

The background features a series of vertical panels with rounded ends. The leftmost panel shows a person's hands typing on a laptop. The subsequent panels contain various white line-art icons on a semi-transparent background: a graduation cap, a play button, a target with an arrow, an open book, a magnifying glass, and a person at a computer. The main title is centered in blue text.

Threat Defense and Information Security Development Trends

Lecture 4

HCIA-Security

Prepared by
Dr. Abdelrhman Ahmed

Forward

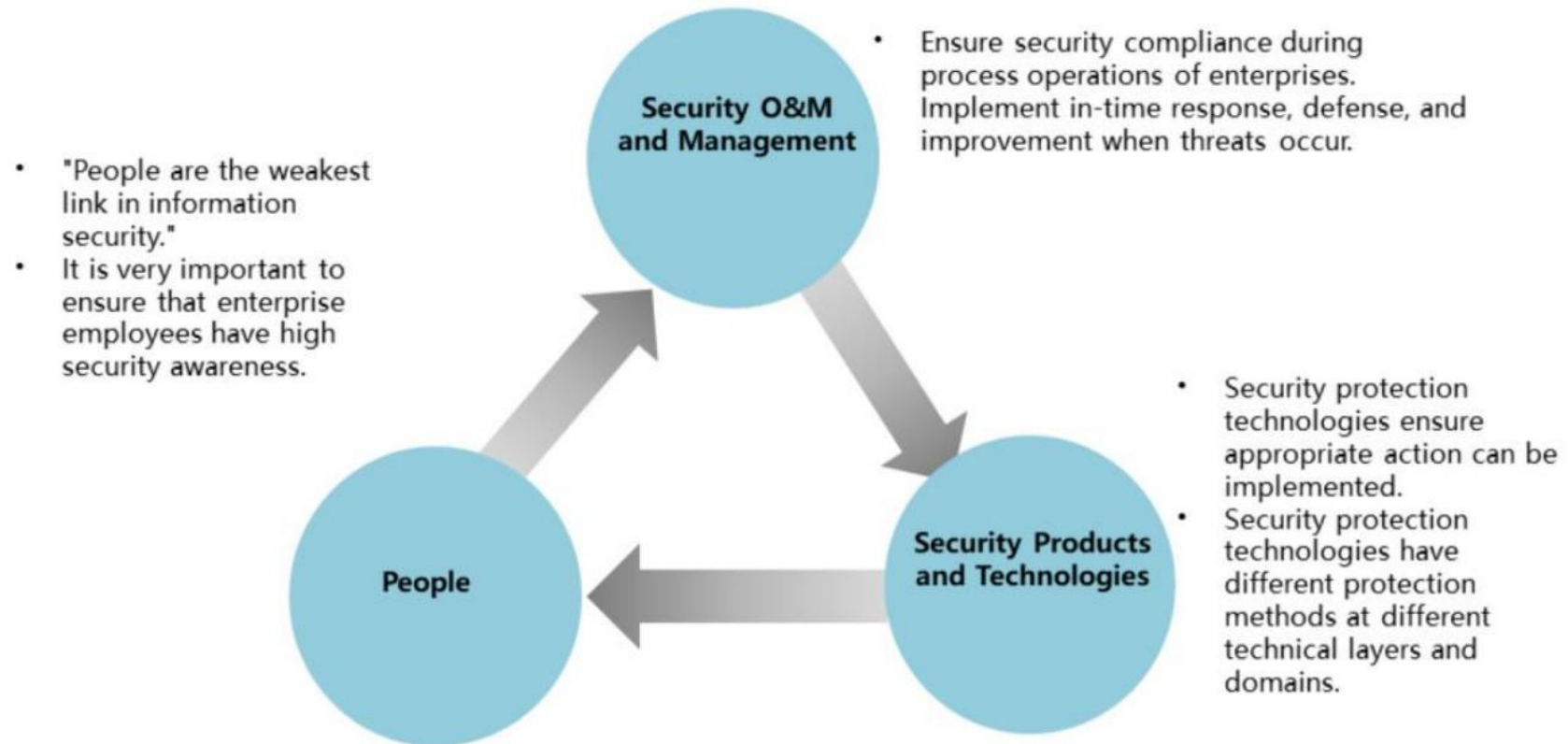
- The previous courses have introduced some basic concepts and knowledge about information security and common attack types.
- Consider this question: What measures should we take to ensure enterprises' information security?
- Defense against security threats not only requires professional tools but also the awareness of everyone involved in information security construction.

Objectives

- **Upon completion of this course, you will be able to:**
 - ☐ **Describe the basic elements of security threat defense.**
 - ☐ **Describe the importance of information security awareness in security protection.**
 - ☐ **Describe the future development trends of information security.**

Chapter
04

Key Elements of Information Security Protection



Three interconnected elements

Information Security Protection Methods

- Network security: firewall, IPS/IDS, anti-DDoS, etc.
- System security: server security, host security, etc.
- Endpoint security: secure access, identity authentication, etc.
- Application security: antivirus, vulnerability scanning, penetration testing, etc.

Security products and technologies

O&M and management

- Security operation
- Emergency response
- Disaster recovery

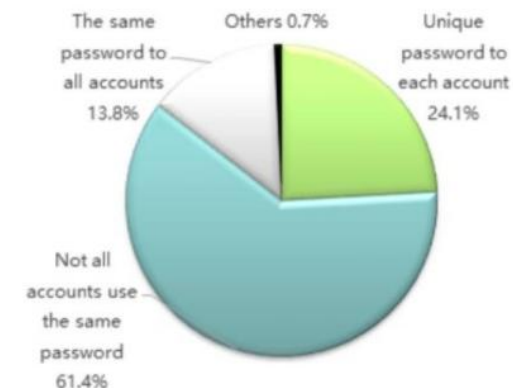
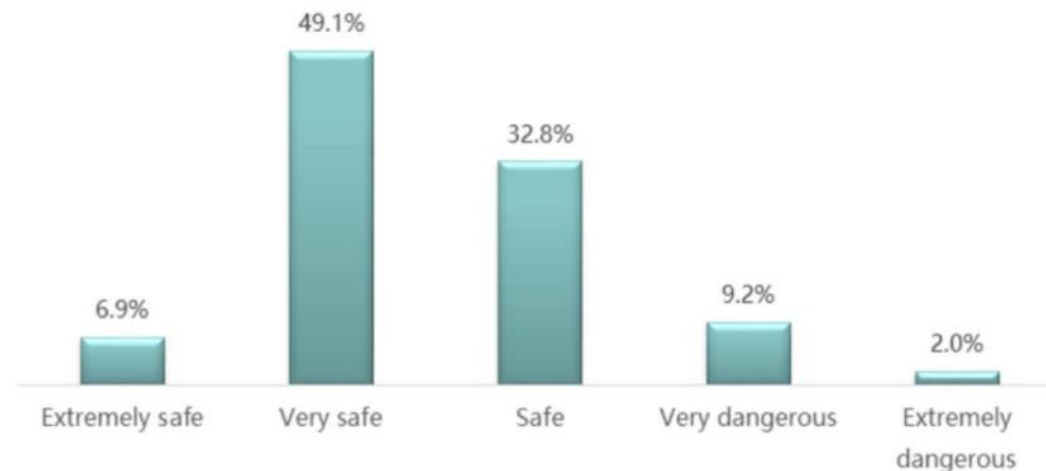
- Fostering security awareness in enterprise employees
- Raising awareness of social engineering

Security awareness

Chapter
04

Cybersecurity Awareness survey

- Do you read the User Agreement in detail when you register an account?
- Do you use the same password for all your accounts?
- Do you think the current cyber environment is secure?



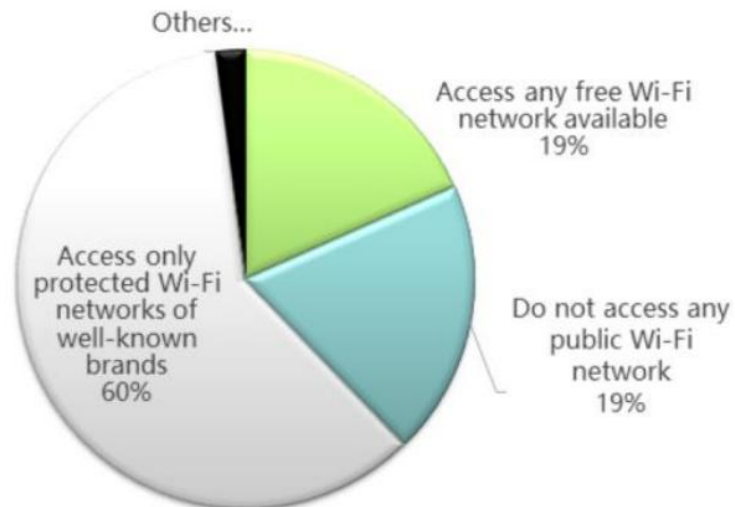
- According to the Survey Report on Cyber Security Awareness of Chinese Internet Users launched by Qihoo 360, 24.1% have a unique password for each account, and 61.4% use different passwords. However, 13.8% use the same password for all accounts, which has high security risks.

Chapter
04

Public Wi-Fi Security Awareness

- Do you connect to free Wi-Fi in public places?
- Do you do online shopping, payment, money transfer, or
- other similar things while connected to a public Wi-Fi network?

Connection to Public Wi-Fi Networks



Things People Do on Public Wi-Fi Networks



Security Risks of Wi-Fi in Public Places

- Eighty percent of Wi-Fi networks can be easily cracked. Every year, access to public Wi-Fi networks incurs an economic loss as high as CNY 5 billion (e-Bank theft, online account theft, etc.). Below are some examples of public Wi-Fi security risks:

Unexpected

The hacker steals CNY 34,000 from the person who steals the neighbor's Wi-Fi

Shocking

A financial scam using McDonalds' Wi-Fi cost some users CNY 2000

Up-to-date

Phishing Wi-Fi in buses

Suffocating

Online game purchases accumulated over a number of years stolen by hackers

Aggrieved

Those who intend to save money may be at risk due to weak security

Harmful

Hackers routinely succeed in obtaining user password information

Chapter

04

Social Engineering

- Social engineering was first appeared in the 1960s as a formal discipline.
- Social engineering was discussed in *The Art of Deception* by the infamous hacker Kevin Mitnick, who authored the book following a prison term for hacking-related offenses. It refers to the psychological manipulation of people to give away important personal information, which can cause great damage to the victims.
- Social engineering first appeared as a formal discipline in the 1960s.



Is this an example of social engineering?

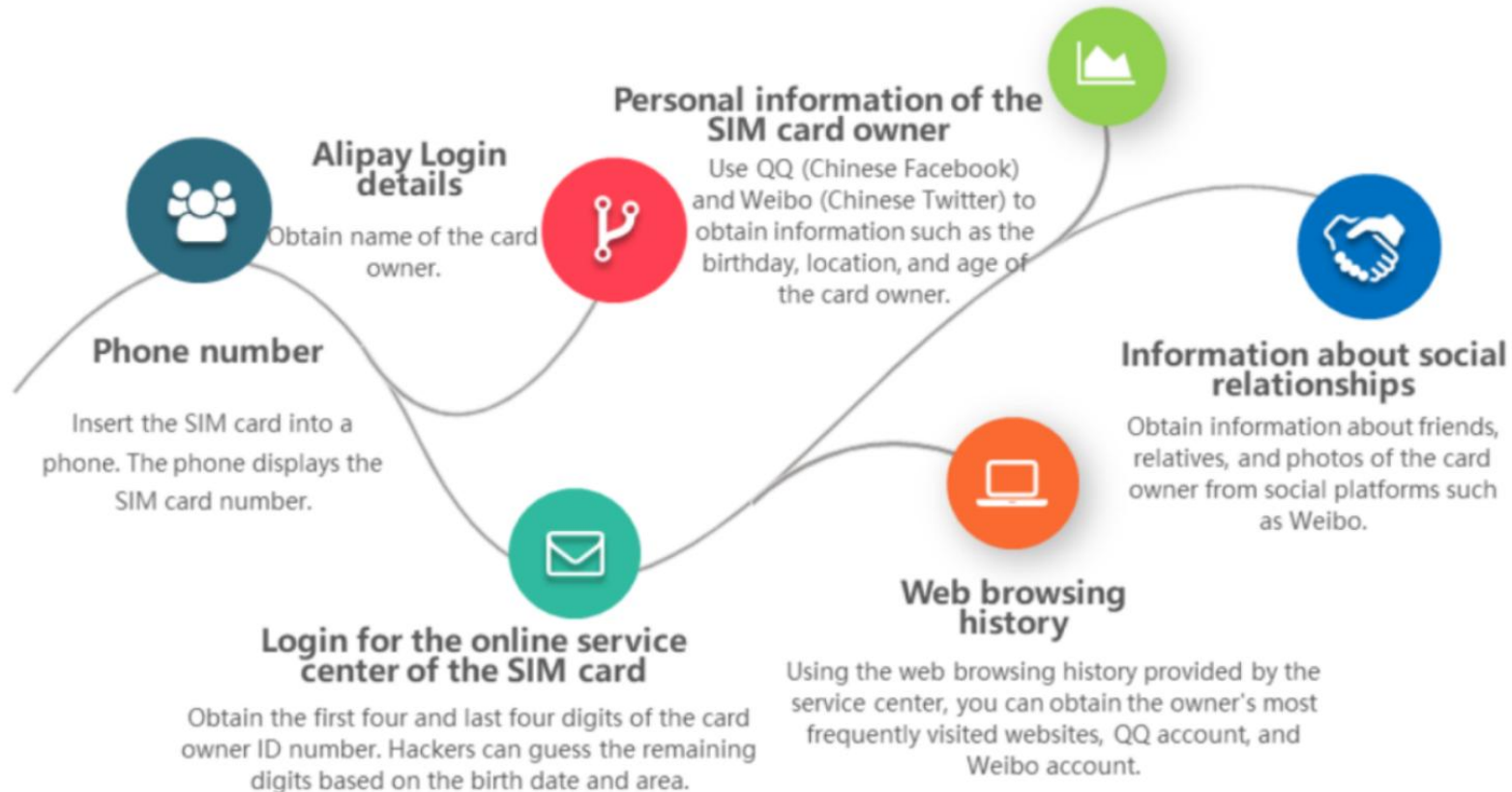
People are the weakest link.

— World's most notorious hacker Kevin Mitnick

Chapter
04

Case Study

Discussion: If you find another person's SIM card, what information can you obtain?



Fostering Security Awareness

- Remaining Vigilant When online is an effective way to defend against cyber security scams.
- Pay attention to news regarding cyber security scams so you are always aware of potential security issues.



Gartner Top 10 Security Technologies



Gartner Top 10 Security Technologies

- Gartner is the world's first information technology research and analysis company. It is also the world's leading research and advisory company.
- **Cloud workload protection platforms (CWPPs)**
 - The definition provided by Gartner is abstract and complex. In simple terms, a CWPP is a platform that protects services running on the public cloud and private cloud. The current practice is to deploy an agent at all operating systems of the service to communicate with the management console. In this way, a distributed monitoring and centralized management client/server (C/S) architecture is formed, allowing O&M personnel to conveniently monitor the security status of multiple hosts at the same time and deliver handling policies.
- **Remote browser**
 - The technology isolates the web page browsing sessions from endpoints. For example, the simplest way is to adopt graphical login to remotely log in to a host to browse web pages. Due to the isolation of the web browser by the graphical login, even if the browser is attacked, it will not harm endpoints of the users. After the browsing is complete, the host that performs the browsing task can be reset to the safest state. This technology can be provided as a service and relies on the virtualization technology. Enterprises lease remote browsing servers, and providers maintain these browsing servers.

Gartner Top 10 Security Technologies

- **Deception**

- ❑ A number of fake servers are deployed in an enterprise to decoy or mislead attackers to incorrectly judge the internal network topology of the enterprise, in turn increasing attack costs and affectivity. If an attacker intrudes into a fake server, an alarm will be generated. A fake server can even be directly embedded into a switch.

- **Endpoint Detection and Response (EDR)**

- ❑ The antivirus software deployed on endpoints is the simplest example of EDR. However, EDR provides more functions, such as identifying suspicious processes and network connections of a device through behavioral analysis. In addition, EDR can use big data technologies to collectively analyze behavior of multiple devices for potential threats. Currently, many mainstream cyber security vendors have launched EDR solutions.

- **Network traffic analysis**

- ❑ This technology detects abnormal network data through all-round enterprise or campus traffic monitoring and big data analysis technologies. For example, the technology mirrors all traffic passing through the switch to the analysis device for comprehensive decoding and statistical analysis. The technology then visualizes and displays the data to allow administrators to intuitively view the security posture of the entire network.

Firewall Development History

- **Managed detection and response**

- ☐ In simple terms, managed detection and response is a "baby-sitter" service for small and medium-sized enterprises that do not have security protection capabilities. For example, small and medium-sized enterprises access the network through a proxy of security vendors. Security vendors can analyze enterprises' network traffic 24/7 through the proxy and clean the threats in a timely manner. In addition, security vendors can push security event warnings to enterprises so that small and medium sized enterprises do not need to purchase or deploy any devices themselves.

- **Micro segmentation**

- ☐ The micro segmentation here does not refer to isolation between servers in traditional equipment rooms. It is isolation between applications. In the cloud era, instead of hosts, applications that provide services are usually perceived by users. Isolation is therefore evolved from the server level to the application level.

Firewall Security Zone

- **Cloud Access Security Brokers (CASBs)**

- ☐ This technology is used to protect cloud security. It obtains all accesses to cloud services through the reverse proxy, and conducts traffic security detection and audit to detect noncompliant and abnormal access in a timely manner, such as penetration and leakage. It is like the previous managed detection and response. The former is to protect service users and the latter is to protect service providers. This solution is generally provided as a service.

- **Software defined perimeters (SDPs)**

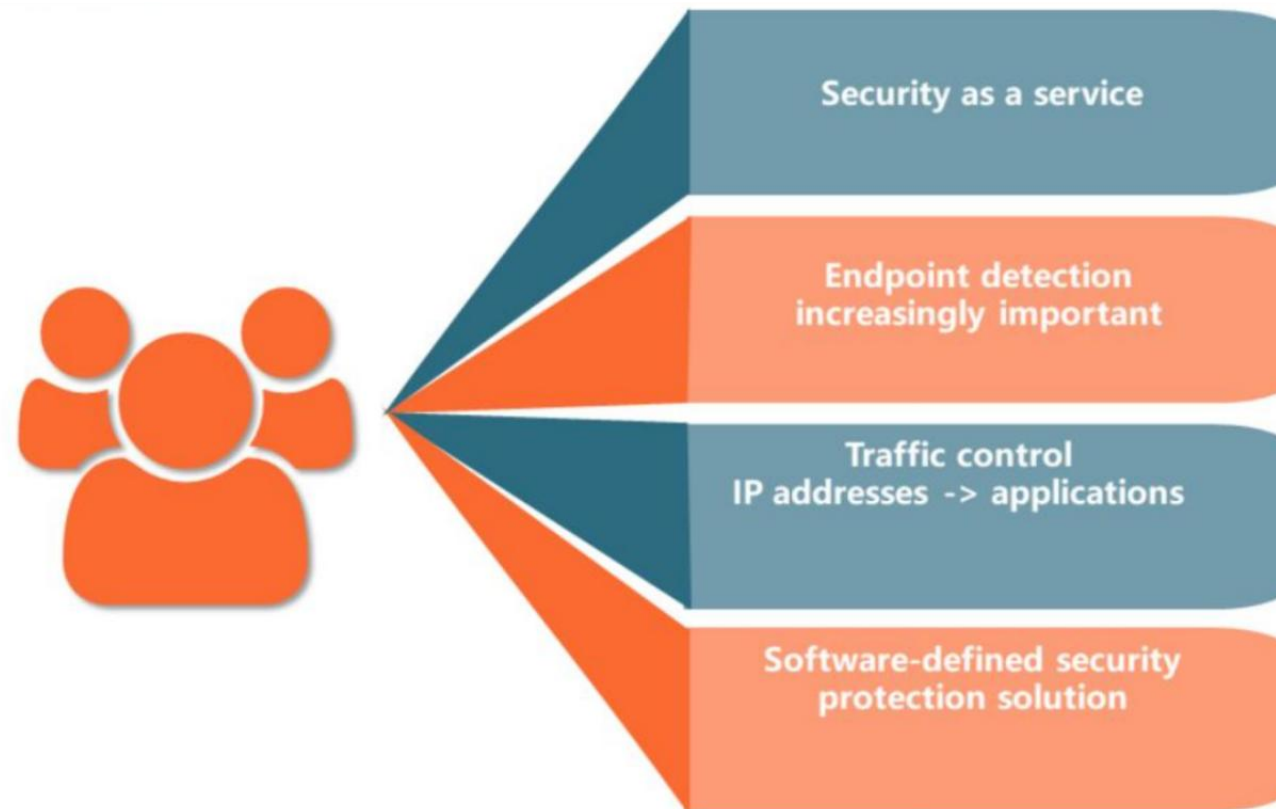
- ☐ This concept is designed to resolve the problem of flexible resource access management in the cloud era. It emphasizes on replacing traditional physical devices with software, which is the same as Software Defined Network (SDN).

- **Container security**

- ☐ Traditional security is oriented to hosts and provided for each host. In the cloud era, applications are containerized, and the concept of a host is weakened. Container security becomes very important.

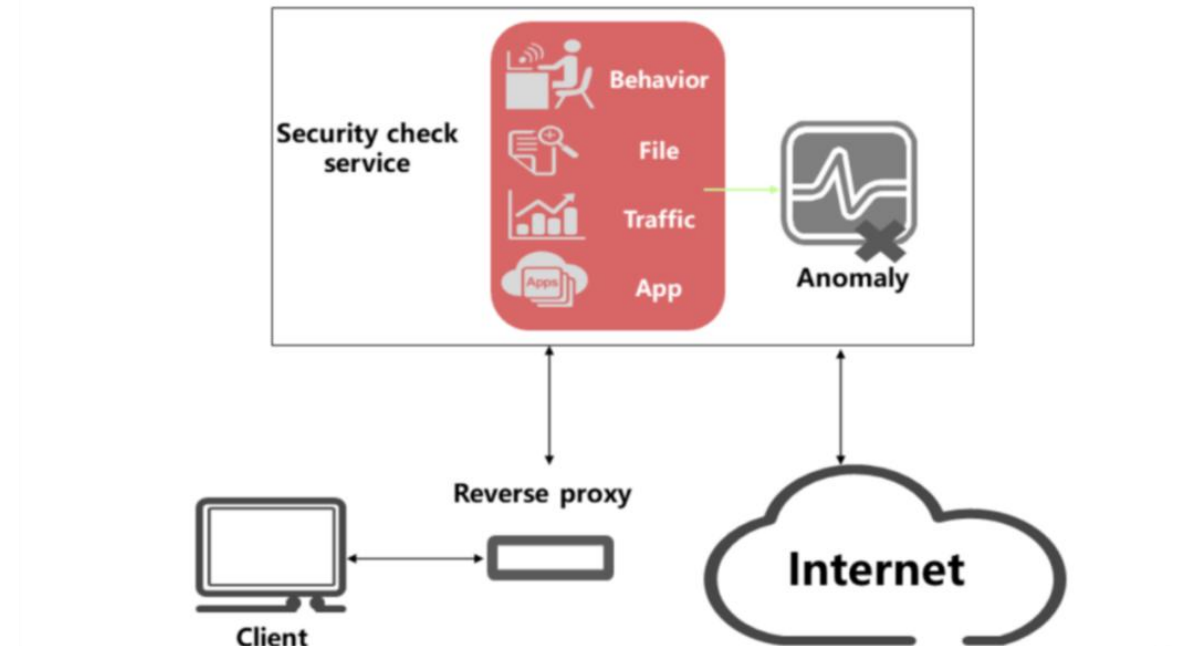
Future Development Trends of Security Protection

- The previous section described Gartner top security technologies. Now, we will summarize other future development trends.



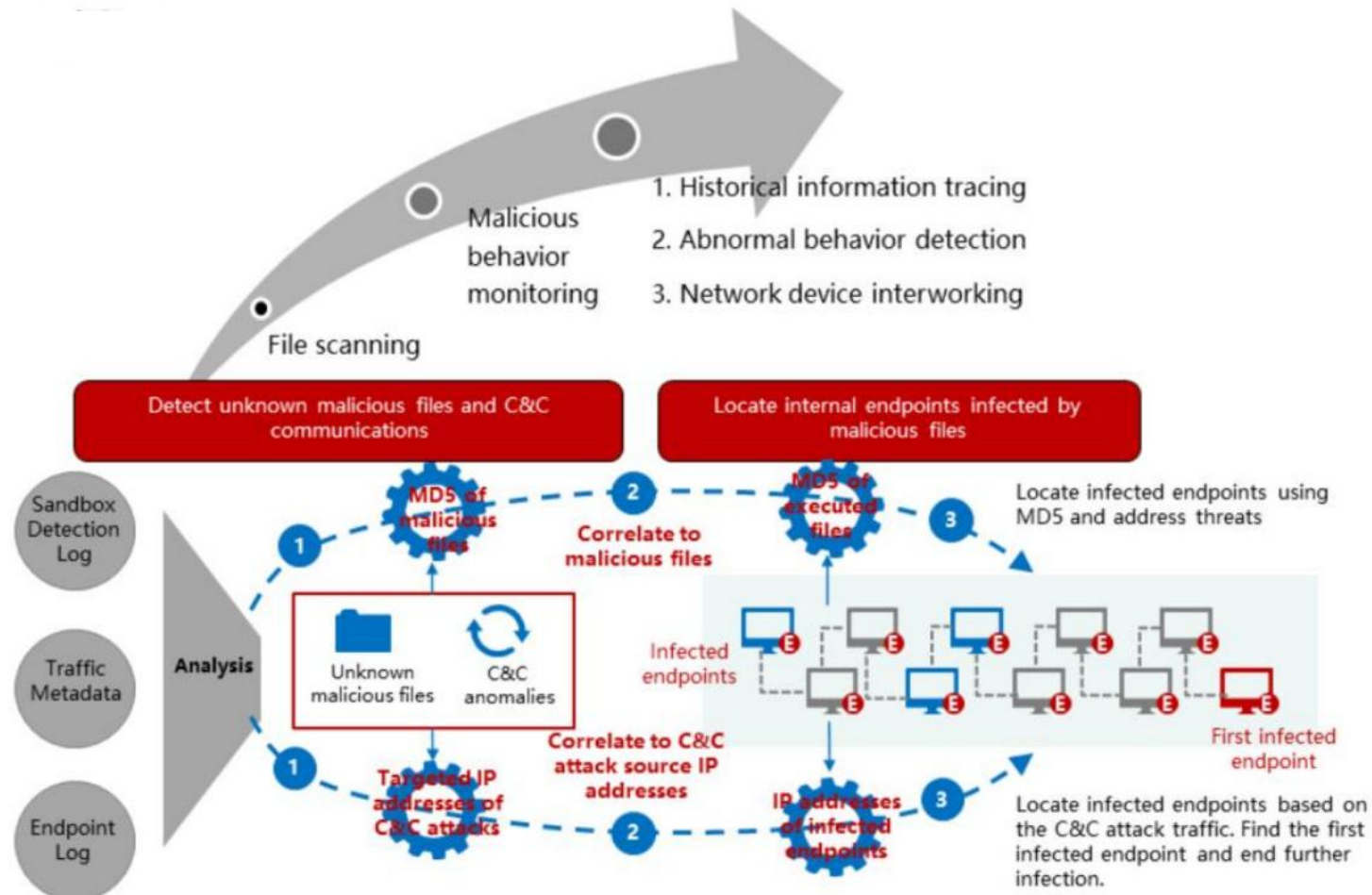
Trend 1: Security as a Service

- In the future, security protection solutions may not consist of any devices. Instead, remote security protection and analysis will be provided. Users' network access traffic is directed to the data centers of the security vendors by proxy for analysis, filtering, and cleaning. All customers need to do is to configure an address of a security proxy server. MDR and CASB are examples of this type of security services.



Chapter
04

Trend 2: Endpoint Detection Increasingly Important



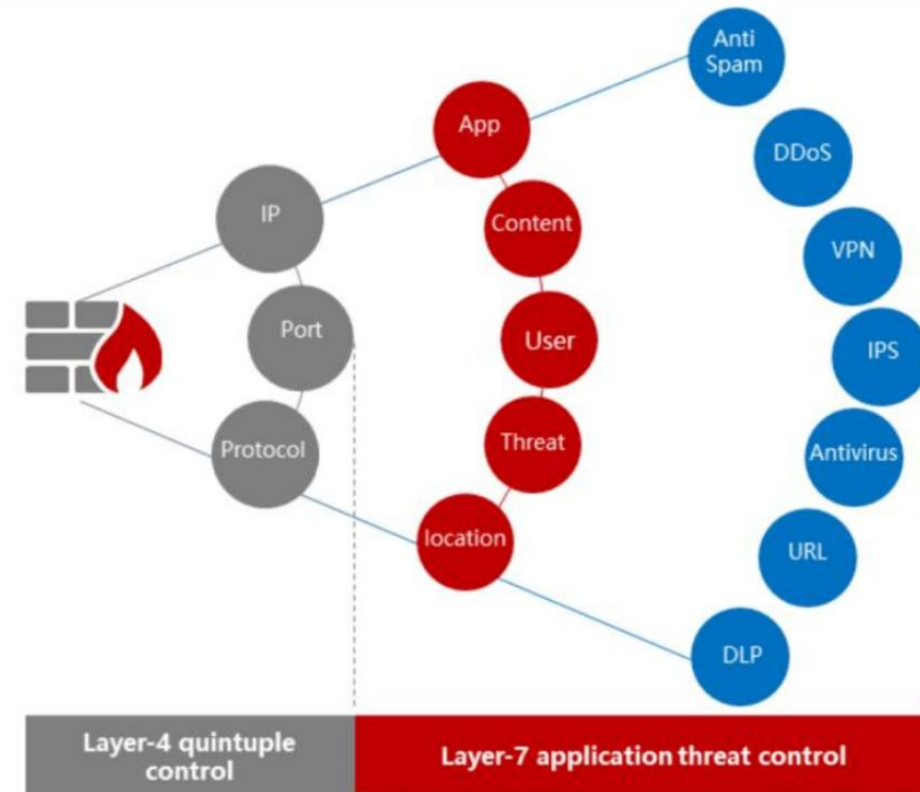
Trend 2: Endpoint Detection Increasingly Important

- In an enterprise, the antivirus software for endpoints will evolve into the EDR with a distributed monitoring and centralized analysis architecture. This allows the enterprise to analyze process behavior and context of all its hosts in a unified manner to more efficiently detect potential threats.
- The security check capability of endpoints is increasingly being used by traditional cyber security vendors. In the past, endpoint security and network security were two separate domains. Endpoint antivirus vendors only inspected files in endpoints, and network security vendors focused on network traffic. Currently, these two functions are being integrated. Due to the interworking of the endpoint security software and the network defense device, direct connection of malicious traffic to the processes and files of the endpoint is enabled, and threats are traced accurately. In the future, security software in endpoints will cooperate more closely with network defense devices.

Chapter
04

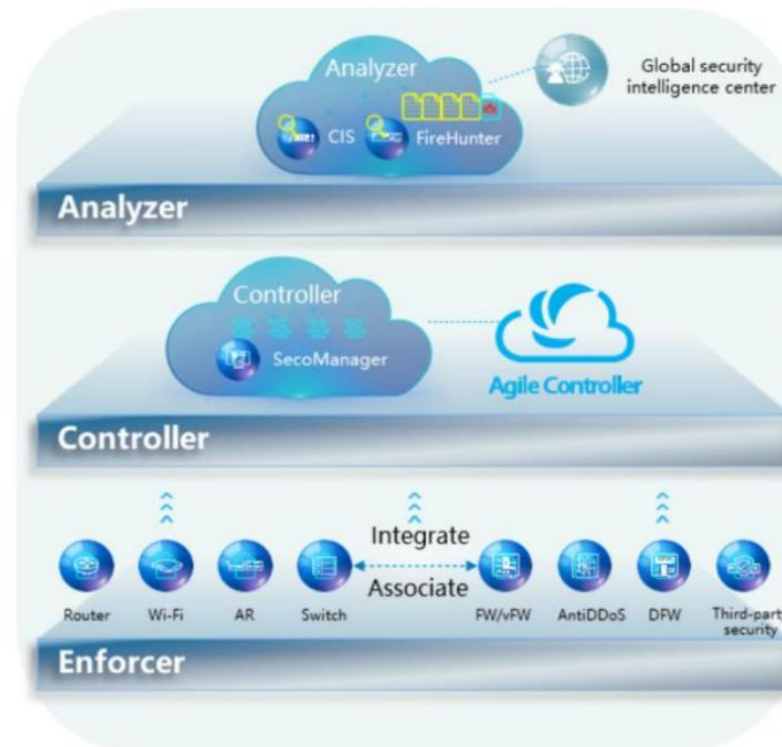
Trend 3: Traffic Control — from IP Addresses to Applications

- With the growth of micro segmentation and container security, the concept of host is weakened while the concept of service is strengthened in the cloud era. Therefore, traffic management must be implemented at the application level and container level. Network topologies viewed by O&M personnel are not host-host topologies but service-service and service-client topologies. In addition, the graphic theories and principles can be better applied to security checks to detect abnormal communication paths of the cloud data centers and potential threats in time.



Trend 4: Software-defined Security Solution (Huawei SDSec)

- All Gartner top security technologies utilize the cloud. Cloud-based deployment of security protection solutions is therefore imperative. The future of security will be based on software (Software-defined Security). All check devices will evolve into software and run-in containers or virtual hosts. Software-based solutions mean O&M personnel can conveniently change the check methods for different application data flows. For example, some application data flows need to be checked by the WAF, and some need virus scanning or IPS checks. Based on the analysis of traffic and process behavior, intelligent change can be implemented.



Detection Intelligence

- AI-based auto-learning and detection of threats, from reactive to proactive defense
- Huawei third-generation sandbox based on deep neural network algorithms



Handling Intelligence

- Cyber security collaboration, single-point defense -> network-wide associative defense
- Security service orchestration



O&M Intelligence

- Service-driven policy management, manual O&M -> intelligent O&M
- Automated service provision for tenants
- Based on automatic mapping from services to policies



Thank You