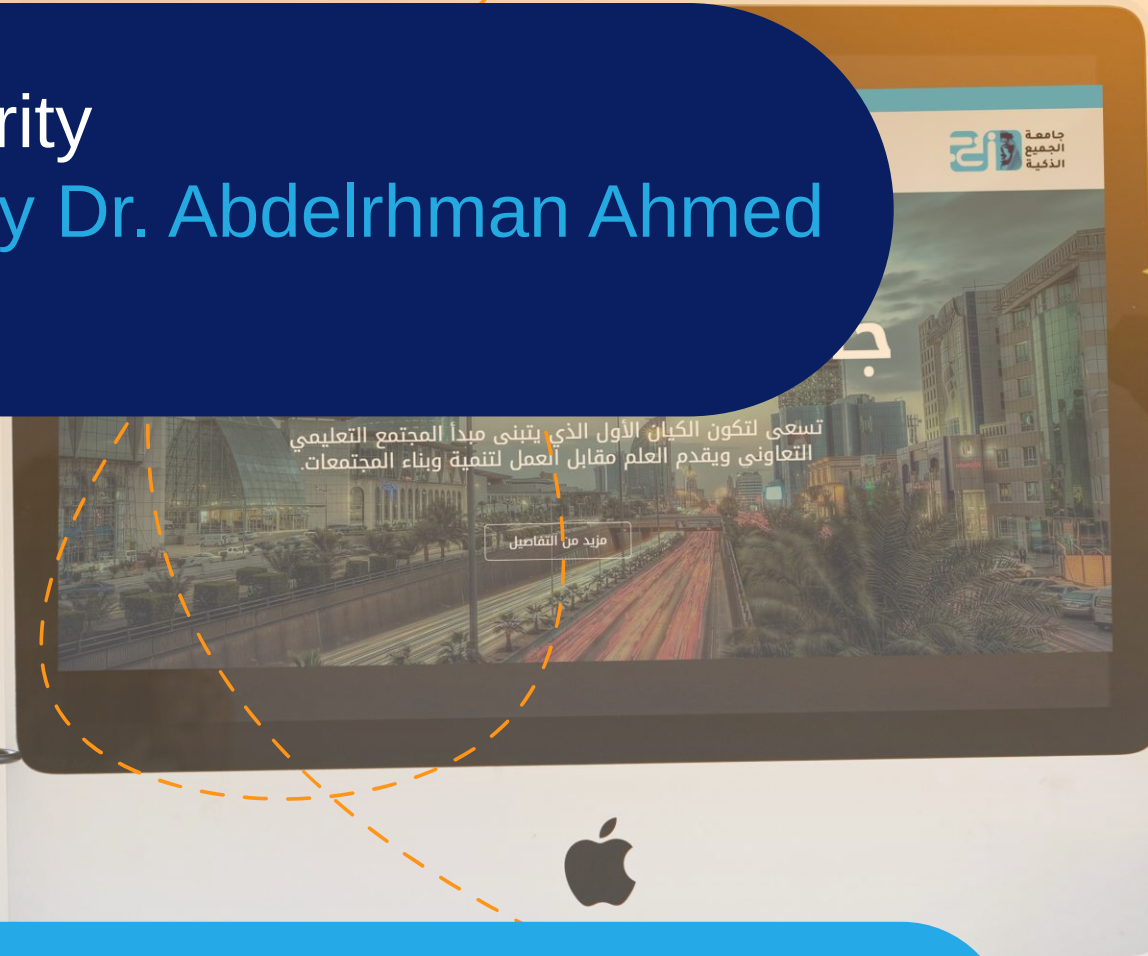


HCIA Security

Prepared by Dr. Abdelrhman Ahmed

Lecture 4

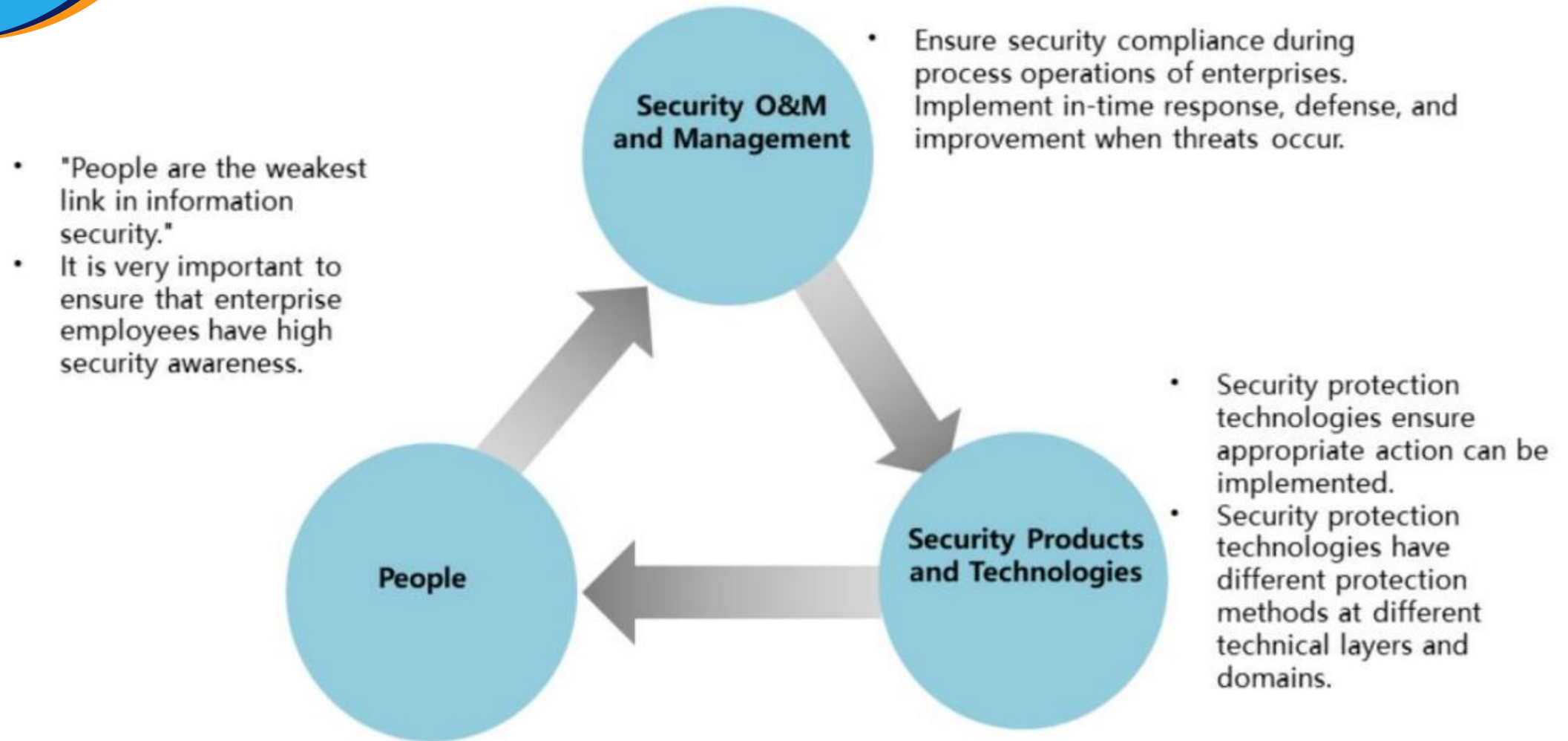


جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

Threat Defense and Information Security
Development Trends

- 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.

- **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.**



Three interconnected elements

- 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

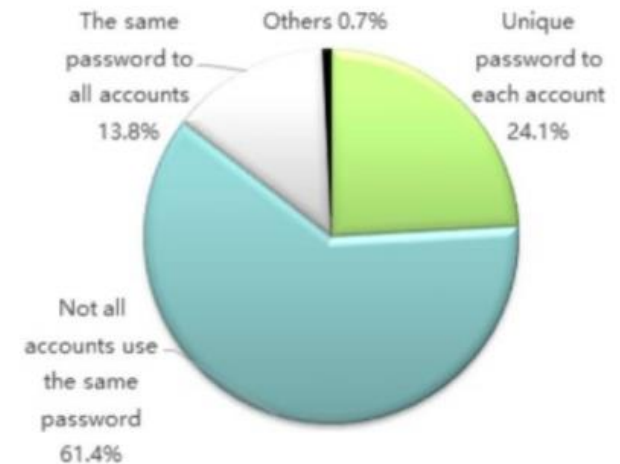
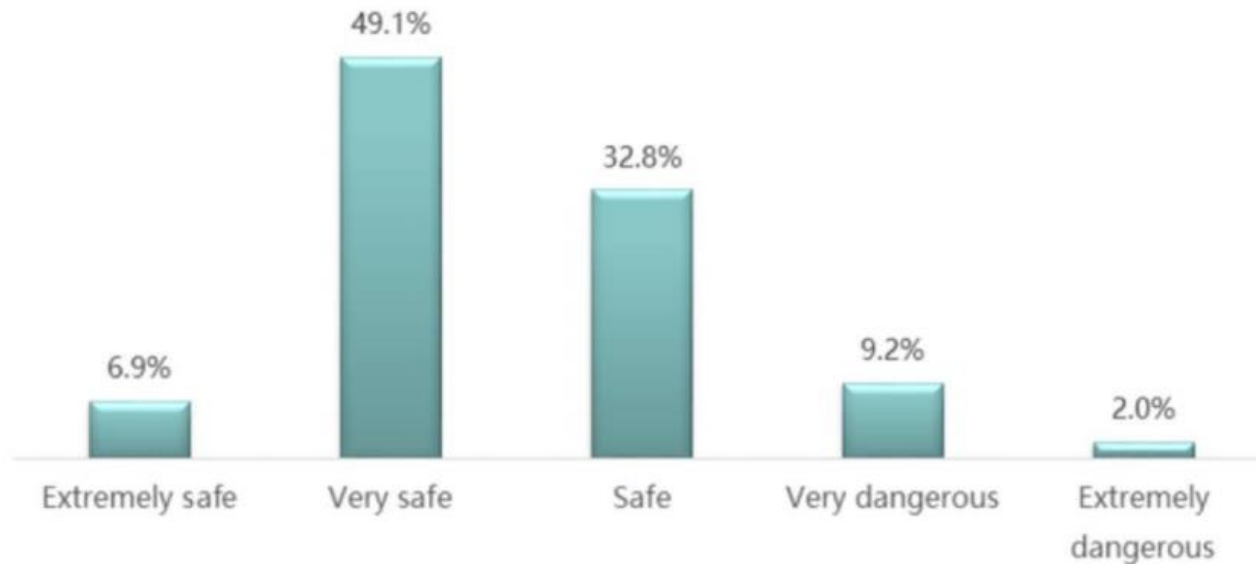
- Security operation
- Emergency response
- Disaster recovery

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

Security awareness

Cybersecurity Awareness survey

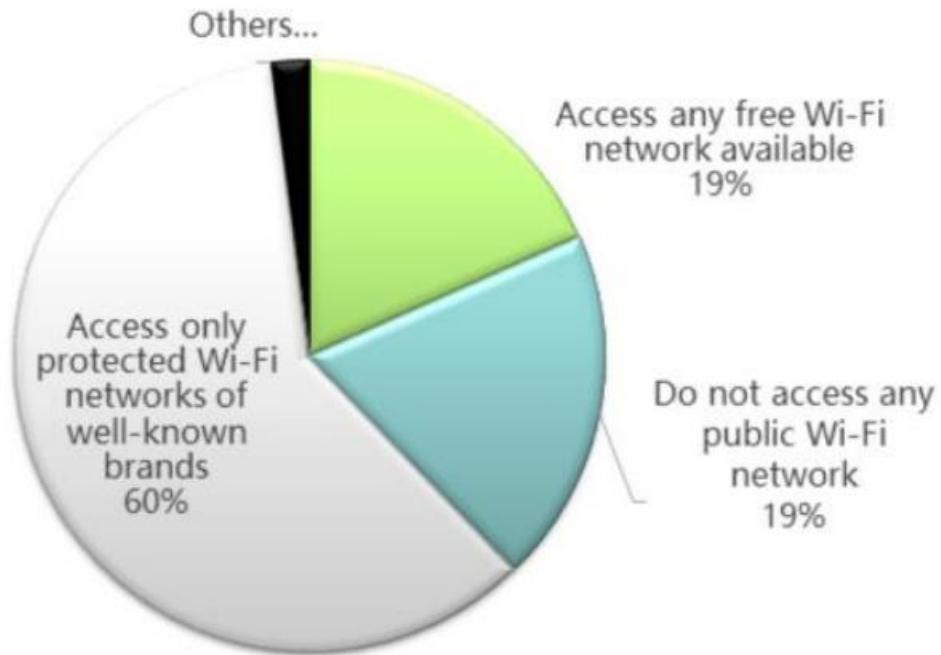
- Do you read the User Agreement in detail when you register an account?
- Do you use the same password for all your accounts?
- Do you think the current cyber environment is secure?



- 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.

- 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



Wall of Sheep

Name	Score	Time	Date
100,000	100,000	00:00	2012/12/12
99,999	99,999	00:00	2012/12/12
99,998	99,998	00:00	2012/12/12
99,997	99,997	00:00	2012/12/12
99,996	99,996	00:00	2012/12/12
99,995	99,995	00:00	2012/12/12
99,994	99,994	00:00	2012/12/12
99,993	99,993	00:00	2012/12/12
99,992	99,992	00:00	2012/12/12
99,991	99,991	00:00	2012/12/12
99,990	99,990	00:00	2012/12/12
99,989	99,989	00:00	2012/12/12
99,988	99,988	00:00	2012/12/12
99,987	99,987	00:00	2012/12/12
99,986	99,986	00:00	2012/12/12
99,985	99,985	00:00	2012/12/12
99,984	99,984	00:00	2012/12/12
99,983	99,983	00:00	2012/12/12
99,982	99,982	00:00	2012/12/12
99,981	99,981	00:00	2012/12/12
99,980	99,980	00:00	2012/12/12
99,979	99,979	00:00	2012/12/12
99,978	99,978	00:00	2012/12/12
99,977	99,977	00:00	2012/12/12
99,976	99,976	00:00	2012/12/12
99,975	99,975	00:00	2012/12/12
99,974	99,974	00:00	2012/12/12
99,973	99,973	00:00	2012/12/12
99,972	99,972	00:00	2012/12/12
99,971	99,971	00:00	2012/12/12
99,970	99,970	00:00	2012/12/12
99,969	99,969	00:00	2012/12/12
99,968	99,968	00:00	2012/12/12
99,967	99,967	00:00	2012/12/12
99,966	99,966	00:00	2012/12/12
99,965	99,965	00:00	2012/12/12
99,964	99,964	00:00	2012/12/12
99,963	99,963	00:00	2012/12/12
99,962	99,962	00:00	2012/12/12
99,961	99,961	00:00	2012/12/12
99,960	99,960	00:00	2012/12/12
99,959	99,959	00:00	2012/12/12
99,958	99,958	00:00	2012/12/12
99,957	99,957	00:00	2012/12/12
99,956	99,956	00:00	2012/12/12
99,955	99,955	00:00	2012/12/12
99,954	99,954	00:00	2012/12/12
99,953	99,953	00:00	2012/12/12
99,952	99,952	00:00	2012/12/12
99,951	99,951	00:00	2012/12/12
99,950	99,950	00:00	2012/12/12
99,949	99,949	00:00	2012/12/12
99,948	99,948	00:00	2012/12/12
99,947	99,947	00:00	2012/12/12
99,946	99,946	00:00	2012/12/12
99,945	99,945	00:00	2012/12/12
99,944	99,944	00:00	2012/12/12
99,943	99,943	00:00	2012/12/12
99,942	99,942	00:00	2012/12/12
99,941	99,941	00:00	2012/12/12
99,940	99,940	00:00	2012/12/12
99,939	99,939	00:00	2012/12/12
99,938	99,938	00:00	2012/12/12
99,937	99,937	00:00	2012/12/12
99,936	99,936	00:00	2012/12/12
99,935	99,935	00:00	2012/12/12
99,934	99,934	00:00	2012/12/12
99,933	99,933	00:00	2012/12/12
99,932	99,932	00:00	2012/12/12
99,931	99,931	00:00	2012/12/12
99,930	99,930	00:00	2012/12/12
99,929	99,929	00:00	2012/12/12
99,928	99,928	00:00	2012/12/12
99,927	99,927	00:00	2012/12/12
99,926	99,926	00:00	2012/12/12
99,925	99,925	00:00	2012/12/12
99,924	99,924	00:00	2012/12/12
99,923	99,923	00:00	2012/12/12
99,922	99,922	00:00	2012/12/12
99,921	99,921	00:00	2012/12/12
99,920	99,920	00:00	2012/12/12
99,919	99,919	00:00	2012/12/12
99,918	99,918	00:00	2012/12/12
99,917	99,917	00:00	2012/12/12
99,916	99,916	00:00	2012/12/12
99,915	99,915	00:00	2012/12/12
99,914	99,914	00:00	2012/12/12
99,913	99,913	00:00	2012/12/12
99,912	99,912	00:00	2012/12/12
99,911	99,911	00:00	2012/12/12
99,910	99,910	00:00	2012/12/12
99,909	99,909	00:00	2012/12/12
99,908	99,908	00:00	2012/12/12
99,907	99,907	00:00	2012/12/12
99,906	99,906	00:00	2012/12/12
99,905	99,905	00:00	2012/12/12
99,904	99,904	00:00	2012/12/12
99,903	99,903	00:00	2012/12/12
99,902	99,902	00:00	2012/12/12
99,901	99,901	00:00	2012/12/12
99,900	99,900	00:00	2012/12/12
99,899	99,899	00:00	2012/12/12
99,898	99,898	00:00	2012/12/12
99,897	99,897	00:00	2012/12/12
99,896	99,896	00:00	2012/12/12
99,895	99,895	00:00	2012/12/12
99,894	99,894	00:00	2012/12/12
99,893	99,893	00:00	2012/12/12
99,892	99,892	00:00	2012/12/12
99,891	99,891	00:00	2012/12/12
99,890	99,890	00:00	2012/12/12
99,889	99,889	00:00	2012/12/12
99,888	99,888	00:00	2012/12/12
99,887	99,887	00:00	2012/12/12
99,886	99,886	00:00	2012/12/12
99,885	99,885	00:00	2012/12/12
99,884	99,884	00:00	2012/12/12
99,883	99,883	00:00	2012/12/12
99,882	99,882	00:00	2012/12/12
99,881	99,881	00:00	2012/12/12
99,880	99,880	00:00	2012/12/12
99,879	99,879	00:00	2012/12/12
99,878	99,878	00:00	2012/12/12
99,877	99,877	00:00	2012/12/12
99,876	99,876	00:00	2012/12/12
99,875	99,875	00:00	2012/12/12
99,874	99,874	00:00	2012/12/12
99,873	99,873	00:00	2012/12/12
99,872	99,872	00:00	2012/12/12
99,871	99,871	00:00	2012/12/12
99,870	99,870	00:00	2012/12/12
99,869	99,869	00:00	2012/12/12
99,868	99,868	00:00	2012/12/12
99,867	99,867	00:00	2012/12/12
99,866	99,866	00:00	2012/12/12
99,865	99,865	00:00	2012/12/12
99,864	99,864	00:00	2012/12/12
99,863	99,863	00:00	2012/12/12
99,862	99,862	00:00	2012/12/12
99,861	99,861	00:00	2012/12/12
99,860	99,860	00:00	2012/12/12
99,859	99,859	00:00	2012/12/12
99,858	99,858	00:00	2012/12/12
99,857	99,857	00:00	2012/12/12
99,856	99,856	00:00	2012/12/12
99,855	99,855	00:00	2012/12/12
99,854	99,854	00:00	2012/12/12
99,853	99,853	00:00	2012/12/12
99,852	99,852	00:00	2012/12/12
99,851	99,851	00:00	2012/12/12
99,850	99,850	00:00	2012/12/12
99,849	99,849	00:00	2012/12/12
99,848	99,848	00:00	2012/12/12
99,847	99,847	00:00	2012/12/12
99,846	99,846	00:00	2012/12/12
99,845	99,845	00:00	2012/12/12
99,844	99,844	00:00	2012/12/12
99,843	99,843	00:00	2012/12/12
99,842	99,842	00:00	2012/12/12
99,841	99,841	00:00	2012/12/12
99,840	99,840	00:00	2012/12/12
99,839	99,839	00:00	2012/12/12
99,838	99,838	00:00	2012/12/12
99,837	99,837	00:00	2012/12/12
99,836	99,836	00:00	2012/12/12
99,835	99,835	00:00	2012/12/12
99,834	99,834	00:00	2012/12/12
99,833	99,833	00:00	2012/12/12
99,832	99,832	00:00	2012/12/12
99,831	99,831	00:00	2012/12/12
99,830	99,830	00:00	2012/12/12
99,829	99,829	00:00	2012/12/12
99,828	99,828	00:00	2012/12/12
99,827	99,827	00:00	2012/12/12
99,826	99,826	00:00	2012/12/12
99,825	99,825	00:00	2012/12/12
99,824	99,824	00:00	2012/12/12
99,823	99,823	00:00	2012/12/12
99,822	99,822	00:00	2012/12/12
99,821	99,821	00:00	2012/12/12
99,820	99,820	00:00	2012/12/12
99,819	99,819	00:00	2012/12/12
99,818	99,818	00:00	2012/12/12
99,817	99,817	00:00	2012/12/12
99,816	99,816	00:00	2012/12/12
99,815	99,815	00:00	2012/12/12
99,814	99,814	00:00	2012/12/12
99,813	99,813	00:00	2012/12/12
99,812	99,812	00:00	2012/12/12
99,811	99,811	00:00	2012/12/12
99,810	99,810	00:00	2012/12/12
99,809	99,809	00:00	2012/12/12
99,808	99,808	00:00	2012/12/12
99,807	99,807	00:00	2012/12/12
99,806	99,806	00:00	2012/12/12
99,805	99,805	00:00	2012/12/12
99,804	99,804	00:00	2012/12/12
99,803	99,803	00:00	2012/12/12
99,802	99,802	00:00	2012/12/12
99,801	99,801	00:00	2012/12/12
99,800	99,800	00:00	2012/12/12
99,799	99,799	00:00	2012/12/12
99,798	99,798	00:00	2012/12/12
99,797	99,797	00:00	2012/12/12
99,796	99,796	00:00	2012/12/12
99,795	99,795	00:00	2012/12/12
99,794	99,794	00:00	2012/12/12
99,793	99,793	00:00	2012/12/12
99,792	99,792	00:00	2012/12/12
99,791	99,791	00:00	2012/12/12
99,790	99,790	00:00	2012/12/12
99,789	99,789	00:00	2012/12/12
99,788	99,788	00:00	2012/12/12
99,787	99,787	00:00	2012/12/12
99,786	99,786	00:00	2012/12/12
99,785	99,785	00:00	2012/12/12
99,784	99,784	00:00	2012/12/12
99,783	99,783	00:00	2012/12/12
99,782	99,782	00:00	2012/12/12
99,781	99,781	00:00	2012/12/12
99,780	99,780	00:00	2012/12/12
99,779	99,779	00:00	2012/12/12
99,778	99,778	00:00	2012/12/12
99,777	99,777	00:00	2012/12/12
99,776	99,776	00:00	2012/12/12
99,775	99,775	00:00	2012/12/12
99,774	99,774	00:00	2012/12/12
99,773	99,773	00:00	2012/12/12
99,772	99,772	00:00	2012/12/12
99,771	99,771	00:00	2012/12/12
99,770	99,770	00:00	2012/12/12
99,769	99,769	00:00	20

- 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

- 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.

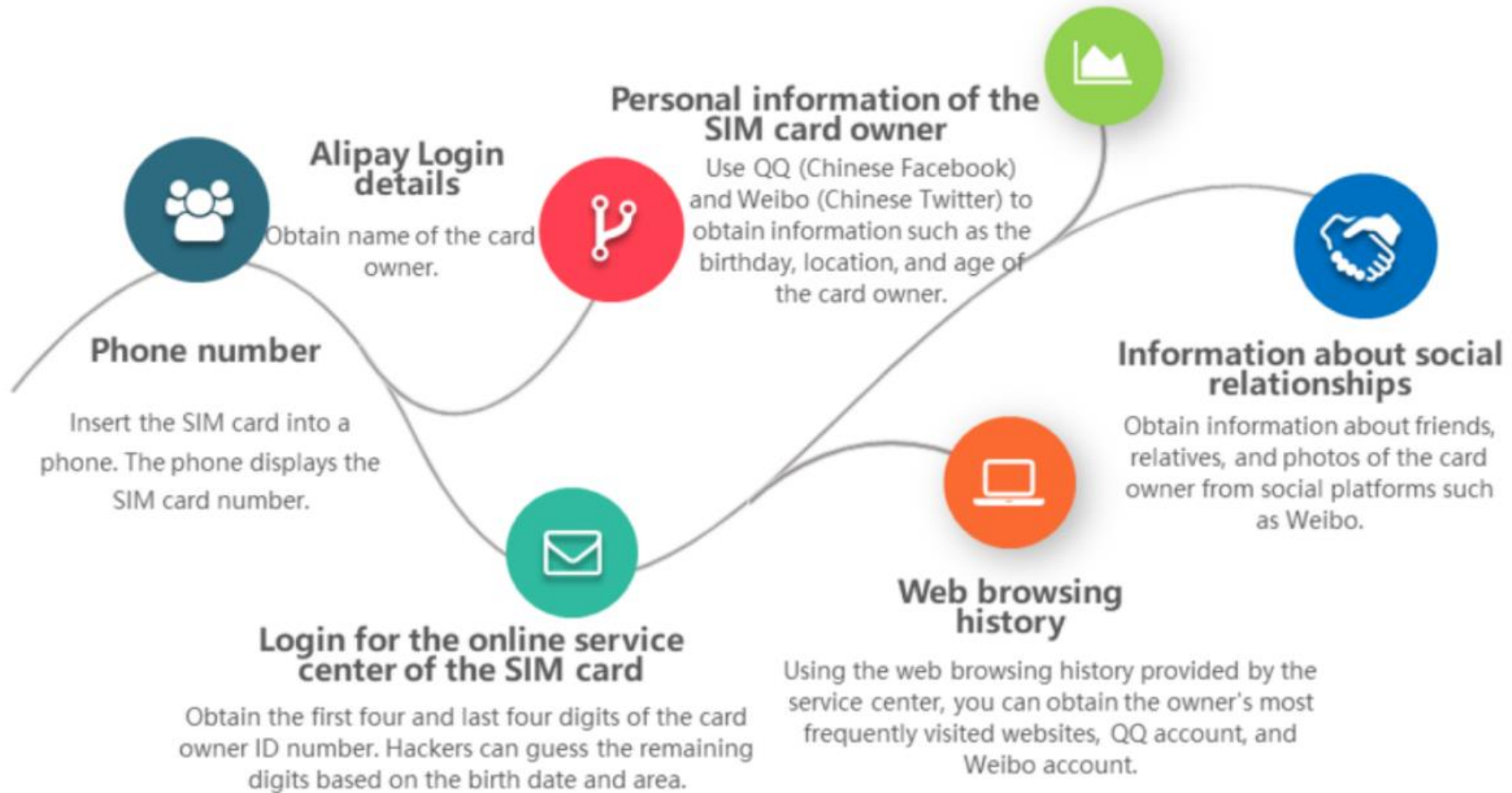


Is this an example of social engineering?

People are the weakest link.

— World's most notorious hacker Kevin Mitnick

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



- 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 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.

- **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.

- **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.

- **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)**

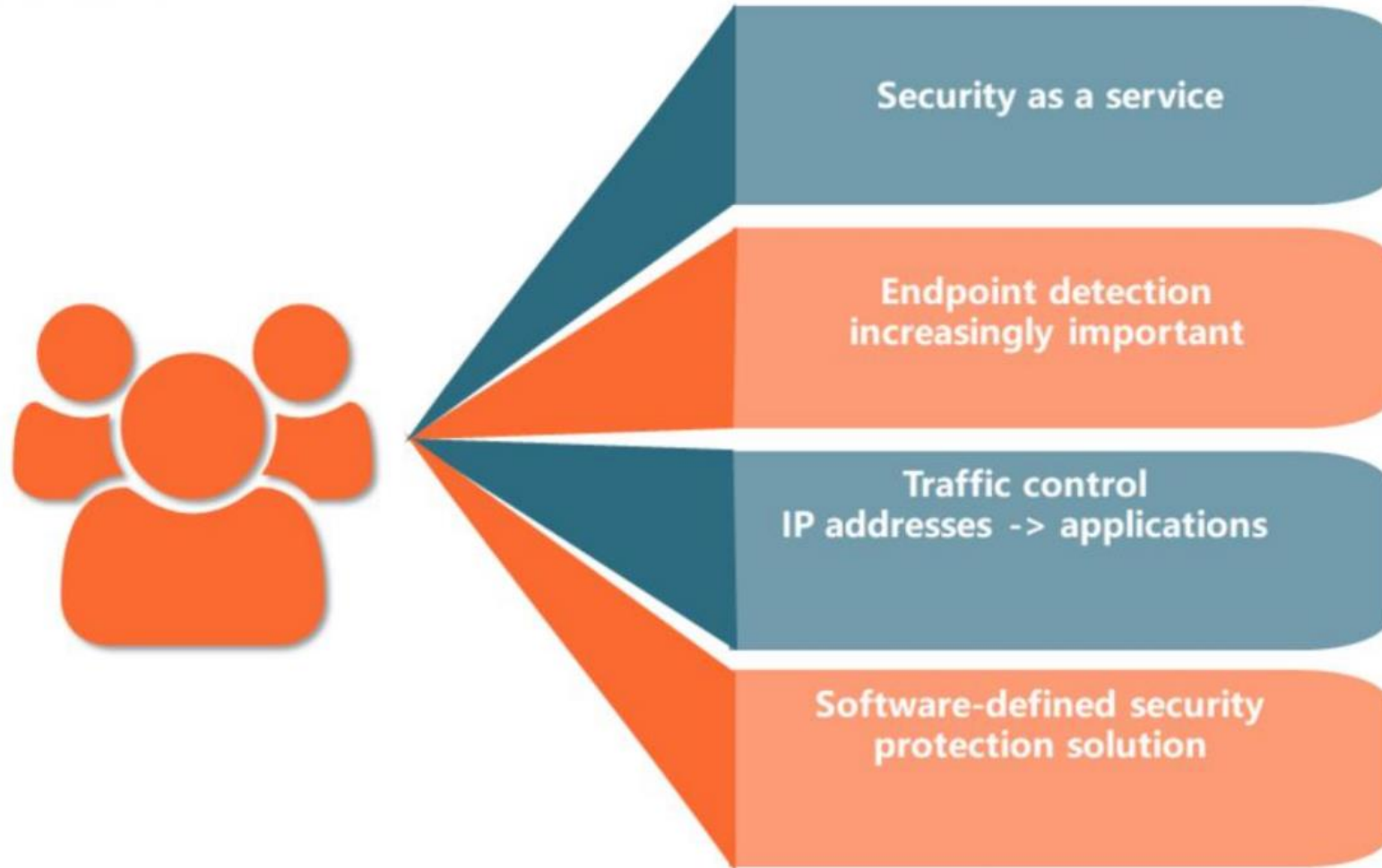
- This concept is designed to resolve the problem of flexible resource access management in the cloud era. It emphasizes on replacing traditional physical devices with software, which is the same as Software Defined Network (SDN).

- **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.

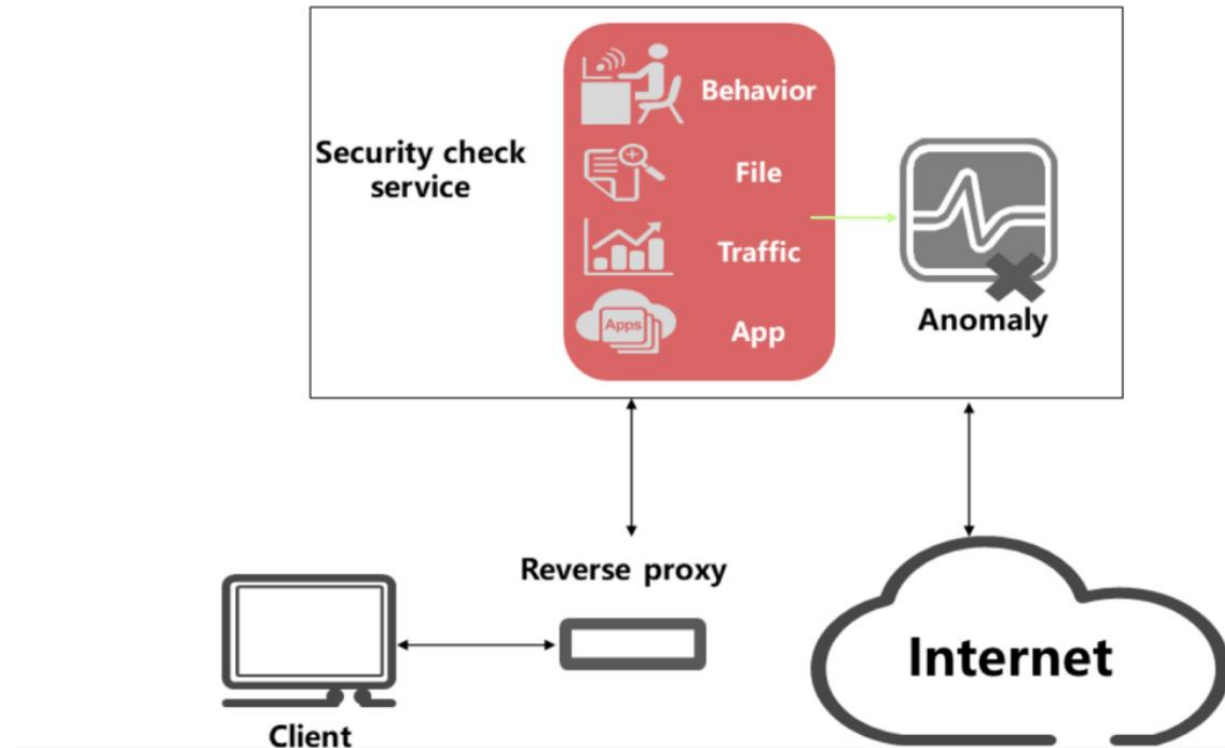
Future Development Trends of Security Protection

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

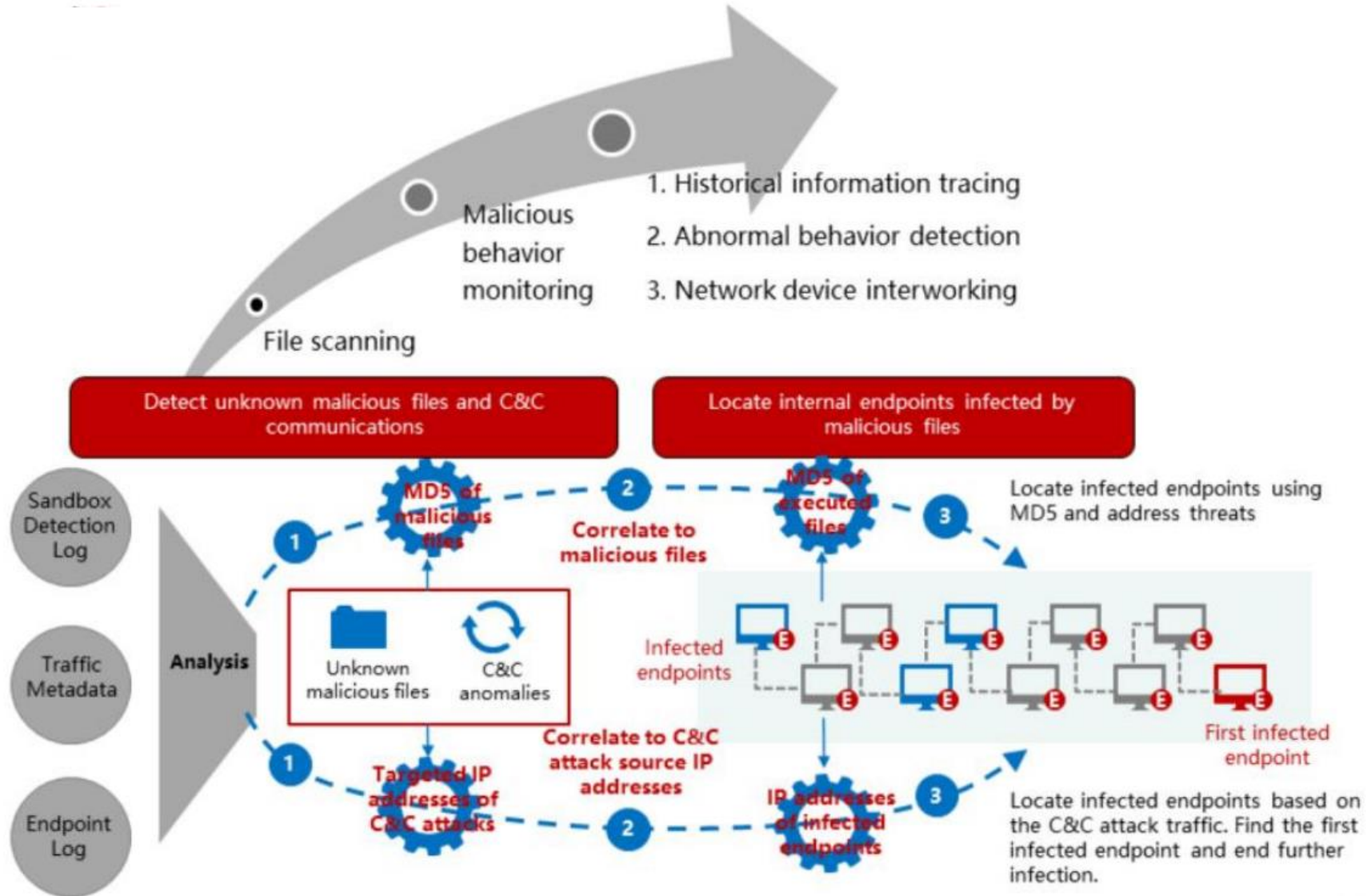


Trend 1: Security as a Service

- 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.



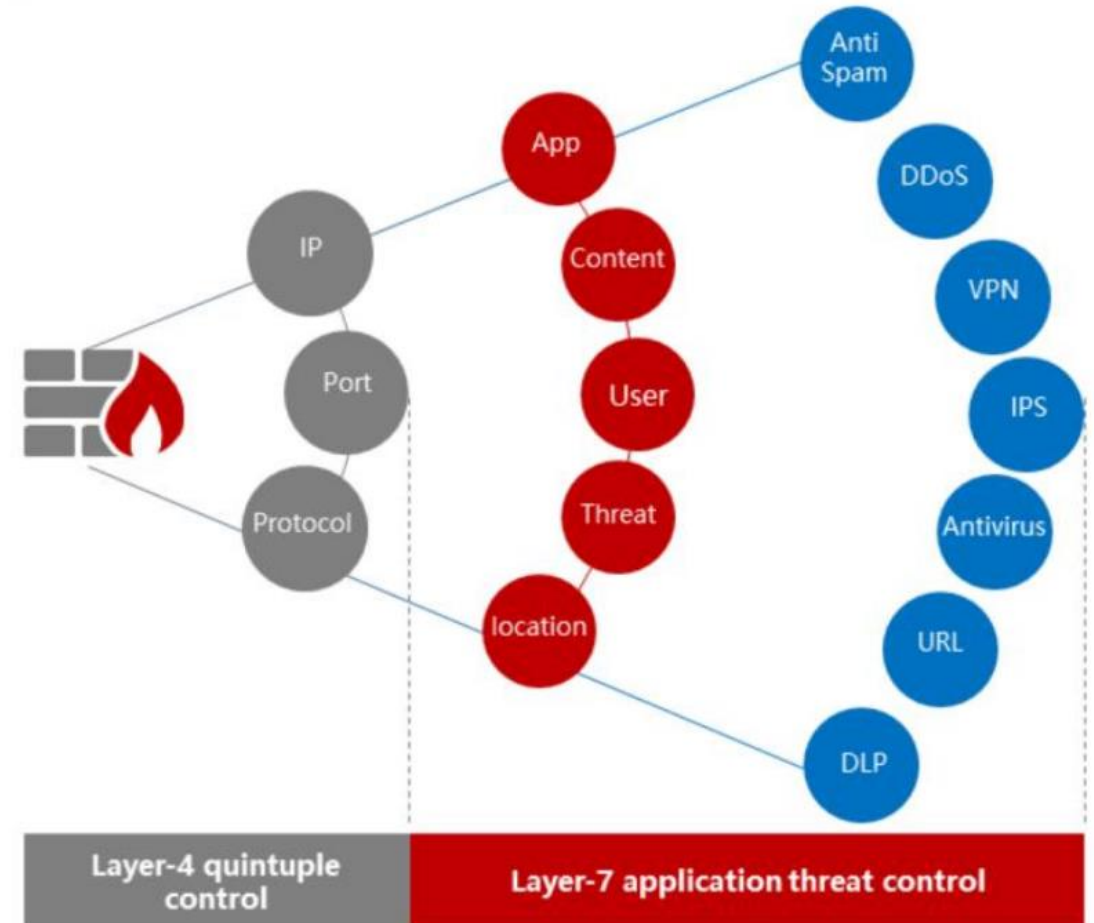
Trend 2: Endpoint Detection Increasingly Important



- 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.

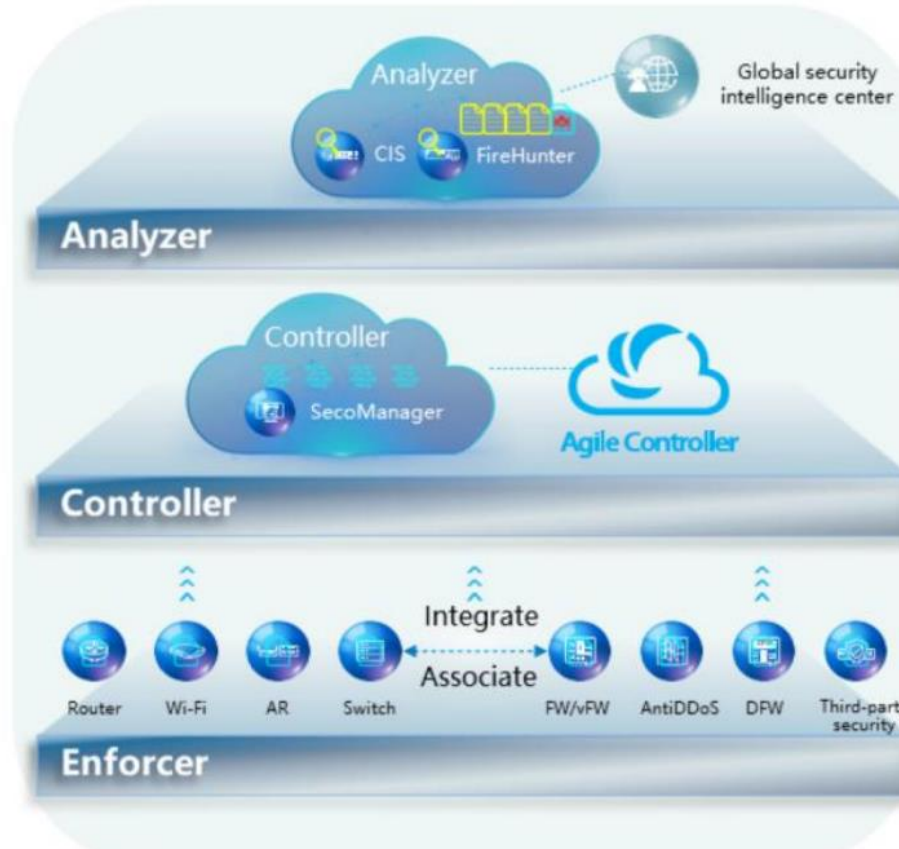
Trend 3: Traffic Control — from IP Addresses to Applications

- 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



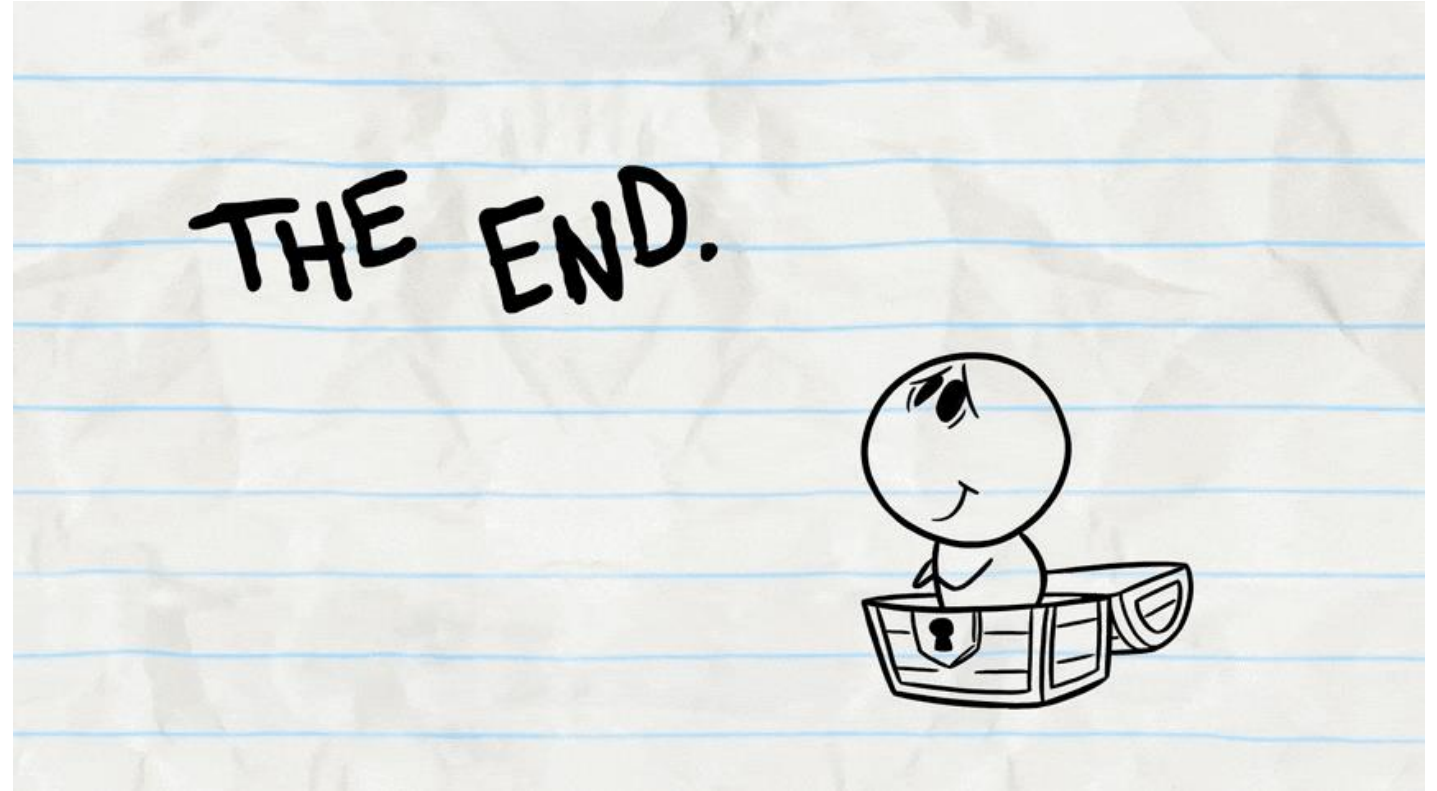
O&M Intelligence

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

The End

Please feel free to contact me anytime if you have any questions

Abdelrhman Ahmed Refaat:
abdelrhmanahmedrefaat@gmail.com



جامعة القادسية
EVERYONE'S SMART UNIVERSITY