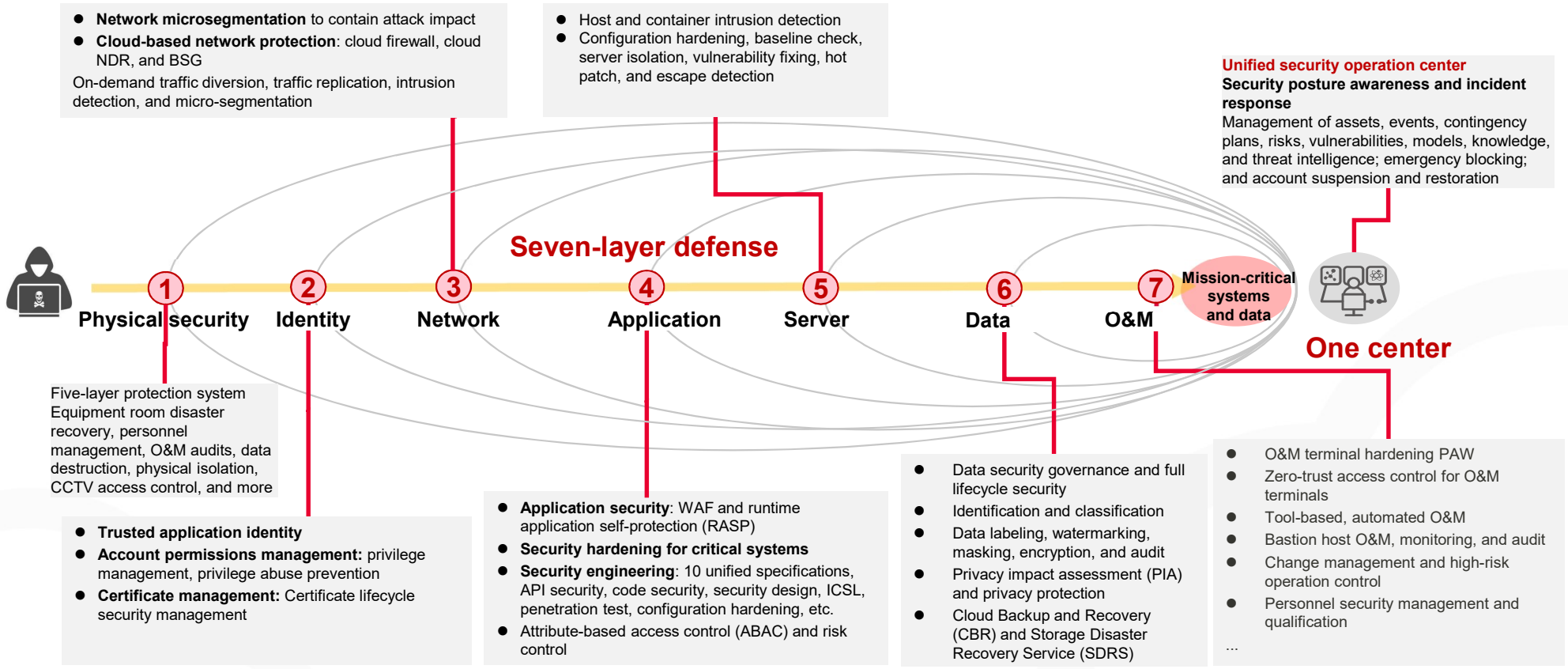
- Trusted cloud solution

- Container security
- Content security
- E-government cloud
- Hybrid cloud
- Trusted cloud container
- Open-source solutions
- Trusted e-government cloud
- Micro-platform service
- Cloud server classification
- Hybrid cloud security
- Cloud service provider credit rating
- CDN credit rating
- Shared responsibility model for security
- Edge cloud trustworthiness
- Cloud computing risk management capability
- Cloud-edge collaboration management solution

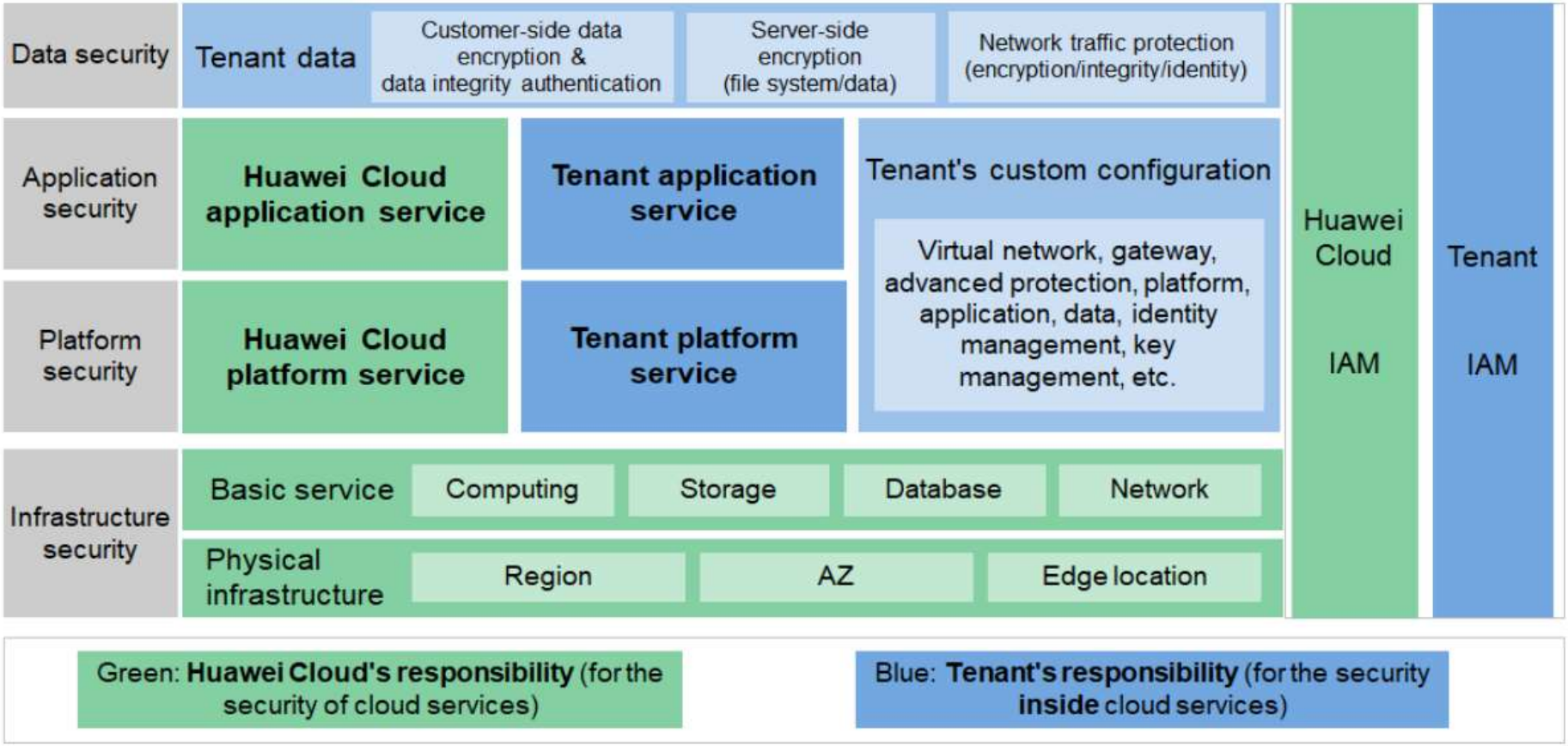
- Big data product capability evaluation

- Basic capabilities of the distributed batch processing platform
- Performance evaluation of the distributed batch processing platform
- Basic capability evaluation of distributed analytical databases
- Time series databases
- Database management tools
- Knowledge graph
- Basic capability evaluation of distributed transactional databases

Trustworthy Cloud: Seven-layer In-depth Defense + Unified Security Operation Center Makes a Cloud Platform Trustworthy and Secure



Huawei Cloud and Tenant Responsibility Sharing



Contents

Anti-DDoS

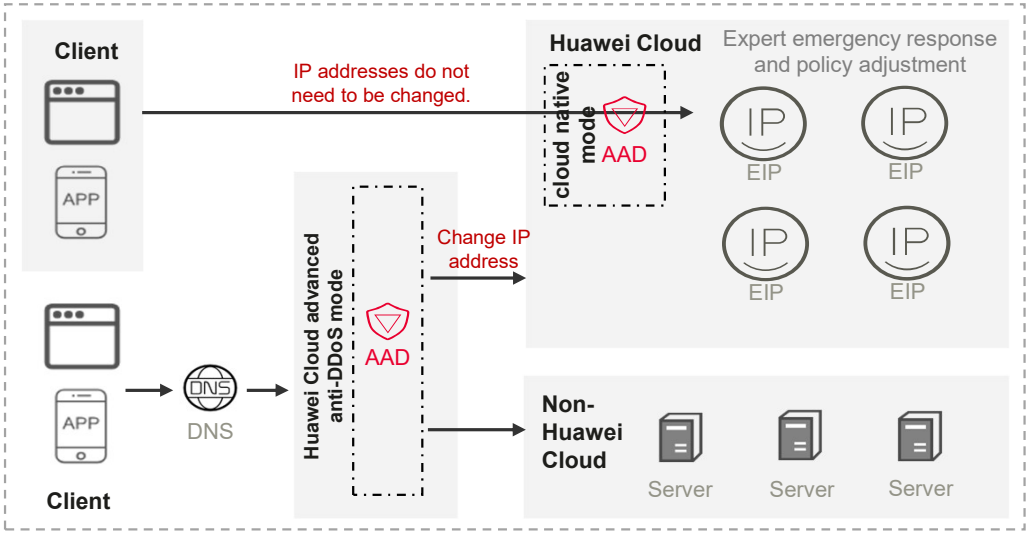
Introduction

Anti-DDoS (AAD) Service provides stronger protection from large volumetric DDoS attacks. Protect your servers, even those not deployed on HUAWEI CLOUD, with special, high-defense IP addresses so your services can weather larger and more sophisticated DDoS attacks. Advanced Anti-DDoS gives you security and reliability you can count on.

Core Functions

- **Out-of-the-box availability, no need to purchase scrubbing devices yourself.**
- **Intelligent, automated protection policies, easy setup.**
- **Large-bandwidth cleaning and defense capabilities priced on a pay-per-use basis, cost-effective.**
- **Prompt emergency response by a professional O&M team.**

Service Architecture



Highlights

1. Unlimited protection
Defend against each DDoS attack with the maximum capability without the need to predict the attack scale. By **International collaborative protection**, Uniform scheduling of **international AAD nodes** for collaborative protection with **IP Anycast**; easily defending against **TB-level attacks** due to **near-source scrubbing**

2. Distributed scrubbing for DDoS
More than 10 scrubbing Centers already deployed. Integrate international traffic scrubbing centers to process attack traffic from all over the world.

3. Intelligent defense for scenario-specific services
Accurately defend diverse service scenarios based on protection practices. **Intelligent CC defense, Over 60** defense models (packet rate, concurrent connection, application type, and protocol status), periodic learning of service traffic, and **smart adjustment** of defense threshold

Notice: ① belongs to East-west firewall, expected to be released in 2024Q1

CFW

Scenarios & pain points

Threat and risk detection

- Zombie, Trojan, and worm attacks
- Unauthorized connections from the internal to the external network
- Inter-VPC threat penetration

Business elasticity

- Support for ultra-high traffic
- Adapted to tenant asset and VPC changes Service reliability

Difficult to configure and use

- Complex manual installation and deployment
- Difficult to trace unauthorized external connections
- Complex problem locating operations

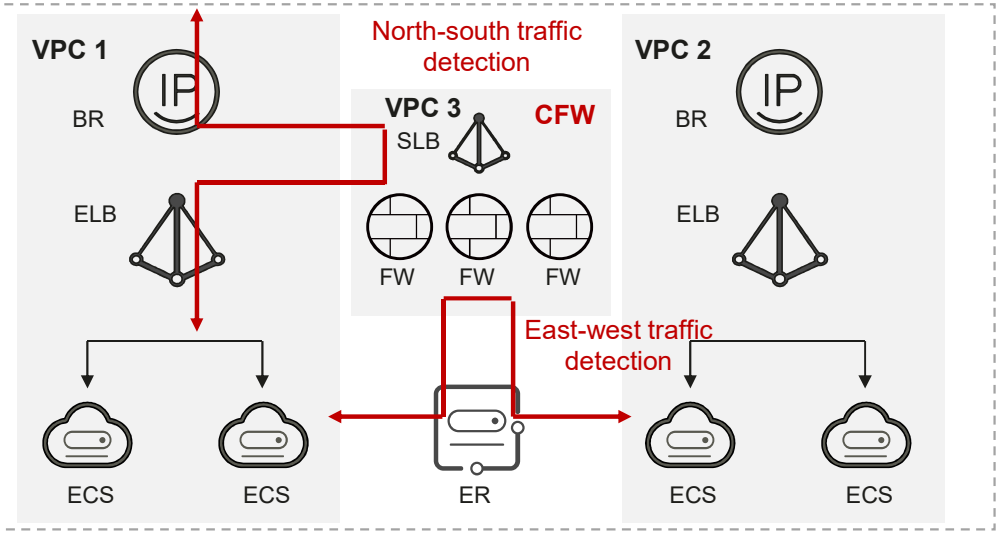
Benefits

Cloud assets are protected by comprehensive cloud-native capabilities that are **updated in real time.**

Pay-per-use, elastic resources can be scaled out to handle peak hour traffic, **costing 30% less.**

Security service provisioning and O&M are more efficient, and O&M OPEX is **reduced by 50%.**

Service Architecture



Advantages

Intelligent defense

- The intrusion prevention engine detects and blocks malicious traffic in real time based on Huawei Cloud intelligence.
- Protection for inbound traffic, outbound traffic, and inter-VPC traffic

Flexible scaling

- No upper limit on key performance and specifications
- Automatic synchronization of tenant assets and VPC resources
- Cluster deployment achieving high reliability

Simplified applications

- One-click provisioning; deployment within minutes
- Graphical web UI, simplified asset management, O&M management, and threat source tracing

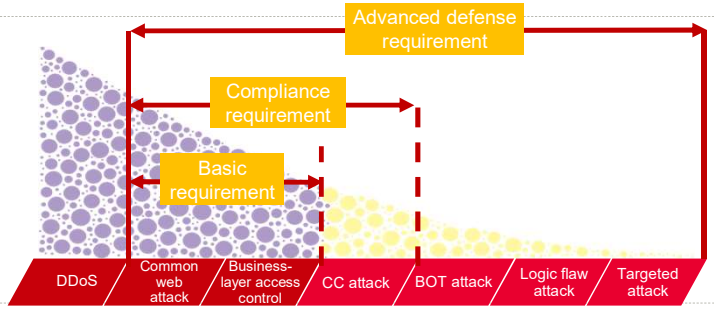
Notice: ① belongs to East-west firewall, expected to be released in 2024Q1

WAF

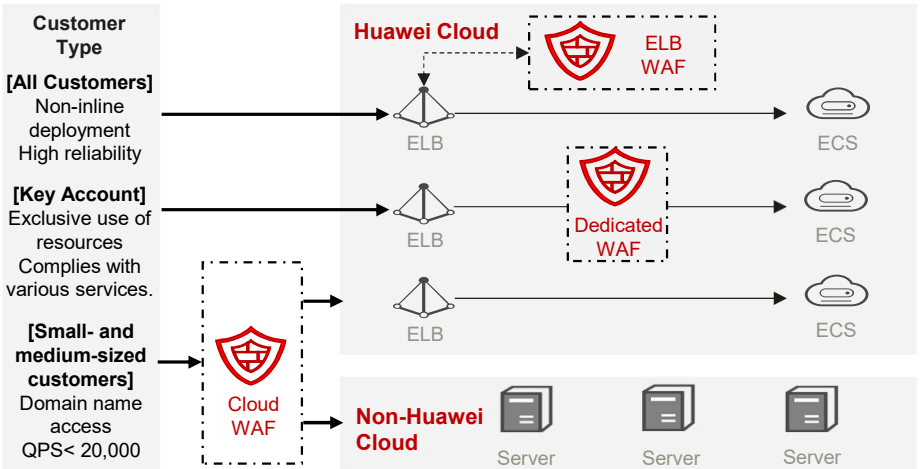
Introduction

Web Application Firewall (WAF) is expertly designed to keep your website safe and secure. It comprehensively examines website service traffic to accurately identify malicious requests and filter attack traffic, ensuring top-class system security and stability for your data

Core Functions



Service Architecture



Highlights

- WAF helps defend against high-risk zero-day vulnerabilities within 2 hours.
- WAF protects workloads from abnormal traffic attacks and ensures 24/7 service continuity.
- WAF can detect OWASP top 10 threats and uses a Huawei-patented technique that prevents threats from bypassing security controls, improving the detection rate by 40%.
- WAF mitigates security risks caused by botnets, such as credential stuffing attacks, brute-force attacks, data breaches, and bonus hunting behaviors.
- WAF enables precise protection with customizable enterprise-grade protection policies, including custom alarm pages, composite rules for CC attack prevention, and IP address blacklists.

Notice: ① belongs to East-west firewall, expected to be released in 2024Q1

HSS

Host Security Service (HSS) provides Comprehensive Protection for Cloud Servers with Threat Prevention, Detection, and Operations

Core Functions

Asset management

HSS identifies security assets, software vulnerabilities, and key configurations of servers, effectively reducing the attack surface by 90%.

Vulnerability management

HSS automatically identifies **server and application vulnerabilities** and provides a rich selection of **up-to-date** vulnerability libraries. It also enables you to fix vulnerability and verify results in just a few clicks.

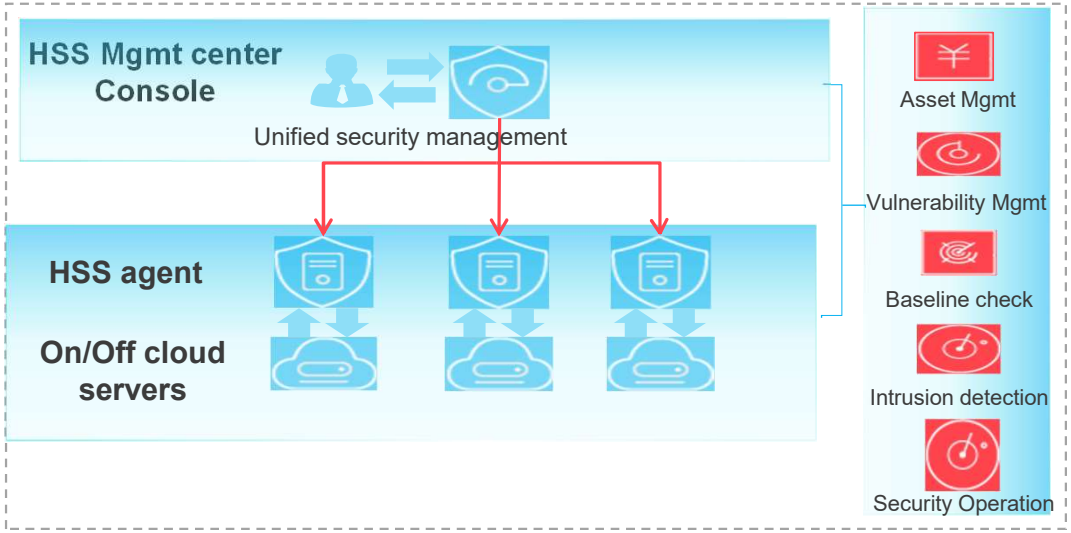
Baseline check

HSS uses **China's DJCP MLPS protection requirements and CIS standards** for check, and has a **rich selection of baseline rules**. HSS **weak password detection is available for many applications and helps you quickly fix unsafe settings and customize your detection rules**.

Intrusion detection

HSS leverages slow and fast brute-force attack detection algorithms and network-wide blacklisted IP addresses to detect and prevent brute-force attacks against accounts.
HSS can detect typical attacks against cloud servers with **precise detection** and **low false positives**, **monitoring system and network behavior**.

Service architecture



Highlights

Asset management: HSS helps customers manage servers and OS images. It can manage assets by group, such as port, account, auto-start asset groups.
Vulnerability management: HSS can detect vulnerabilities in OSs and Web-CMS, including image and emergency vulnerabilities, and provide fixes.
Baseline check: HSS can detect unsafe baseline settings on servers, such as detection of weak passwords in OSs and Tomcat,Nginx, SSH these three applications. It also provides suggestions to improve security.
Intrusion detection: HSS can detect advanced threats, such as privilege escalation, unauthorized external connections, and high-risk commands. It also supports two-factor authentication.
Security Operation: HSS provides alarm notifications and weekly/monthly report.
Unified multi-cloud management: HSS can manage hundreds of thousands of servers running mainstream OSs, such as Linux and Windows, no matter what cloud they are deployed and which architectures (x86 and Arm) they are using.

HUAWEI

DSC

Service Overview

Data Security Center (DSC) is a next-generation cloud data security platform. It helps you to classify data, identify risks, mask sensitive data, and track data sources through watermarks. DSC gives you an insight into security status in all phases of data lifecycle management and presents status of your data assets in an intuitive way.

Core functions

Classification

- ✓ Automatic identification
- ✓ AI and expert knowledge bases
- ✓ A range of templates for regulations can be customized for GDPR, PCI DSS, and HIPAA

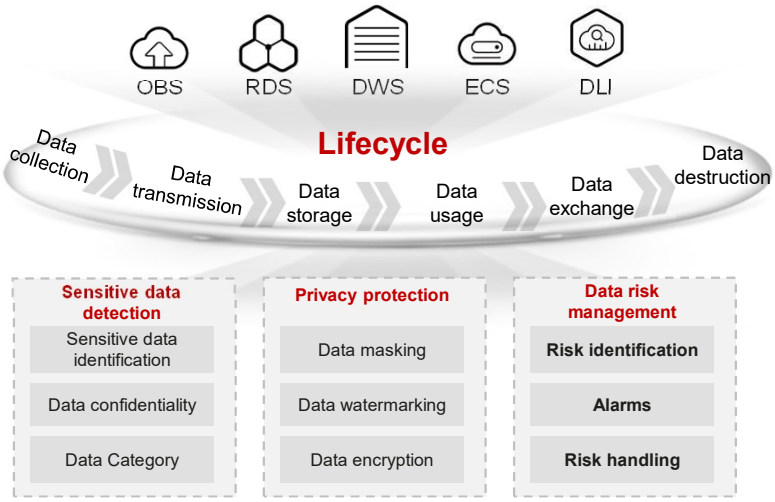
Masking

- ✓ APIs
- ✓ Over 20 preset masking rules
- ✓ Custom masking rules

Watermarking

- ✓ Watermarking injected to data robustness

Service architecture



Advantages

Intuitive display	Intuitive data security status, distribution, and risks
Unified management	You can manage data by levels and classifications, adjust encryption methods, and control data exchanges.
Data tracing	Both structured and unstructured data can be traced.
Open capabilities	You can call DSC APIs to use our data security functions.

DBSS

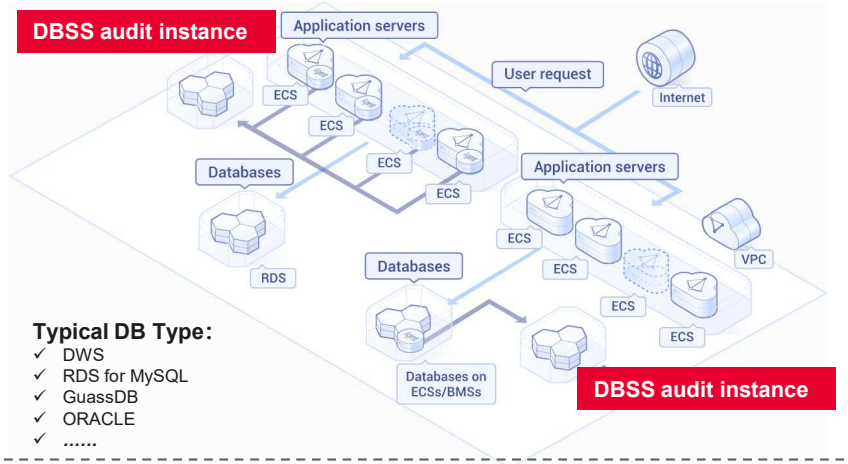
Introduction

Database Security Service (DBSS) provides the database audit function in out-of-path mode. It records user access to the database in real time, generates fine-grained audit reports, and generates alarms on risky behaviors and attack behaviors in real time. The database audit service generates compliance reports that meet data security standards (such as Sarbanes-Oxley) to locate internal violations and improper operations, thus ensuring data asset security.

Core functions

Fine-grained behavior audit	Security risk alarms	Multi-dimensional analysis	Fine-grained reports
Record and correlate access behaviors at the application and database layers.	Detect database risks and report alarms based on SQL command characteristics and risk levels.	Behaviors Sessions Statements	Session behavior report Risk distribution report Compliance report

Service architecture



Typical DB Type:

- ✓ DWS
- ✓ RDS for MySQL
- ✓ GuassDB
- ✓ ORACLE
- ✓ .....

Advantages

Simple deployment	Database audit is easy to use, and is deployed in out-of-path mode. O&M operations do not affect services. You can audit DWS instances without installing the agent.
Efficient analysis	You can import tens of thousands of data records per second, store mass data, and process hundreds of millions of data records within seconds.
Quick recognition	Comprehensive SQL parsing and accurate protocol analysis
Compliance with standards	Database audit complies with DJCP L3 and laws in and outside China, such as the cybersecurity law and SOX.

KMS

Service Overview

Key Management Service (KMS) is a secure, easy-to-use service that uses HSMs to protect your keys. It seamlessly interworks with other services to protect service data and can be used to develop encryption applications.

Core functions

Key Lifecycle Management

- ✓ Create, view, enable, disable, schedule deletion, cancel deletion customer master key
- ✓ Modifying the alias and description of the customer master key

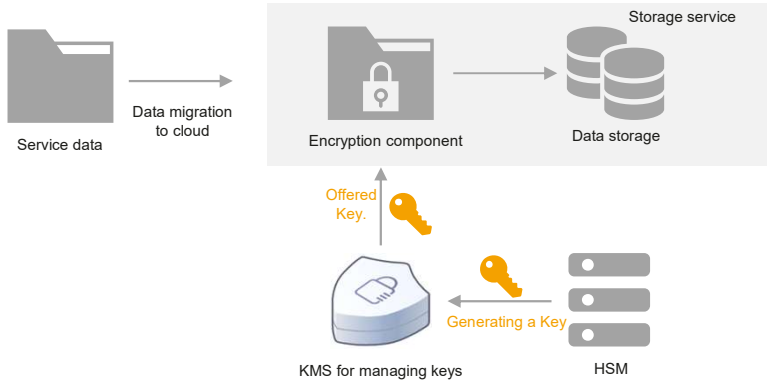
Cloud service encryption

- ✓ Supports encryption for storage cloud services, such as OBS, EVS, IMS, SFS, RDS, DDS, and DWS.

Key rotation

- ✓ Extensive reuse of encryption keys poses risks to encryption key security. KMS key rotation ensures encryption key security.

Service architecture



Advantages

Interconnecting with KMS **45 +**	Covers storage, big data, databases, and IoT.
KMS performance for a single customer **3000TPS**	The API invoking performance of a single customer is four times higher than the industry average.
Local data encryption **SDK**	Quickly build local/client encryption capabilities, support AES, RSA, and ECC encryption algorithms, and support cross-region key DR through key rings.

CBH

Service Overview

Cloud Bastion Host (CBH) helps with fine-grained management of users, resource accounts, and access processes by establishing one-on-one mappings between administrator accounts and resource accounts. It helps you establish a security management system that features pre-event planning, in-event control, and post-event audit, reducing the risks of data leakage and IT accidents caused by internal threats.

Core functions

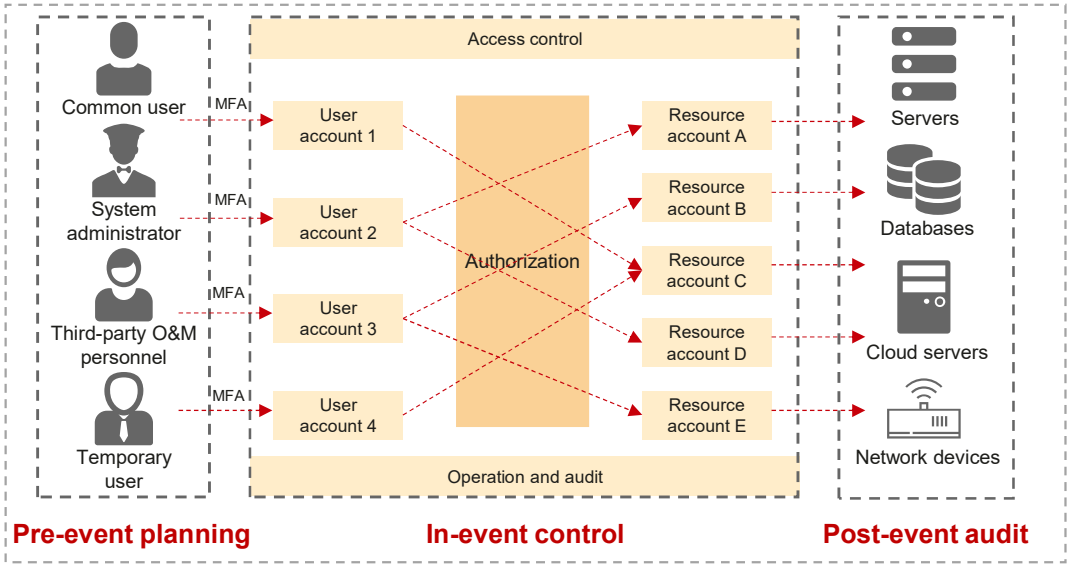
User management
- ✓ User management
- ✓ Role management
- ✓ MFA
- ✓ Access policies

Resource management
- ✓ Password hosting
- ✓ Password change rules
- ✓ O&M authorization
- ✓ Application release

Access control
- ✓ SSO
- ✓ Command interception
- ✓ Two-level authorization
- ✓ Ticket management

Operation audit
- ✓ Real-time monitoring
- ✓ Operation recordings
- ✓ Command audit
- ✓ Report analysis

Service architecture



Highlights

Support for H5 O&M with a web browser
CBH makes it possible for users to perform O&M anytime, anywhere, using any device using mainstream browsers without installing clients or plug-ins.

Application release extension
CBH gives you the ability to use a single point of entry to manage different application resources, such as databases, web applications, and client programs. It also supports OCR-based O&M audit, enabling you to convert graphical operations into text files for audit.

Extensive permissions control
You can set strict access permissions for resources such as ECSs to ensure that only authorized users can gain access.

HUAWEI

SecMaster

Service Overview

SecMaster is a next-generation cloud-native security operation center. Backed by Huawei's over three decades of security expertise, SecMaster provides a wide range of capabilities, such as cloud asset management, security posture management, security incident detection, security information and incident management, security orchestration, risk mitigation, and automatic response to and closure of security incidents

Key functions

Risk Prevention & Situational Awareness

- ✓ Baseline checks help you meet the standards of cloud security best practices.
- ✓ Vulnerability management helps you easily discover and fix vulnerabilities in your system.
- ✓ Situational awareness helps you learn the attack history, the present, and the future.

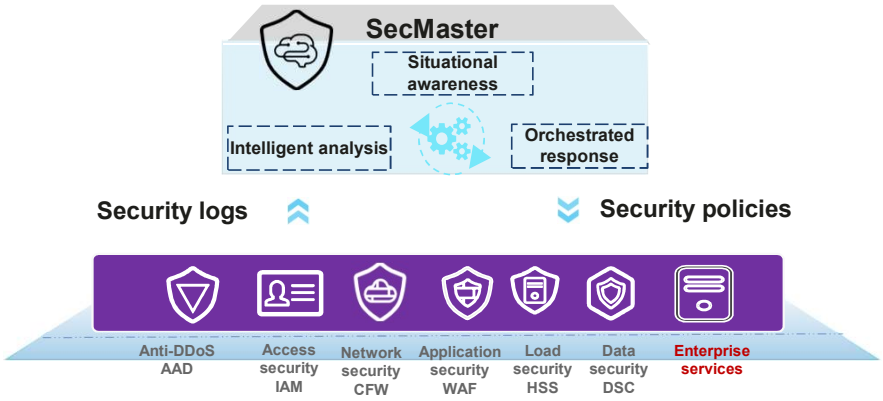
Threat Management

- ✓ Threat detection models are used to detect threats and generate alarms.
- ✓ A wide variety of security response playbooks automate alarm analysis and handling.

Security Orchestration

- ✓ Security response playbooks can be orchestrated through drag-and-drop to adapt to your service requirements.
- ✓ You can also flexibly extend and define security operation objects and interfaces.

Service architecture



Highlights

Comprehensive awareness	Unified management of assets on and off the cloud, PB-level logs + search in seconds **A library of 100,000+ vulnerabilities, and 10,000+ security risk baselines**
Intelligent analysis	**300+ empirical models (100+ AI detection models)** for effective threat management
Efficient handling	**100+ playbooks**, global collaboration, and **automatic response to 99% alarms within 5 minutes**

HUAWEI

EdgeSec

Service Overview

Edge Security (EdgeSec) is a security service that protects the edge nodes of Huawei Cloud Content Delivery Network (CDN). It provides anti-DDoS, CC attack protection, and Web Application Firewall (WAF) on edge nodes.

Key functions

Web Protection

- ✓ Full support for OWSAP threat protection
- ✓ 0-day vulnerability fixing within 2 hours and automatic signature database update
- ✓ Unique anti-escape detection engine, precise control

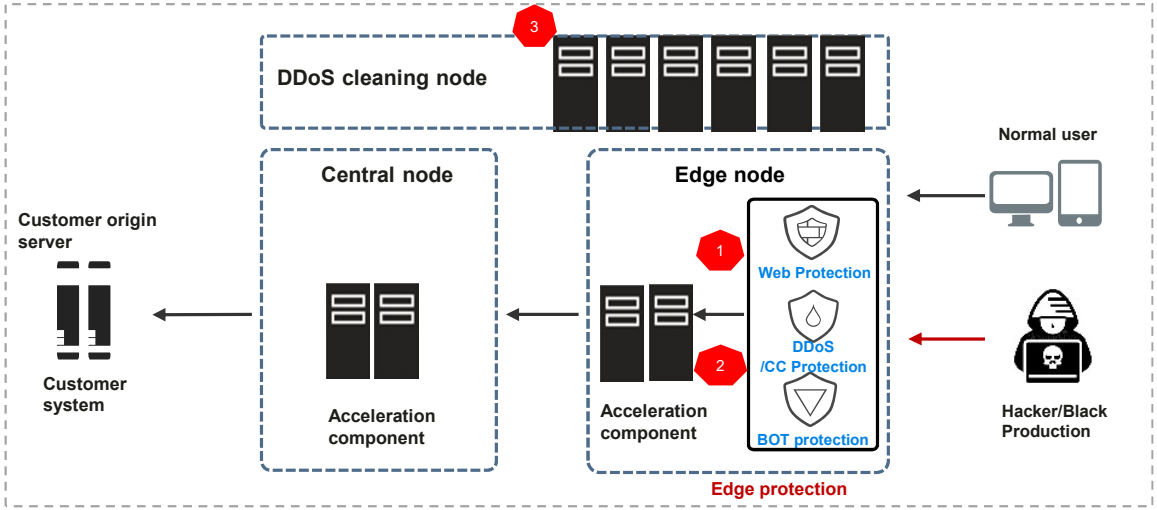
Access Control Engine

- ✓ Supports area blocking and precise blocking of high-risk areas.
- ✓ Precise access control and flexible definition of blocking conditions
- ✓ Flexible CC protection mechanism

Feature Matching

- ✓ Blocking BOT traffic at the edge, reducing the load on the web server
- ✓ Feature Matching and JS Challenge Quick Crawler Identification
- ✓ Advanced BOT Management Function from River Security

Service architecture

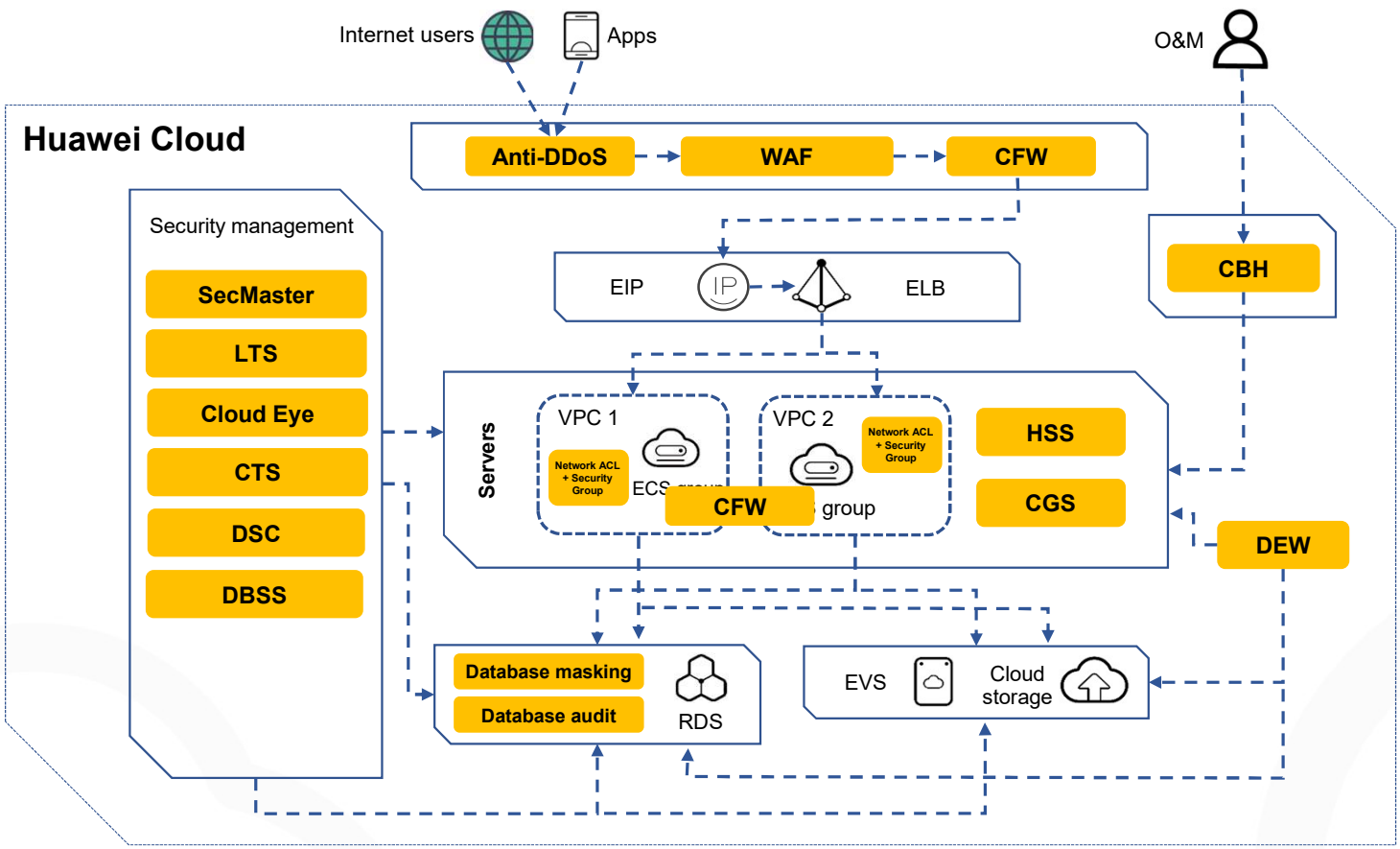


Highlights

Ultra-Large Protection Bandwidth	The global anti-DDoS bandwidth exceeds 15 Tbit/s, easily defending against heavy-traffic DDoS attacks at the network and application layers.
Precise threat identification	Built-in semantic analysis engine and regex engine which can automatically decode common code .
Anti-Crawler Protection	Dynamically analyzes and accurately identifies over 700 types of crawler behavior based on data risk control and bot identification systems.

HUAWEI

Huawei Cloud Security Design Reference



Secure communication network

① The Anti-DDoS service is used to defense against DDoS attacks.
② WAF is used to defend against web attacks.
③ SSL certificates are used for communication encryption.

Security zone border

WAF is deployed between Internet borders and VPCs.

Secure computing environment

① HSS and CGS are deployed.
② Network ACLs and security groups are used for access control within a VPC.
③ Data Security Center manages data security across the data use lifecycle.
④ Data encryption is enabled for storage by default.
⑤ Database Security Service is deployed for the security of key databases.
⑥ The Cloud Backup Service is used to prevent data loss.

Security management center

① SA is used to ensure cloud resource security.
② Cloud resources are periodically scanned for vulnerabilities.
③ Log Tank Service (LTS), Cloud Trace Service (CTS), and Cloud Eye are used to manage cloud resources.
④ CBH is used for O&M.

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home and organization for a fully connected, intelligent world.

HUAWEI

HUAWEI CLOUD TechWave APAC 2024