腾讯云

08 Introduction to Tencent Cloud Security Products

腾讯云

CONTENTS

Course Objectives

- At the end of this course, you will have a better understanding of:
  - The industry's common cloud security systems, standards, and technologies.
  - The features, technical principles, advantages, and billing methods of Tencent Cloud security products.

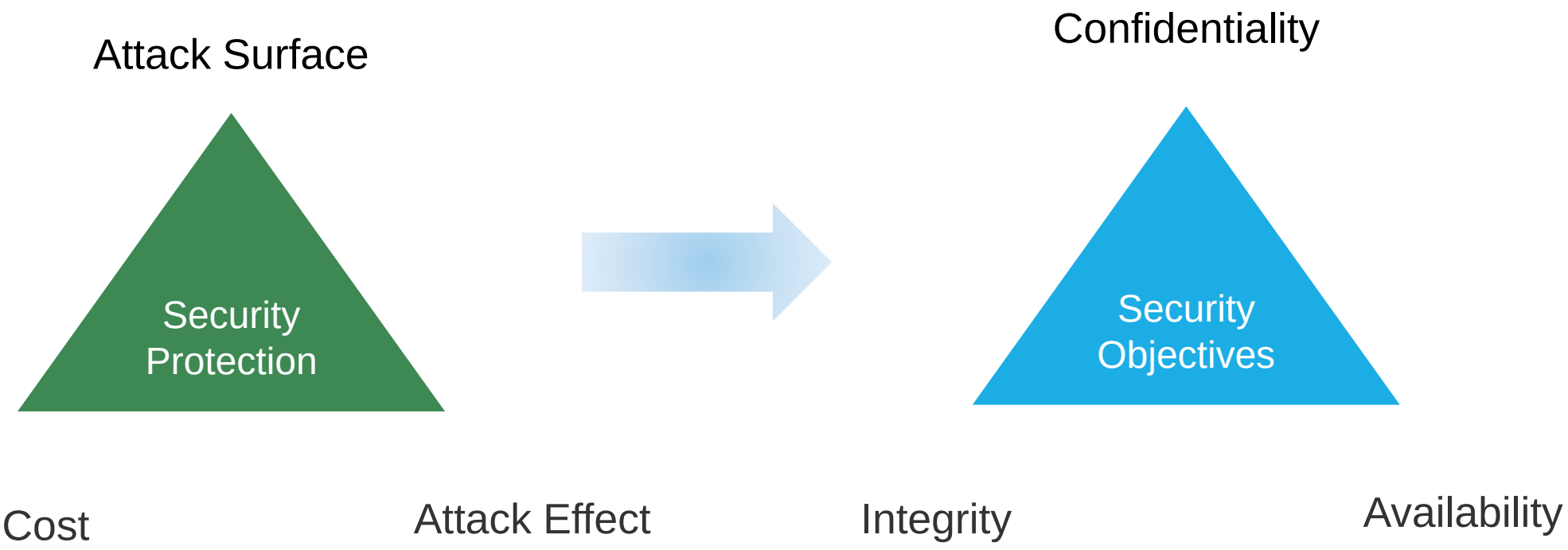
腾讯云

CONTENTS

Chapter 1

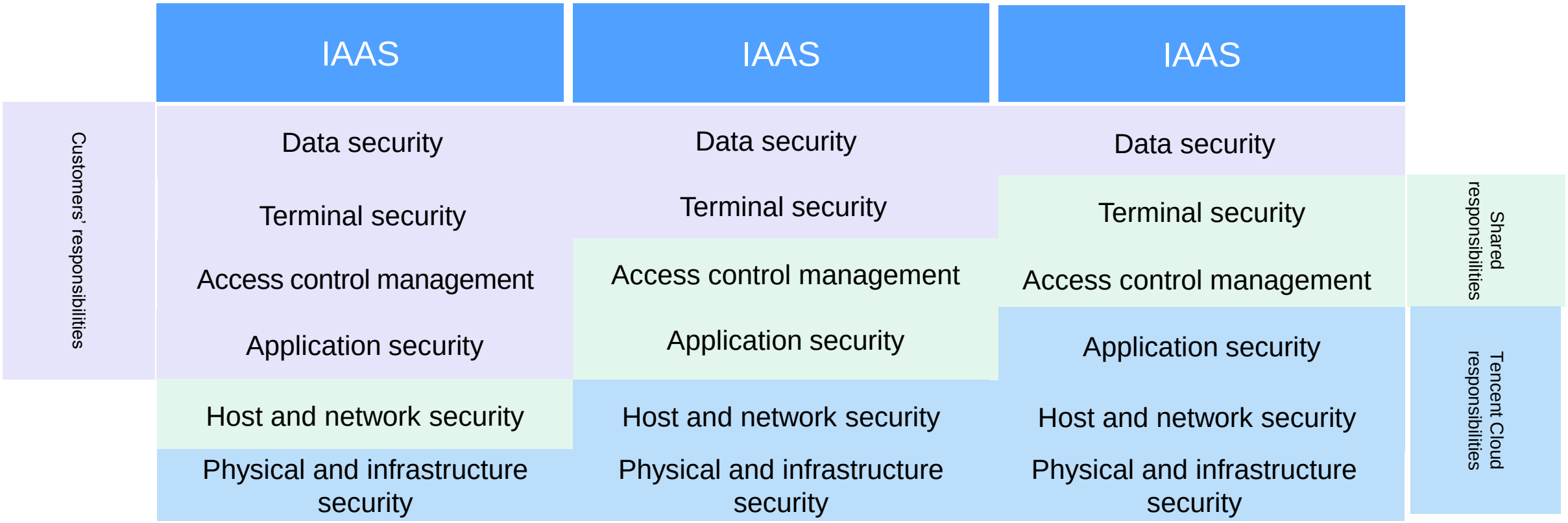
Chapter 1 Cloud Security Systems and Standards

1.1 Basic Principles of Cloud Security



Tips: Security measures prioritize prevention. Back up your data in advance.

1.1 Basic Principles of Cloud Security (Continued)



Shared Responsibility Model

1.2 Cloud Security Standards and Technologies

Cloud Security Standards and Technologies	
1	Cloud Security Alliance (CSA) Security Guidance v4.0
2	Classified Protection Standard 2.0
3	Trusted Cloud Service Certification
4	Gartner Top 10 Security Projects

1.2.1 Cloud Security Alliance (CSA) Security Guidance v4.0

- **CSA4.0 defines 2 categories and 13 domains, describing the strategic and tactical security difficulties of a cloud environment and corresponding measures.**

- **Governance (strategic)**
  - Governance and Enterprise Risk Management
  - Legal Issues: Contracts and Electronic Discovery
  - Compliance and Audit Management
  - Information Governance

- **Operation (tactical)**
  - Management Plane and Business Continuity
  - Infrastructure Security
  - Virtualization and Containers
  - Incident Response
  - Application Security
  - Data Security and Encryption
  - Identity, Authorization, and Access Management
  - Security as a Service (SaaS)
  - Related Technologies

1.2.2 Classified Protection Standard 2.0

- **Management requirements:**
  - Security management unit and personnel
  - Security construction management
  - Security OPS management
  - Security policy and management system
- **Technical requirements:**
  - Logistics and environment security
  - Network and communication security
  - Device and computing security
  - Application and data security

1.2.3 Trusted Cloud Service Certification

- Trusted Cloud Service (TRUCS) is the only recognized certification system for cloud services in China.
- 16 metrics and 3 categories cover 90% of the problems in cloud service providers' SLAs.
- Tencent Cloud provides many TRUCS-certified services and is among the first to pass TRUCS' Gold Class Operations Special Assessment

Data Security	Service Quality	User Right Protection
1. Data persistence 2. Data migration 3. Data confidentiality 4. Data transparency and privacy 5. Data auditability	6. Service functions 7. Service availability 8. Service resiliency 9. Failure recovery 10. Network access performance 11. Accuracy of service usage calculation	12. Service changes 13. Termination clauses 14. Service indemnity clauses 15. User constraint clauses

1.2.4 Gartner Top 10 Security Projects

腾讯云

Gartner Top 10 Security Projects

Security Field	2017	2018	2019
IAM		Privileged access management (PAM)	Privileged access management (PAM)
Cloud Security	Software-defined perimeter (SDP)	Software-defined perimeter (SDP)	
	Cloud access security broker (CASB)	Cloud access security broker (CASB)	Cloud access security broker (CASB)
	Microsegmentation	Microsegmentation	
	Cloud workload protection platform (CWPP)		
	Container security		Container security
		Cloud security posture management (CSPM)	Cloud security posture management (CSPM)
Endpoint Security	Endpoint detection and response (EDR)	Detection and response - endpoint protection platform (EPP) + endpoint detection and response (EDR)	Detection and response - endpoint protection platform (EPP) + endpoint detection and response (EDR)
		Application control for server workloads	
Network Security	Remote browsers		
	Fraud detection	Detection and response - fraud detection	
	Network traffic analysis (NTA)		
		Detection and response - user and entity behavior analytics (UEBA)	
		Active anti-phishing	Business email compromise
Application Security	OSS security scanning and software composition analysis for DevSecOps	Automated security scanning: OSS software composition analysis for DevSecOps	
Data Security			Dark data discovery
Secure Operations	Managed detection and response (MDR)	Detection and response - MDR	Detection and response – SIEM + SOAR
			Detection and response – MDR
		Vulnerability management	CARTA-inspired vulnerability management
			Security incident report
			Security rating services (SRS)

1.2.4 Gartner Top 10 Security Projects (Continued)

1. Privileged Access Management (PAM)
2. CARTA-Inspired Vulnerability Management
3. Detection and Response
4. Cloud Security Posture Management (CSPM)
5. Cloud Access Security Broker (CASB)
6. Business Email Compromise
7. Dark Data Discovery
8. Security Incident Response
9. Container Security
10. Security Rating Services

1.3 Common Security Threats

Virus attacks
By spreading malicious code such as viruses on the Internet, hackers corrupt computer systems or system files so that they cannot be used normally.

DDoS web attacks
Official websites, payment interfaces, apps, and other businesses are prone to attacks. These attacks mainly target the real-time online business systems of finance, e-commerce, and gaming platforms.

WebShell attacks
Hackers invade websites by exploiting vulnerabilities, implant dynamic scripts, and continuously control servers through backdoor webshells to perform various operations, such as file uploading and downloading and command execution.

Penetration attacks and data theft
Hackers steal data by launching drag and drop attacks and intrusions. An attack of this type is unobtrusive and durative so that massive data can be leaked before the enterprise detects the attack.

App vulnerabilities
By exploiting the vulnerabilities resulting from flaws or bugs in the logic design written by app developers, hackers can easily implant malicious code, steal sensitive information, and remotely control devices.

Scammers who profiteer from promotions
In China, users who profiteer from online promotions with little or zero costs are called the "wool-puling party". Such scammers undermine campaign objectives and seize large portions of campaign resources.

1.3 Common Security Threats (Continued)

Internet Business	Security Risk
Business layer	Loan delinquency fraud: Illegal loan brokers use fake ID information to apply for consumer loans.
	Incidents such as batch registration, cheating, and voucher hunting cause great losses to business platforms.
App application layer	Hackers exploit vulnerabilities in app source code to hijack large numbers of users.
	Sensitive data such as payment information is exposed due to malicious code implanted in the app.
Web application layer	Developers cannot quickly fix code when website security vulnerabilities are not promptly identified.
	Incidents such as injection attacks and XSS attacks can damage the public image of an enterprise and drive customers away.
Host layer	High-risk loopholes in servers cannot be promptly detected, nor fixed quickly.
	Malware and backdoors cannot be quickly detected on servers.
	Servers suffer brute-force attacks.
Network layer	Tenants who share the same platform are not isolated.
	DDoS attacks cause the server to crash and to be unable to provide services to external users.

1.4 From Traditional Security to Internet Security

Information Security System		Traditional Data Center
Security audit and risk control	Security assessment	Penetration testing
	Event management	SIEM system
	Intrusion detection	IDS & IPS equipment
	Vulnerability detection	Vulnerability scanning system
App application layer protection		MDM system
Web application layer protection		WAF equipment
Host layer protection		Security protection software
Network layer protection	Anti-DDoS	Anti-DDoS equipment
	Network isolation	Hardware firewall

1.5 Tencent Cloud Security System

腾讯云

Network Security	Data Security	Application Security	Business Security	Security Management
Anti-DDoS	Data Encryption Service	Web Application Firewall	Registration and Login Protection	Secure Operations Center
Anti-Virus Engine	Sensitive Data Processing	Web Vulnerability Scanning	Verification Code	Situation Awareness
Spoofing Defense and Threat Perception System	Data Security Audit	Mobile Security	Campaign Anti-Arbitrage	Business Risk Intelligence
Advanced Threat Detection System	Data Security Gateway	Mobile Game Security	Marketing Risk Control	Security Governance
Advanced Threat Tracing System	Data Security Governance Center	Application Intelligent Gateway	Anti-Fraud	Quantitative Assessment of Network Security Risks

腾讯云

Chapter 2

CONTENTS

Chapter 2 Network Security Products

2.1 Anti-DDoS Overview

- Massive terminals - Tencent Cloud covers the entire DDoS attack chain

Example blackmail email

Hello,

To introduce ourselves first:

http://[redacted].html

http://[redacted].html

http://[redacted]

Or just google "DD4BC" and you will find more info.

So, it's your turn.

Unless you pay 10 BTC to [redacted] within 12 hours from now, your pool servers are going under heavy DDoS attack.

Pay, and you will never hear from us again. 12小时内你得向我们支付10比特币，不然你渣渣的服务器将会受到严重的DDoS攻击

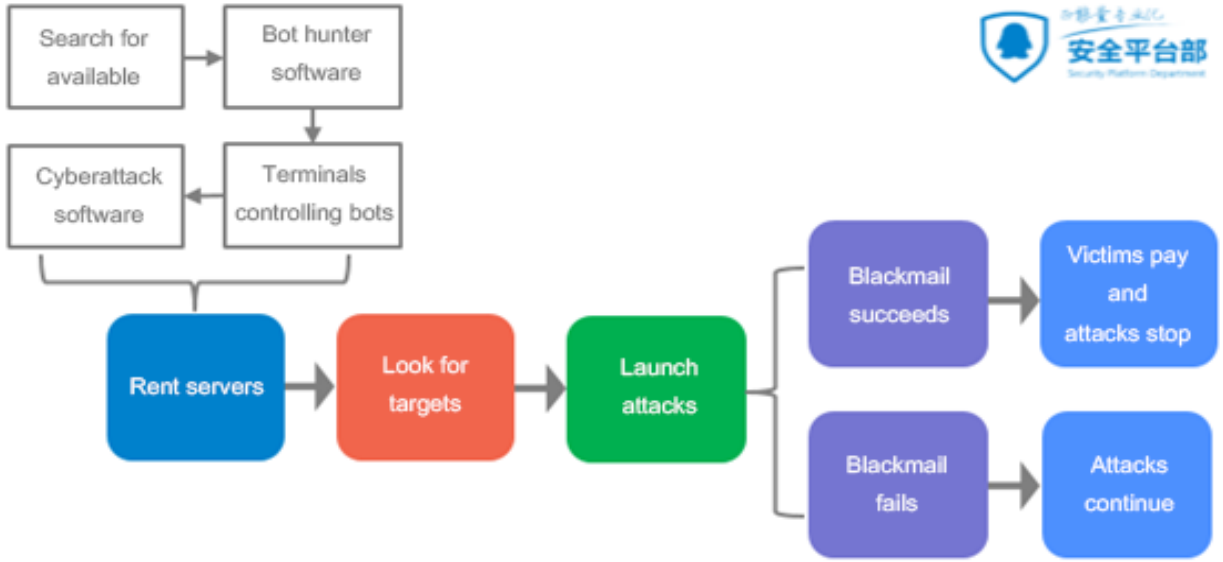
Usually, we attack first, then ask BTC to stop, but since your pool is too big, one of the largest Bitcoin pools, we are giving you time to act first, because we are well aware that even 1 hour offline would cause much larger damage then 10 BTC.

12 hours, because we are not in the same time zone and it's morning in China, so we want to make sure that you had time to act.

AS PROOF that this is not an empty threat, we will run a small attack on on your servers now. Don't worry it's not going to be hard and will run for just 1 hour, so your server will not get null routed.

But if not paid, all your servers are going down for good. 不给钱的话，你所有的服务器就永远完蛋啦

Please note that it will not be easy to mitigate our attack, because our current UDP flood power is 400-500 Gbps.



Low costs for DDoS attacks: For an attack traffic under 100 GB, buyers only need to pay RMB 200 for a single attack, and RMB 600 for 24 hours of continuous attacks. Attackers cash in mainly on blackmail emails and attacks on competitors.

2.1 Anti-DDoS Overview (Continued)

- Anti-DDoS Portfolio

- Free Anti-DDoS
- 2 Gbps protection bandwidth

- DDoS and CC protection
- Custom editing of binding settings
- 300 Gbps protection bandwidth

- DDoS and CC protection
- 300 Gbps protection bandwidth

- DDoS and CC protection
- 1.7 Tbps protection bandwidth

- DDoS and CC protection
- IP address polling

2.2 Technical Principles

Protection architecture

Double cleansing

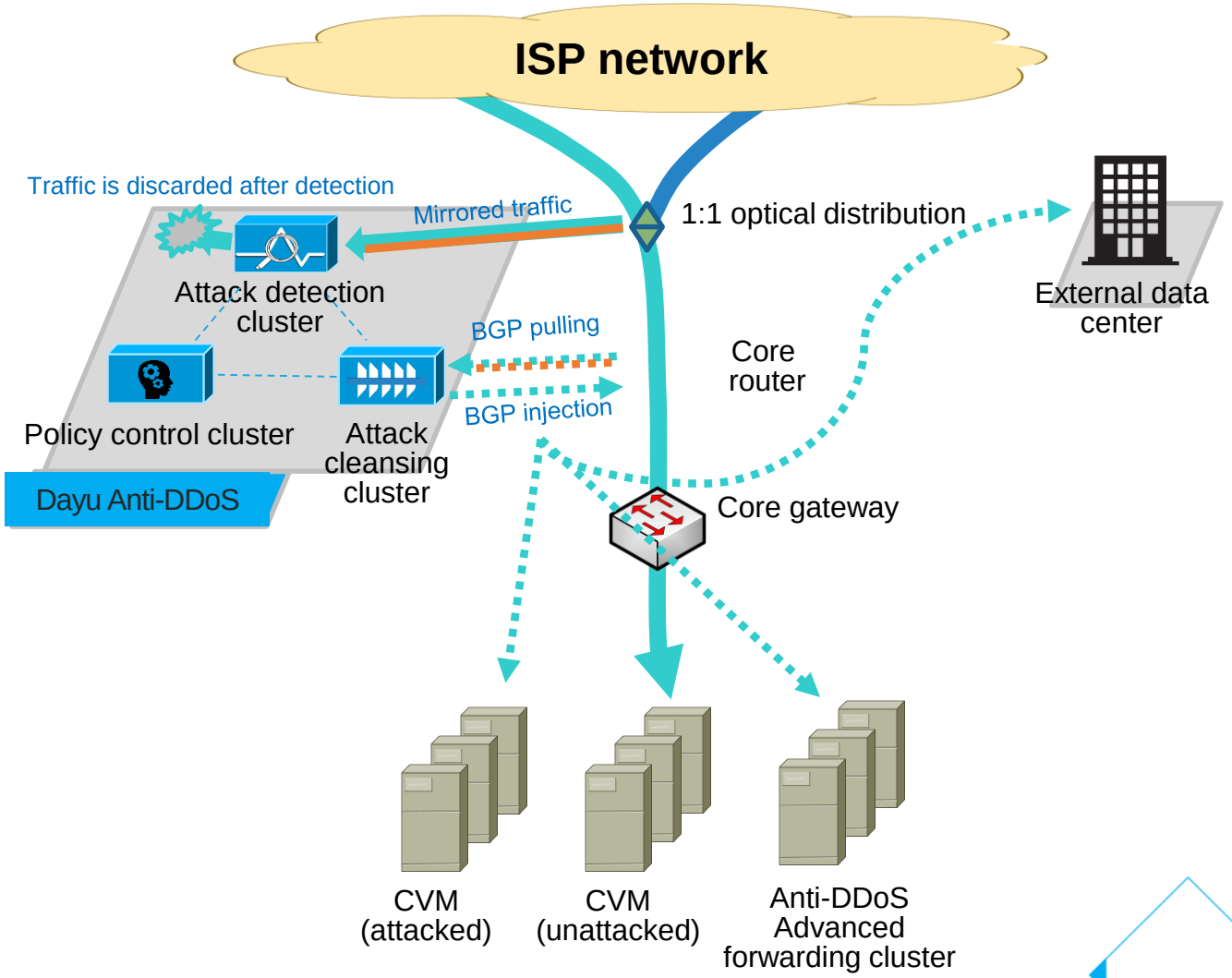
- The first cleansing uses a general policy to remove common attacks.
- The second cleansing uses a custom policy to remove uncommon attack variants and ensure optimal protection results.

Support non-cloud customers

- The forwarding cluster can forward clean traffic to non-Tencent data centers.

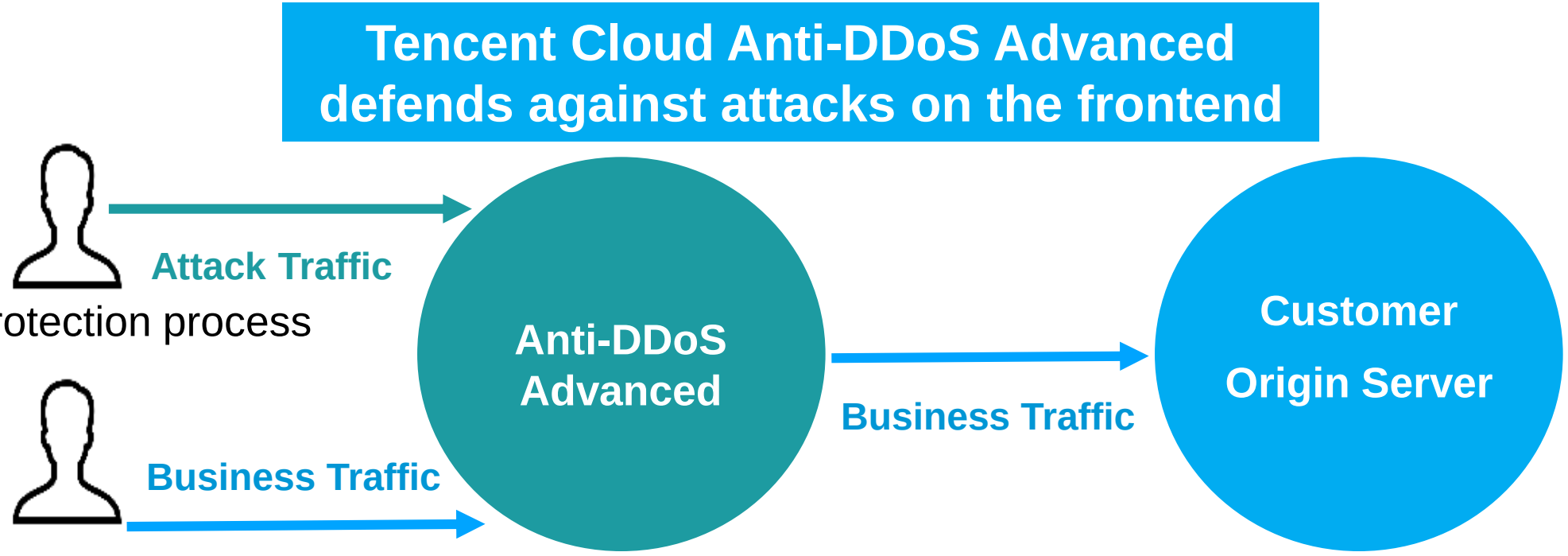
One-to-many protection

- Each Anti-DDoS Advanced IP supports up to 60 forwarding rules.
- Each rule can be configured with up to 20 origin server IP addresses.



2.2 Technical Principles (Continued)

- Protection process



The customer uses the Anti-DDoS Advanced IP address as its business IP address to direct attacking traffic to the Tencent Anti-DDoS Advanced data center. The business traffic is directed back to the customer's origin server after cleansing.

2.3 Advantages

Ultra-large protection bandwidth

The platform provides a **single-point** protection bandwidth in terabytes.
It also provides customers with a protection bandwidth of up to **610 Gbps** for a single point.

Millions

Withstand millions of attacks every year

Optimal access experience

The industry's most comprehensive **28-channel BGP**
Low access latency and reliable channels

600 Gbps+

Withstand 600 Gbps+ attacks at a single point

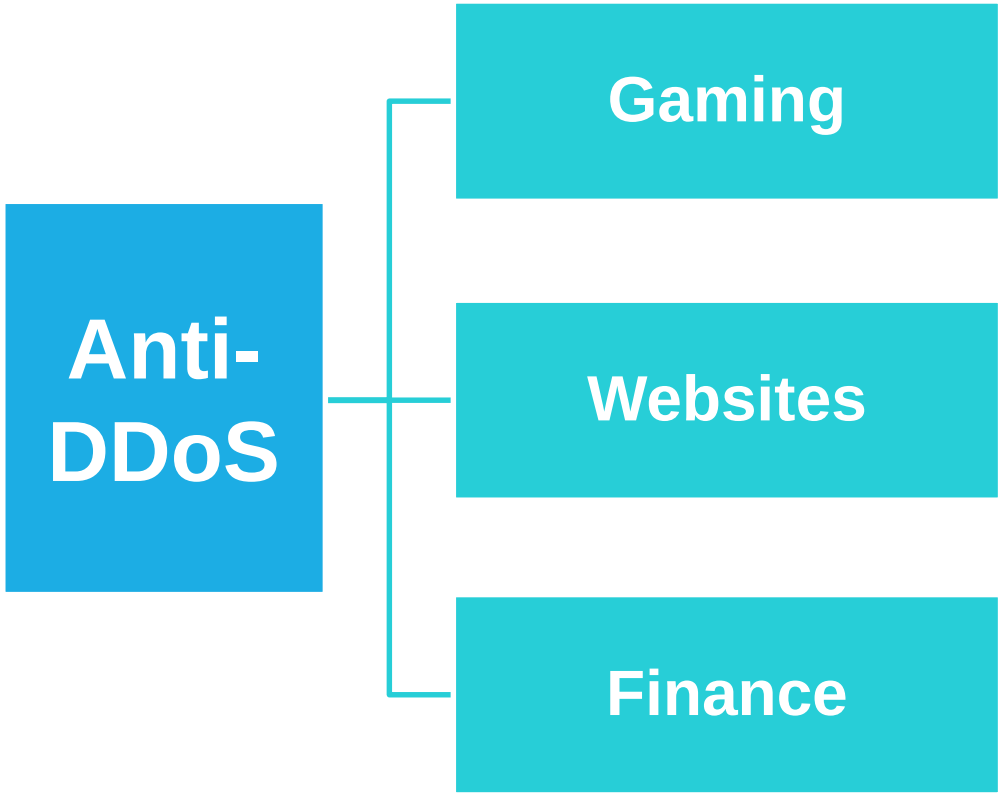
Accurate recognition algorithm

We use a self-developed algorithm empowered by the AI technology.
It defends against millions of attack attempts every year, with a **success rate higher than 99.995%.**

99.995%

Defense success rate higher than 99.995%

2.4 Use Cases



- Malicious attacks prevent or slow down the access of large numbers of users.
- Various types of attacks, such as UDP mini packet attacks, ACK flood attacks, and cheat game plugins that cause user attrition.

- With their real IP addresses exposed, website servers can suffer traffic attacks or application-layer attacks, causing slow website access or service breakdown.

- In the banking, insurance, security, and Internet finance industries, malicious competitors use DDoS attacks to crash competing websites or apps, severely compromising investor confidence.

2.5.1 Anti-DDoS Advanced Billing

Anti-DDoS Advanced uses a combination billing model that utilizes monthly subscription and pay-as-you-go. Base Protection Bandwidth and Forwarding Traffic are billed by monthly subscription. Elastic Protection Bandwidth is pay-as-you-go with a daily billing cycle.

Billing Item	Billing Method	Payment Method	Payment Description
Base Protection Bandwidth	Monthly Subscription	Frozen Fees	Bandwidth for base protection. The fee is calculated based on base protection bandwidth limit and the service plan period. Fees for the first month will be frozen in your account upon purchase and deducted on the 1st day of the next month. If you increase the bandwidth, extra fees will apply. Please note that you can only upgrade or keep your current service plan. Downgrade is not supported.
Elastic Protection Bandwidth	Pay-as-you-go	Postpaid	Once elastic protection is enabled, you will be charged a fee based on the range of elastic protection bandwidth during the maximum attack traffic of the day. The bill will be sent the next day. No fee occurs if the elastic defense is not triggered and you can adjust the set bandwidth as needed.
Forwarding Traffic	Monthly Subscription	Frozen Fees	Bandwidth of cleansed traffic forwarded back to the real server.

For more pricing information about Anti-DDos Advanced, see here .

2.5.2 Anti-DDoS Pro Billing

Anti-DDoS Pro service uses combined billing methods, including monthly subscription and pay-as-you-go. The Base Protection Bandwidth adopts monthly subscription, while the Elastic Protection Bandwidth adopts the pay-as-you-go method and is billed by day.

Billing Items	Billing Methods	Payment Methods	Payment Description
Base Protection Bandwidth	Monthly Subscription	Freeze Payment	Provides basic protection bandwidth. The prepaid fee is based on the base protection bandwidth and the purchased usage duration. The cost will be frozen after you purchase it, and the cost of the previous month will be billed on the first day of the following month, etc.
Elastic Protection Bandwidth	Pay-as-you-go by Day	Postpaid	When the elastic protection is triggered, the bill is based on the corresponding elastic protection bandwidth of the highest attack bandwidth of that day. The bill will be generated the next day. You will not be billed if the elastic protection is not triggered. It supports upgrading and degrading configuration.

For more pricing information about Anti-DDos Pro, see here .

腾讯云

Chapter 3

CONTENTS

Chapter 3 Host Security Products

3.1 Main Features of Host Security

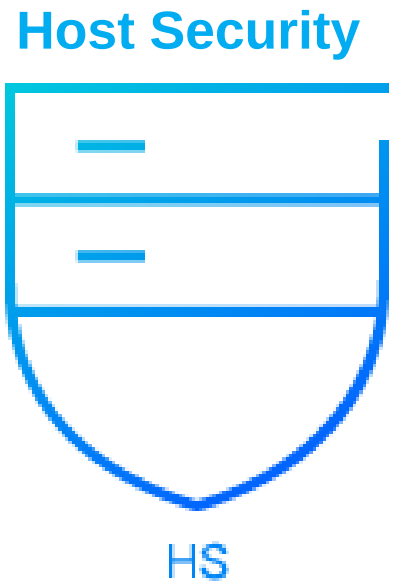
- Challenges of enterprise host security management

Dispersed intrusion channels

Blurred security boundaries

Developers lack sufficient security expertise

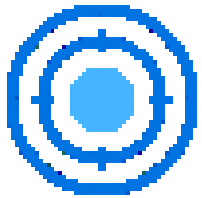
Traditional solutions do not work well for the cloud



Gartner: An enterprise averagely loses 11% of its customers for each data leakage incident.

Brand damage | **Stress of legal actions** | **Stress of operating costs** | **Stress of public opinions** | **Cash flow losses**

3.1 Main Features of Host Security (Continued)

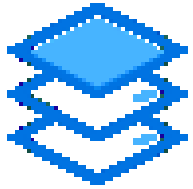


Trojan File Detection

Password Cracking Detection

Login Audit

Vulnerability Detection



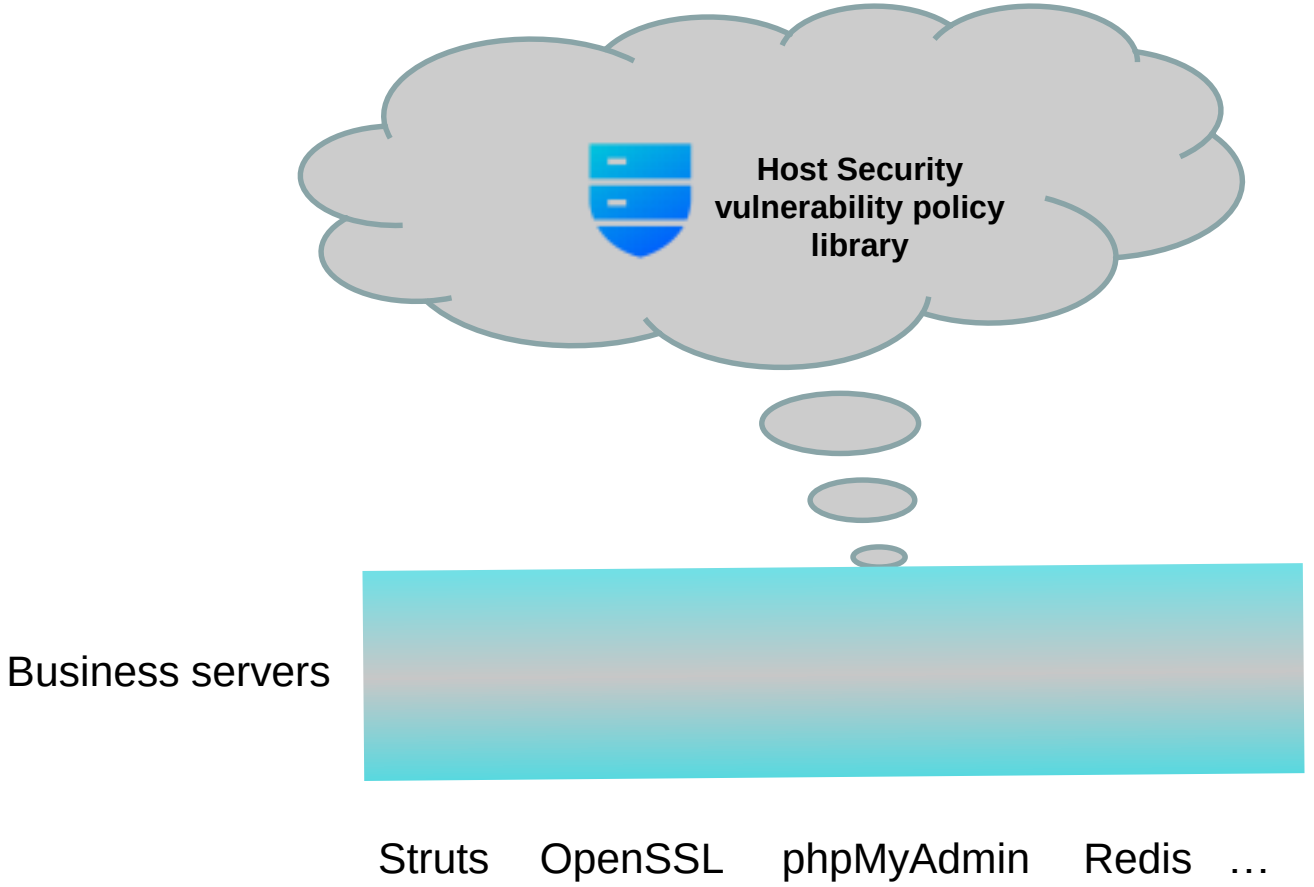
Asset Component Identification

3.1 Main Features of Host Security (Continued)

Key Feature	Basic Protection	Professional Protection
Password Cracking Detection	Supported	Supported
Login Log Audit		Supported
WebShell Detection	Limited to five free detections	Supported
Hacker Tool Detection		Supported
Binary Virus and Trojan Detection		Supported
Weak Account Password Detection		Supported
Web Component Vulnerability Detection		Supported
Common Component Vulnerability Detection		Supported
System-Level Vulnerability Detection		Supported
Vulnerability Repair Solution Push		Supported
Zero-Day Vulnerability Intelligence Push	Not supported	Supported
Configuration Risk Item Detection		Supported
Expert Service		Supported

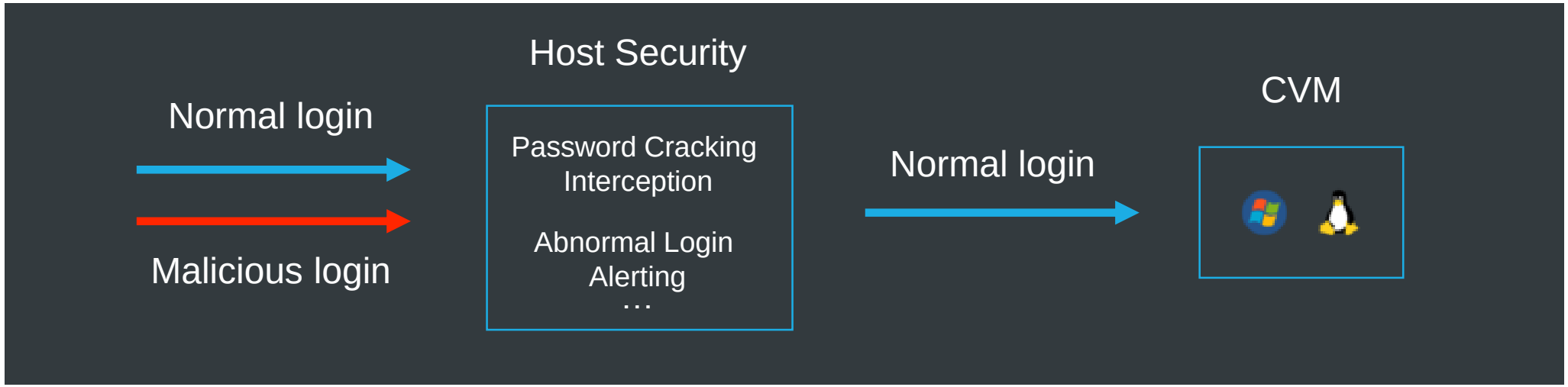
3.2 Host Security Technical Principles

- Vulnerability risk management based on a powerful Host Security vulnerability policy library



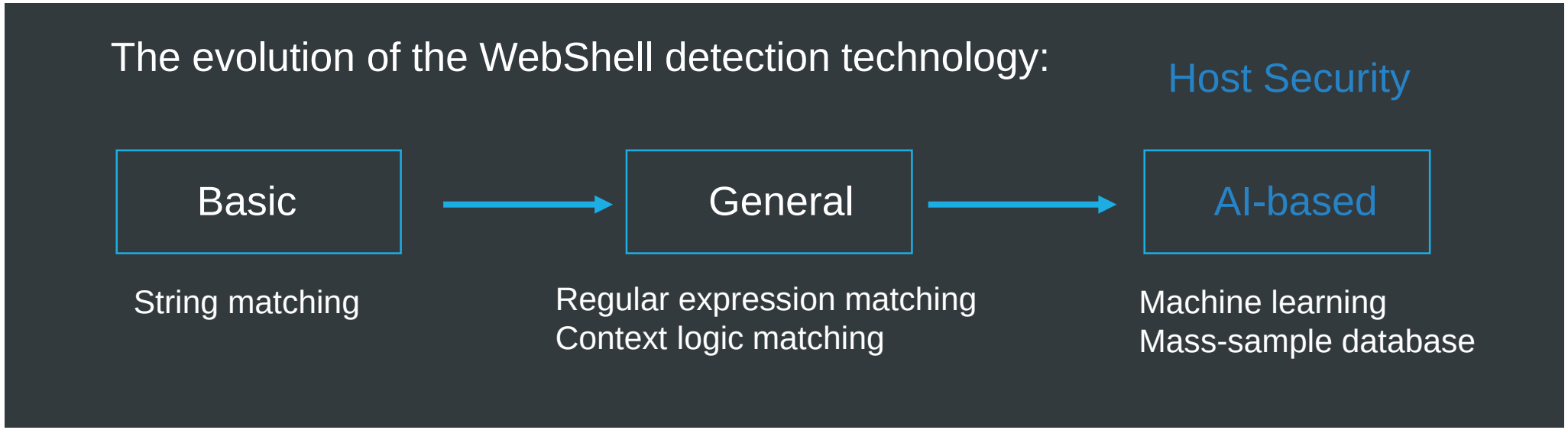
3.2 Host Security Technical Principles (Continued)

- Block password cracking attempts with the advantages of cloud



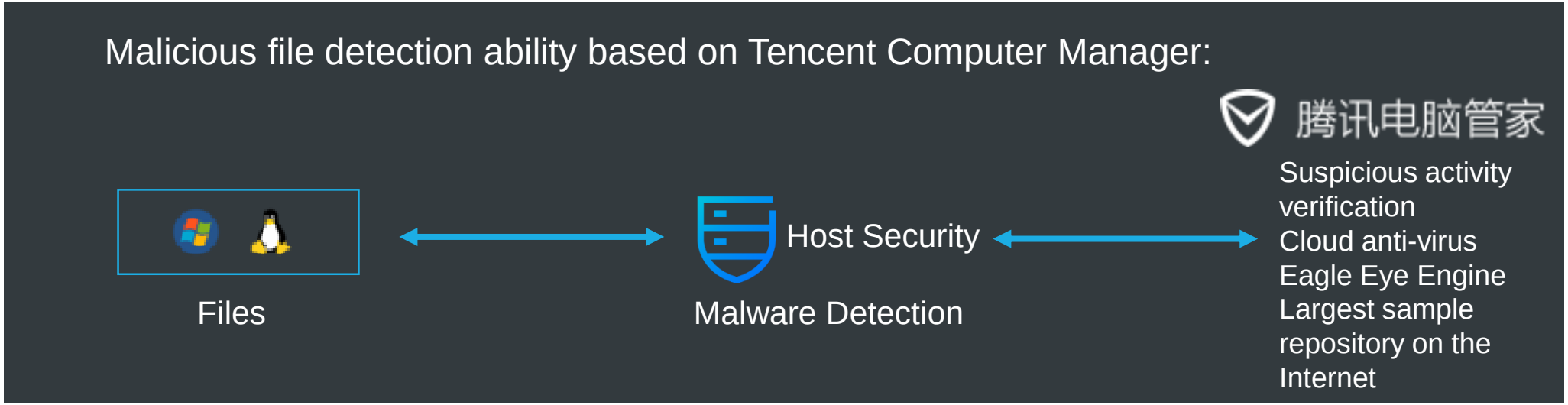
3.2 Host Security Technical Principles (Continued)

- AI-based WebShell detection technology



3.2 Host Security Technical Principles (Continued)

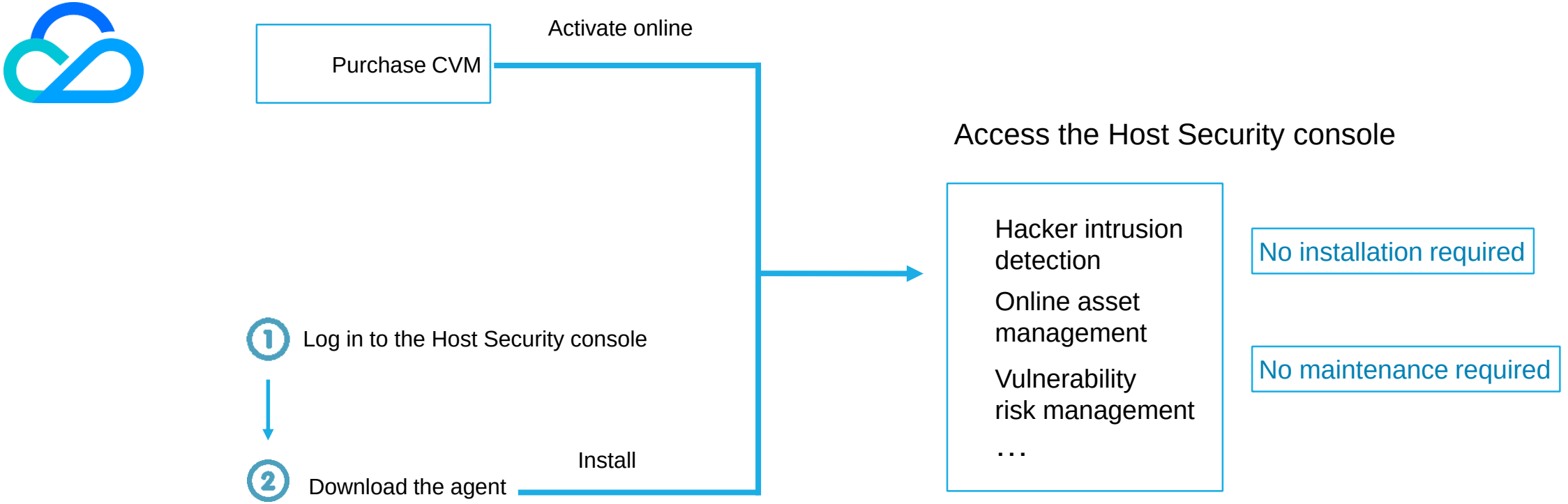
- Malicious file detection ability based on Tencent Computer Manager



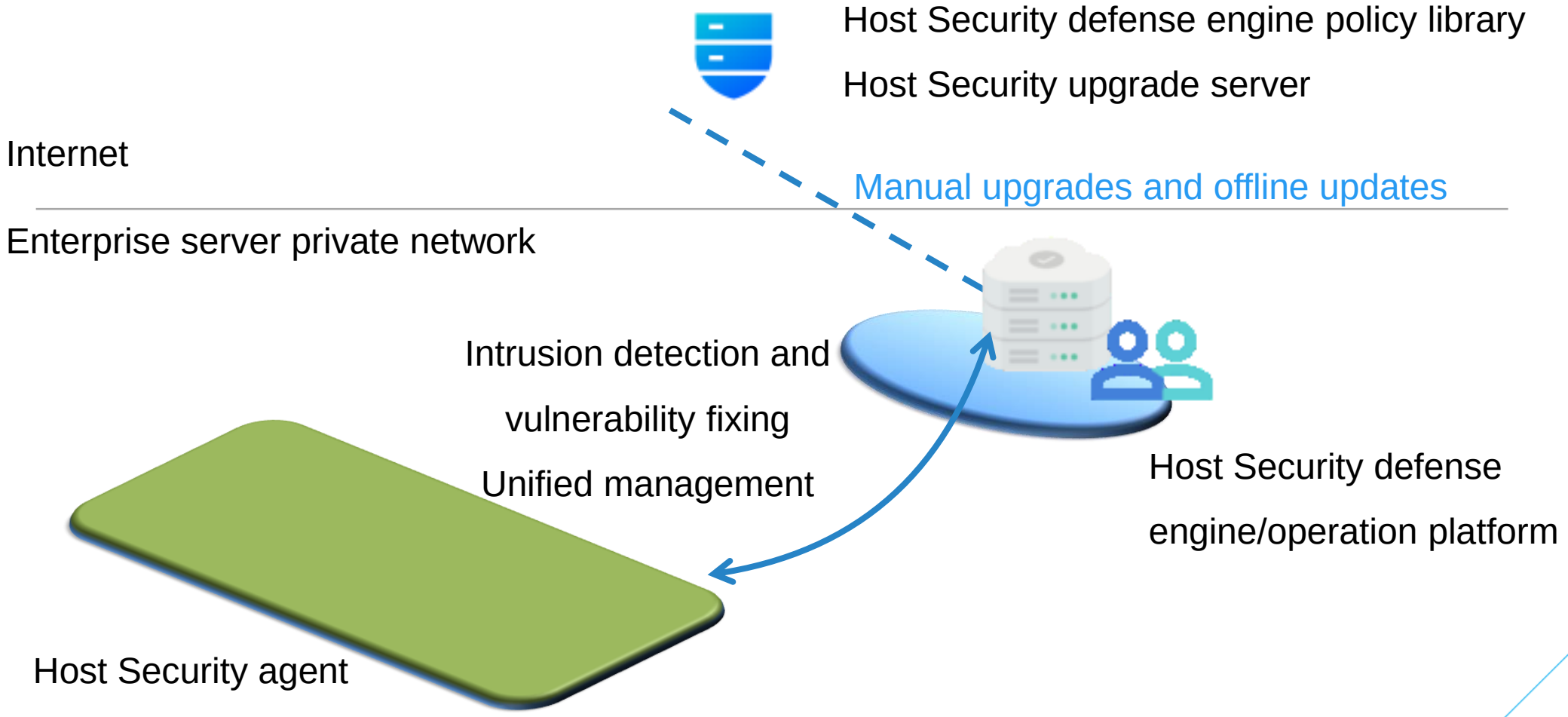
3.3 Host Security Applications

Host Security Applications	
1	Public Cloud Scenario
2	Private Cloud Scenario

3.3.1 Public Cloud Scenario



3.3.2 Private Cloud Scenario



腾讯云

CONTENTS

Chapter 4

Chapter 4 Website Security Products

4.1 Web Application Firewall Overview

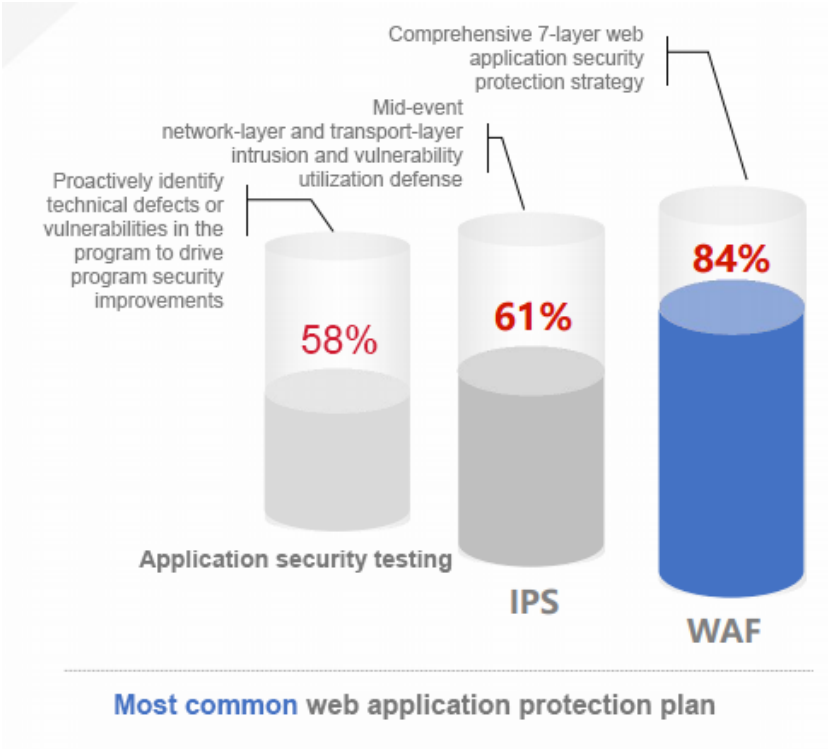
With massive user data and a better chance of financial gain, financial, portal, and e-commerce websites become the primary targets of hackers.

4.1 Web Application Firewall Overview (Continued)

- Web Application Firewall (WAF) is the most common and effective web application protection solution. Gartner WAF Magic Quadrant 2017

(1) Business architecture before WAF is deployed

(2) Business architecture after WAF is deployed



4.1 Web Application Firewall Overview (Continued)

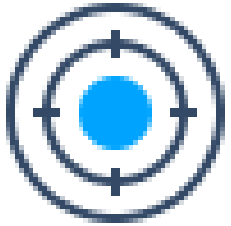
Tencent Cloud Web Application Firewall (WAF) is an AI-based one-stop website protection platform:

AI + Web Application Firewall

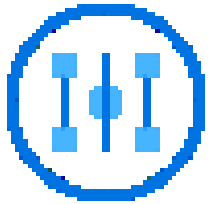
Patches for Zero-Day Vulnerabilities

Webpage Tampering Prevention

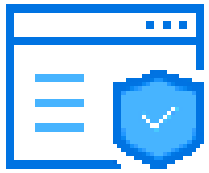
Data Leakage Prevention



CC Attack Prevention



Crawler and Bot Behavior Management

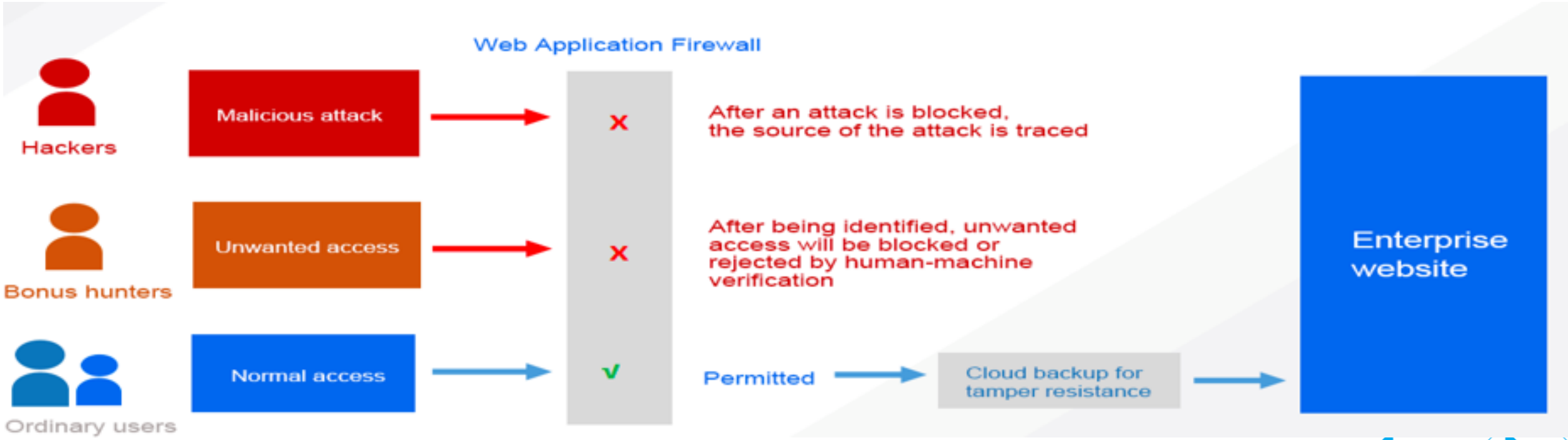


DNS Hijacking Detection

30-Channel BGP IP Access Protection

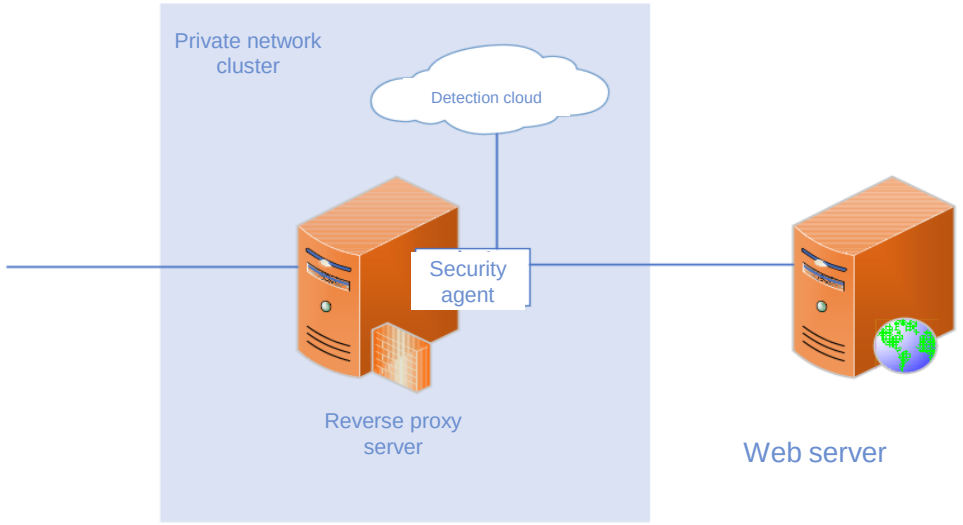
4.2 WAF Technical Principles

- **Before an attack:** Monitor and analyze potential security risks in real time
- **During an attack:** Identify and block malicious attacks and unwanted access attempts
- **After an attack:** Ensure the normal display of webpage content with cloud backup



4.2 WAF Technical Principles (Continued)

- **Reverse proxy + detection cloud:**
  - The service modifies the DNS record and forwards the traffic to a reverse proxy.
  - The security module of the reverse proxy receives the user request and encapsulates it before sending it to the detection cloud.
  - The detection cloud receives the request, performs detection, and sends the disinfected traffic to the service server.



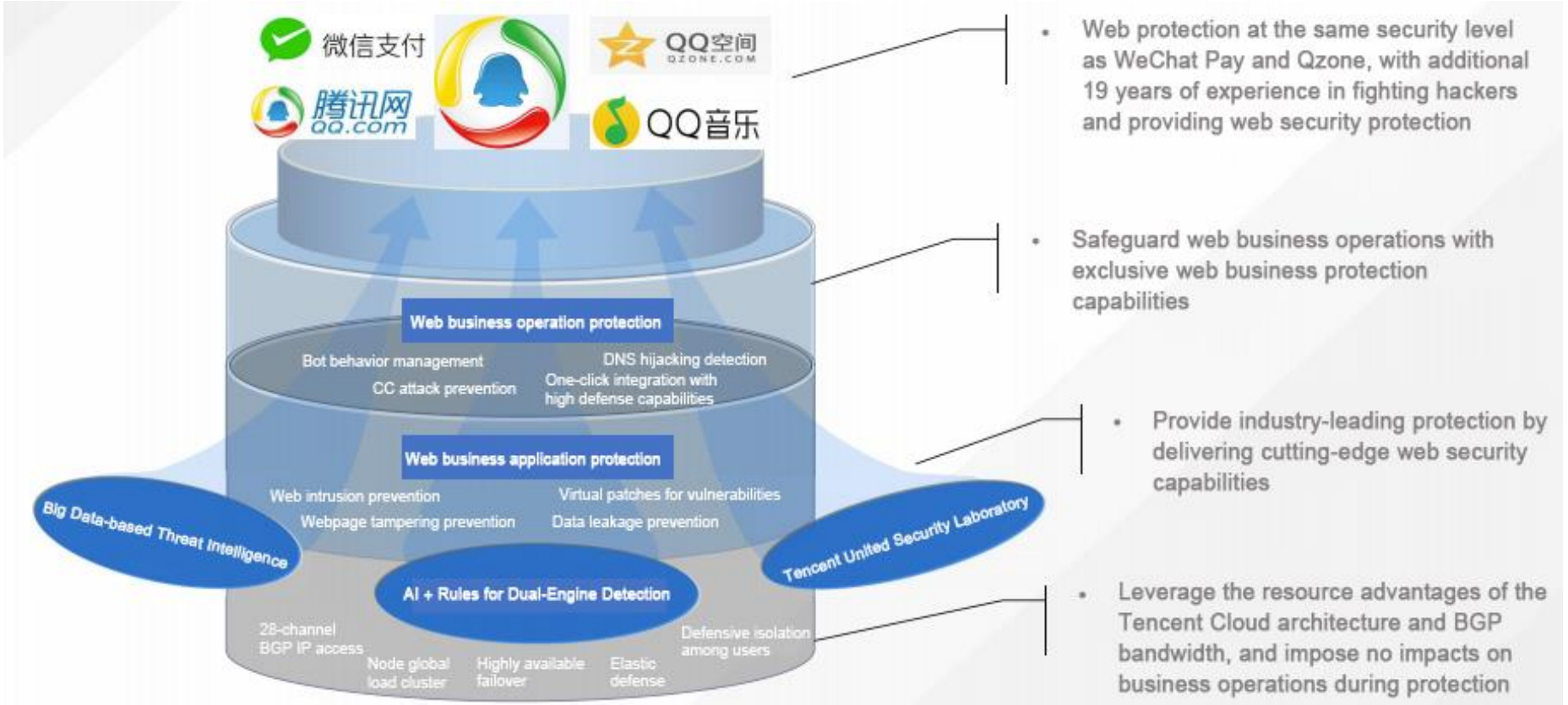
Common strategies used by WAF:

4.2 WAF Technical Principles (Continued)

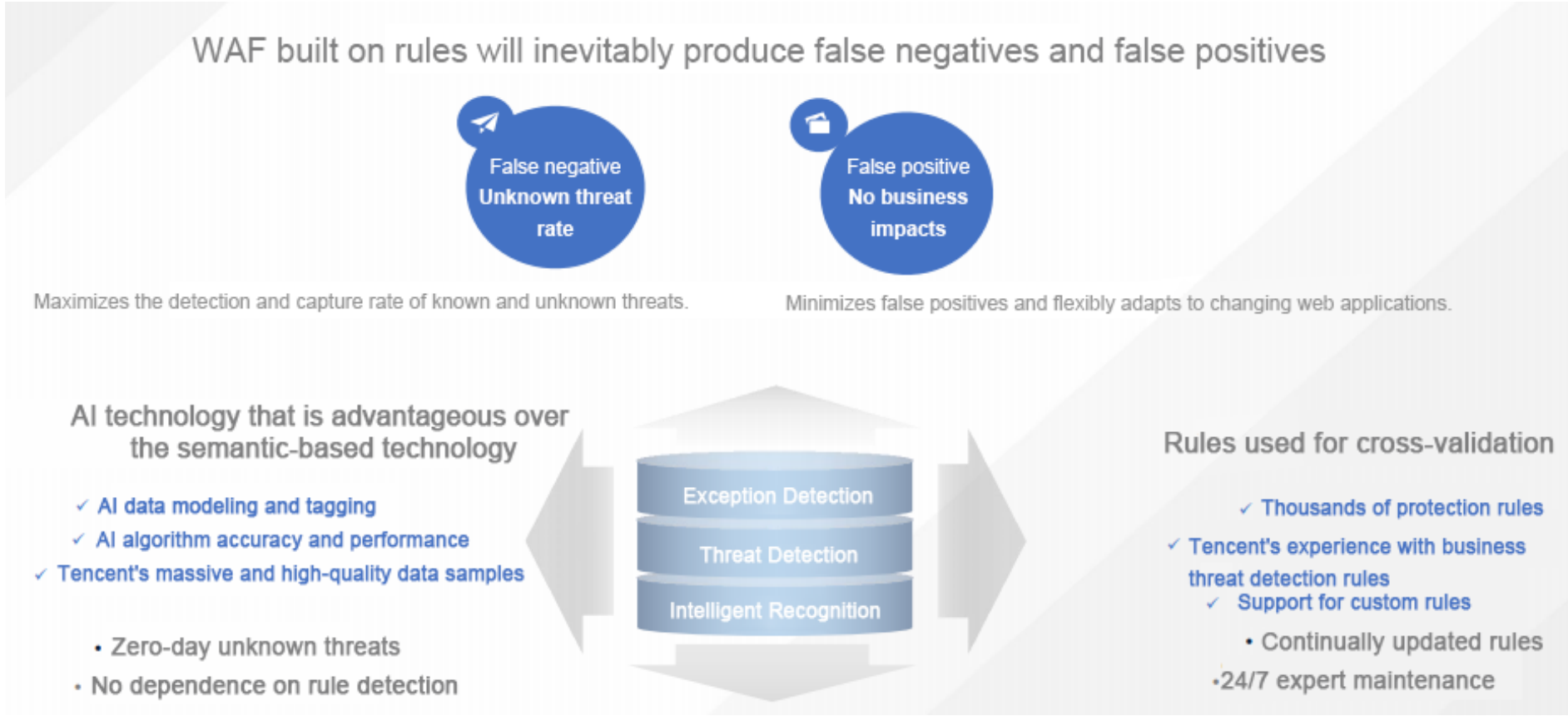
腾讯云

Feature Recognition	Algorithm Recognition	Pattern Matching
• Recognize attack behavior features • For example, recognize viruses and worms	• Recognize based on semantic understanding • For example, recognize SQL injections and DDoS attacks	• Attack behavior can be identified as an intrusion once it matches a certain pattern derived from previous attack behaviors

4.3 WAF Advantages



4.3 WAF Advantages (Continued)



4.3 WAF Advantages (Continued)

- High performance and availability

99.9% high-availability WAF	Over 10,000 protective regular expressions	Zero-day hot patching 24/7 follow-up	Network latency less than 5-10 ms

4.4 WAF Use Cases

1

Government website protection

- Prevents government website content from being tampered with and data from being stolen by hackers.
- Ensures correct website information, the availability of government services, and smooth public access.

- Intelligently filters off malicious attacks and junk access attempts to ensure smooth access to businesses.
- Eliminates the negative impact of competitor price comparisons, inventory queries, and malicious SEO caused by malicious crawlers.

E-commerce website protection

2

3

Financial website protection

- Monitors DNS link hijacking to prevent the malicious redirection of website traffic.
- Effectively detects unexpected access attempts, such as account credential enumeration attacks, to prevent user information from being tampered with, stolen, or leaked.

4.5 WAF Billing Methods

Billing formula: Daily bill = Daily peak QPS x QPS rates

- Daily peak QPS
Daily peak QPS is based on data between 00:00:00 and 23:59:59 in one day. Website QPS is the total number of requests per second for your domain received by the WAF. Counting starts once domain name is configured.

- QPS rates
See below for tiered QPS rates:

```
If peak QPS is between 5-50 (number less than 5 will be counted as 5), per QPS rate is 0.2 USD/day.
If peak QPS is between 50-200, per QPS rate is 0.18 USD/day.
If peak QPS is between 200-1,000, per QPS rate is 0.15 USD/day.
If peak QPS is greater than 1,000, per QPS rate is 0.12 USD/day.
```

Tiered Price Table:

Peak QPS	QPS Rates
< 5 QPS	0.2 USD/day
5-50 QPS	0.2 USD/day
50-200 QPS	0.18 USD/day
200-1000 QPS	0.15 USD/day
> 1000 QPS	0.12 USD/day

For more pricing information about WAF, see here .

4.6 Web Vulnerability Scanning

- Tencent Cloud Web Vulnerability Scanning is a security service that monitors website vulnerabilities. It provides enterprises with comprehensive and accurate 24/7 vulnerability monitoring and professional patching recommendations.

SasS service

Clients do not need to install any hardware or software

Various vulnerability scans

Cover common and particular vulnerabilities

Various scanning modes

Provide standard scanning and deep scanning

- Web Vulnerability Scanning is charged on a prepaid basis based on the number of domain scans.

腾讯云

Chapter 5

CONTENTS

Chapter 5 Mobile Security Products

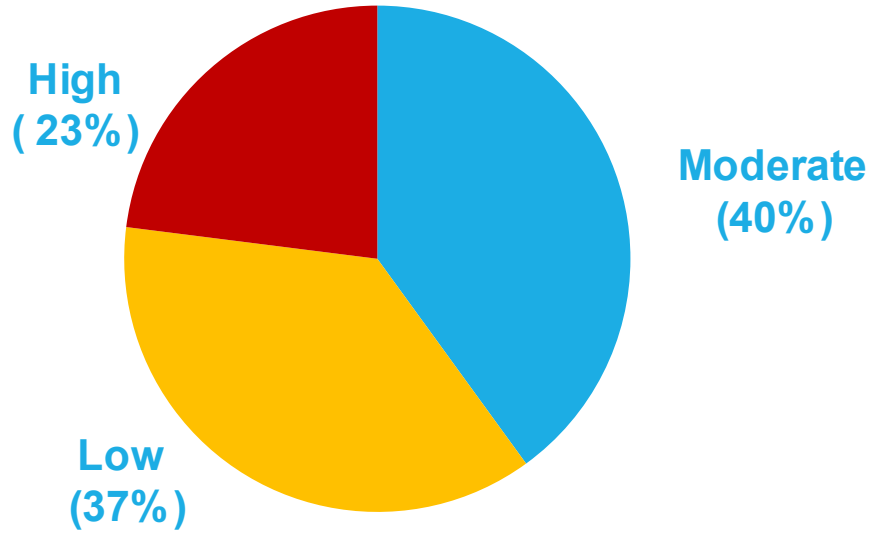
5.1 Mobile Security Overview

CCTV's Consumer Rights Day Gala in 2016 demonstrated the process of monitoring app traffic and exposing users' private information. This gave the public a better understanding of the risks of app vulnerabilities.

5.1 Mobile Security Overview (Continued)

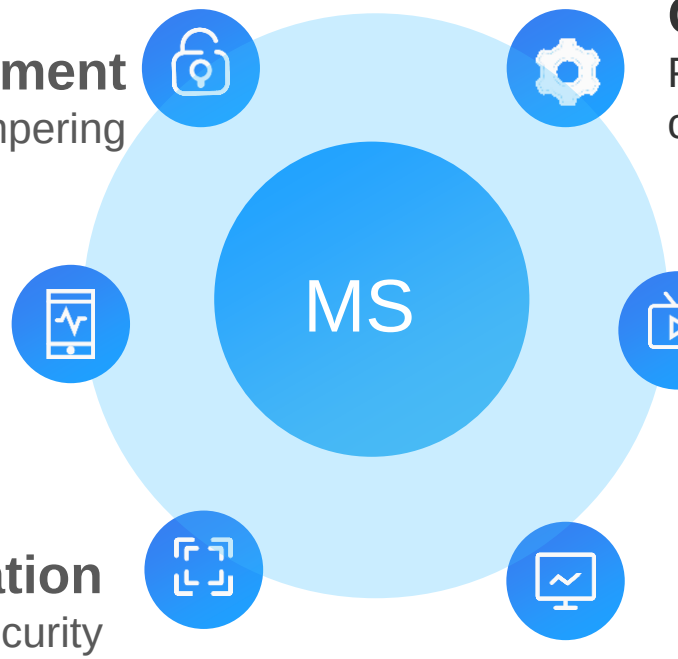
- Top 10 security risks for financial apps:
  - Information data transmitted in clear text
  - Communication data can be decrypted
  - Sensitive data can be cracked on premises
  - Debugging information exposure
  - Sensitive information exposure
  - Misuse of cryptography
  - Functionality exposure
  - Modification and repackaging
  - Debugging
  - Code can be reverse engineered

Evaluation of vulnerabilities in financial apps



Data source: Tencent Cloud App Security Statistics for 2016

5.1 Mobile Security Overview (Continued)



Application Reinforcement
Piracy monitoring and anti-tampering

Channel Monitoring
Precisely monitor distribution channels and downloads

Compatibility Testing
50 types of physical machines for automatic compatibility and adaptability testing

Quality Tracking
Real-time crash information

Security Evaluation
Data leakage prevention, security audit, and vulnerability scanning

Security SDKs
Database security protection, keyboard input protection, and anti-game plugin SDKs

5.2 MS Technical Principles

腾讯云

Static and dynamic scanning

- By using the data flow analysis mechanism, static scanning covers all hidden code.
- The taint checking mechanism enables register-level granularity.
- Dynamic scanning uses fuzz testing to generate accurate results.

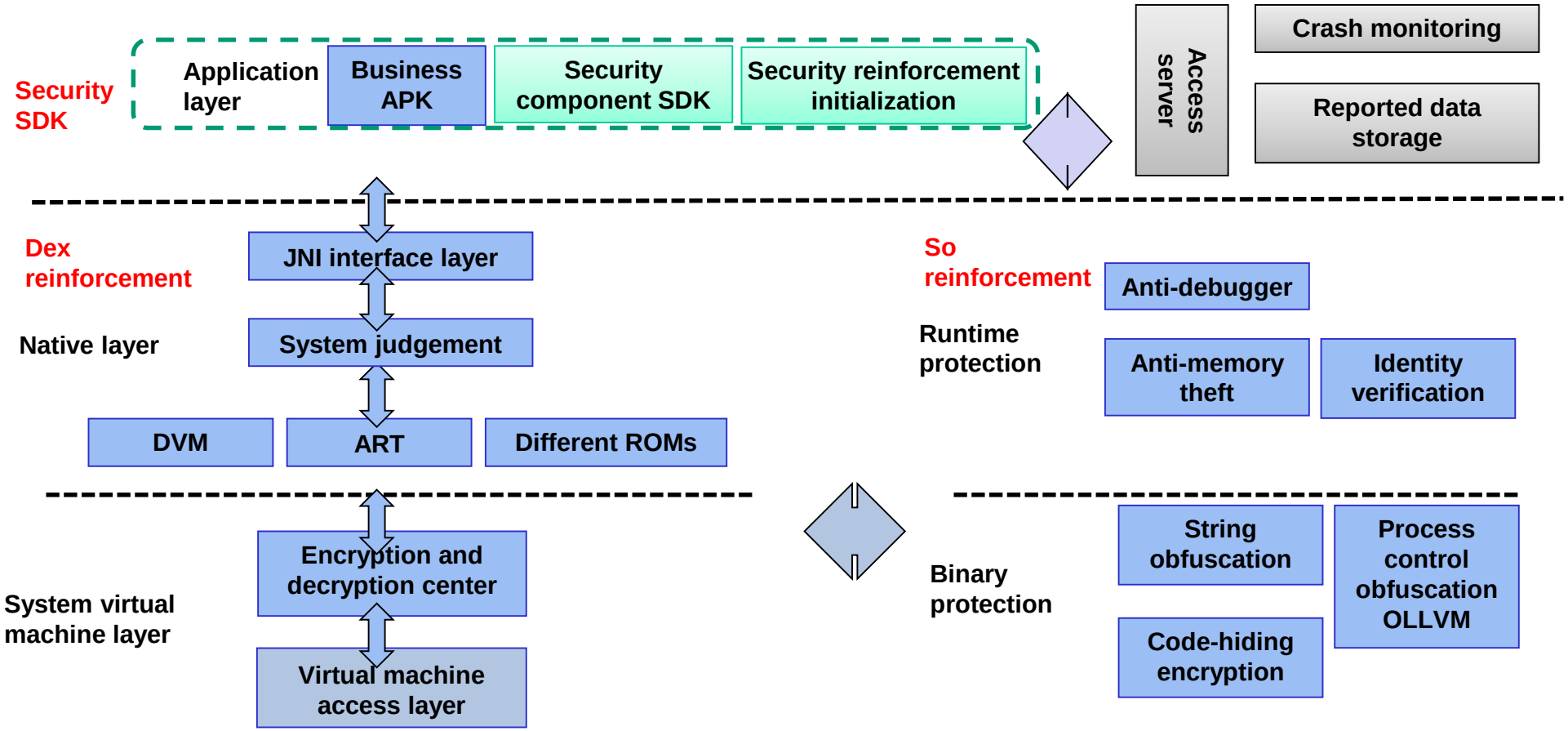
Accurate location and detailed modification recommendations

- Accurately locates vulnerabilities and provides modification recommendations.
- Quickly responds and provides updates to fix emergent and new vulnerabilities.

Unpack scanning

- Enforces unpack scanning on reinforced and packaged applications to identify potential risks in applications at the maximum.

5.2 MS Technical Principles (Continued)



5.3 MS Advantages

Top-level app distribution market

MyApp covers mainstream channels in China, helping you obtain precise information about channel distribution.

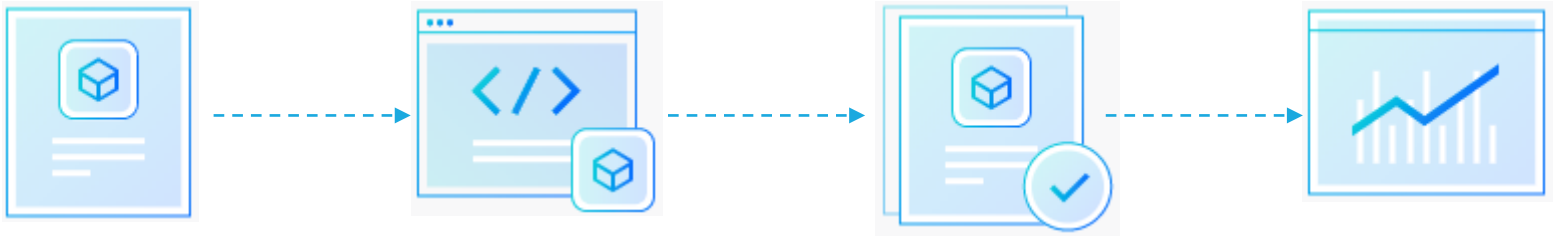
Top-level sample channel source

Tencent **Mobile Manager** holds the latest and most comprehensive malicious samples.

Comprehensive Channel Monitoring

24/7 monitoring is available to track both copyrighted and pirated channel downloads.

5.4 MS Use Cases



Requirement Planning Phase

- Security consultation
- Security training

App Testing Phase

- White-box cryptography
- Soft keyboard
- Security testing

Application Release Phase

- Application reinforcement
- Compatibility testing

Application Operation Phase

- Crash testing
- Piracy monitoring

5.4 MS Use Cases (Continued)

3. App distribution

Requirement Planning Phase

- Security consultation
- Security components

App Acceptance Phase

- Security testing
- Application reinforcement
- Compatibility testing

Before App Release

- Security testing

After App Release

- Regular security detection

Quizzes

- What are the products in the Anti-DDoS portfolio?
- What are the basic features of Host Security?
- What are the basic features of WAF?
- What are the basic features of Mobile Security?

Course summary

- This course covers the following subjects:
  - Cloud Security System and Standards: cloud security principles, the shared security responsibility model, CSA4.0, Classified Protection Standard 2.0, TRUCS, cloud security threats, and the Tencent Cloud security system.
  - The features, principles, advantages, use cases, and billing methods of mainstream Tencent Cloud security products.

腾讯云

Thank you.