IDC | ANALYZE THE FUTURE

SANGFOR

Future-Proof Effective Protection

Safeguarding Digital Transformation for Enterprises

Executive Summary

With the frequent occurrence of cyberattacks on a global scale, the crisis, caused by cyber security issues, is becoming unprecedentedly severe, which has turned into a huge obstacle to the digital transformation of enterprises worldwide. IDC believes that enterprises around the world, including China, have entered the period of multiplied innovation in the process of digital transformation. Large numbers of new business systems based on third platform technology are put on line on a large scale. A lot of potential security threats may exist in these new business systems, and the risks brought by these threats are much greater than those of the traditional business systems. IDC predicts that by 2022, the number of all kinds of newly developed applications will reach 500 million, equivalent to the total of the past 40 years. In such a rapid process of digital transformation, it is particularly important for enterprises to adopt scientific methods to build a security protection system that meets their own needs.

Based on the current global cybersecurity situation, this white paper will expound the fundamental reasons why enterprises need to continue cybersecurity construction, namely:

Potential threats increase as IT systems boost during digital transformation

Emerging IT systems are the core force driving digital transformation in all walks of life around the world. However, with the increase of new IT systems, security threats are also growing. Therefore, it is of great necessity to continue cybersecurity construction.

New technologies are deeply utilized in the black industry

To improve attack efficiency, expand its impact and achieve its purpose, attackers will often make more active use of new technologies such as AI, cloud computing and IoT. Therefore, defenders must continue to strengthen their cybersecurity construction, so as to effectively cope with attacks.

Close cybersecurity protection becomes a necessity

In the process of digital transformation, the IT department and business departments have shifted from their past practice of doing things on their own to in-depth integration. Cybersecurity construction has become an indispensable part to ensure the smooth digital transformation of enterprises.

At the same time, in relation to IDC's global and China's research, this white paper puts forward four points that enterprises need to pay attention to in the process of cybersecurity system planning and building, namely:

Idea

Passive defense can hardly meet the demand of cybersecurity safeguard under the trend of global digital transformation. Building an active defense system on the digital transformation platform based on threat intelligence and analysis has become the mainstream idea of cybersecurity construction in the world.

Cooperation

With so many cybersecurity products available in the market, cybersecurity construction requires the support of various product suppliers. Therefore, it is necessary for enterprises to build a largely integrated technology ecosystem. In addition, enterprises need to make different investments in cybersecurity construction in different stages of their development. The assistance of "external brain" can help enterprises to build cybersecurity in the most cost-effective way.

Leveraging

Enterprise's cybersecurity safeguard is inseparable from security management. With the wide application of third platform technology, security management has being increasingly difficult, making it hard for enterprises to analyze cyberattacks timely and accurately on their own. With the help of management security service providers (MSSPs), enterprises can effectively improve their cyberattack management.

Leadership

New technologies make attacks more effect. Therefore, the defender must continue to introduce innovative technologies to enhance its system defense capability. At present, AI technology is being fast applied in various industries worldwide. In the cybersecurity industry, AI-enabled analysis platforms will help enterprises to optimize their judgment on attacks and improve handling speed. Therefore, AI technology will become a must to be introduced into cybersecurity defense systems in the next few years.

This white paper can serve as a reference for organizations to formulate their cybersecurity strategy development plans. Meanwhile, it can also provide a reference for organizations to build their own cybersecurity defense systems.

Table of Contents

Index of Figures

01
Digital Trust Faces Challenges

1.1 Threat Escalation in the Digital Age

Currently, the Fourth Industrial Revolution with artificial intelligence (AI), robotics technology and virtual reality (VR) as breakthroughs is in full swing all over the world. These technologies have continuously pushed forward the development of the digital era, while bringing unprecedented opportunities and challenges for enterprises to carry out digital transformation and upgrading. Cybersecurity in the digital age is also becoming increasingly severe as threats escalate.

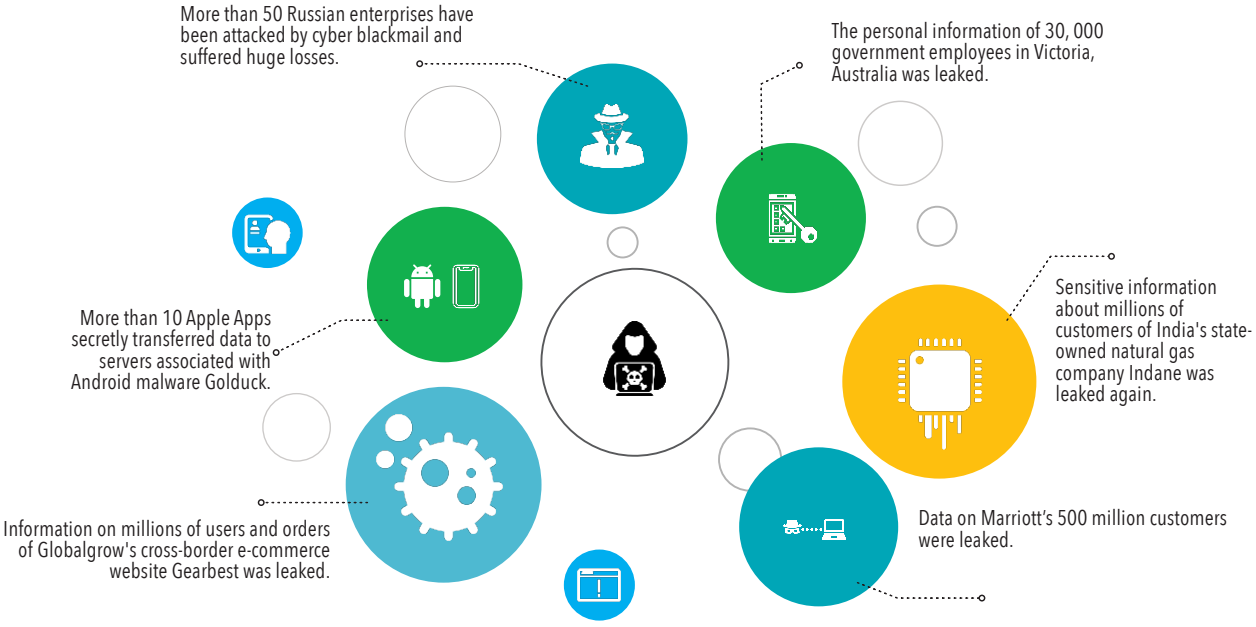
1.1.1 Attacks are Everywhere

As the Internet has spread around the world, attacks are now everywhere in the cyberspace, and the "manipulated machine" of cyber attackers can be found in all corners of the world. No country, enterprise or even individual can be immune to the increasingly rampant cyberattacks. Currently, global cyberattacks show the characteristics of being frequent, diversified and highly concealed.

Being Frequent

In recent years, the number of cybersecurity incidents in the world has increased dramatically. In 2019 alone, there were over one hundred cybersecurity incidents with great impact happened. For example, more than 50 companies in Russia have been under cyberattacks. The attackers blackmailed many enterprises by infecting their encrypted corporate infrastructure, causing huge losses to enterprises. In Australia, detailed data on more than 30,000 civil servants in the Victorian state government have been leaked. A dozen Apple Apps have been infected with malware, transmitting data to servers related to Android malware Golduck.

Figure 1 Well-known Cybersecurity Incidents in the World in 2019

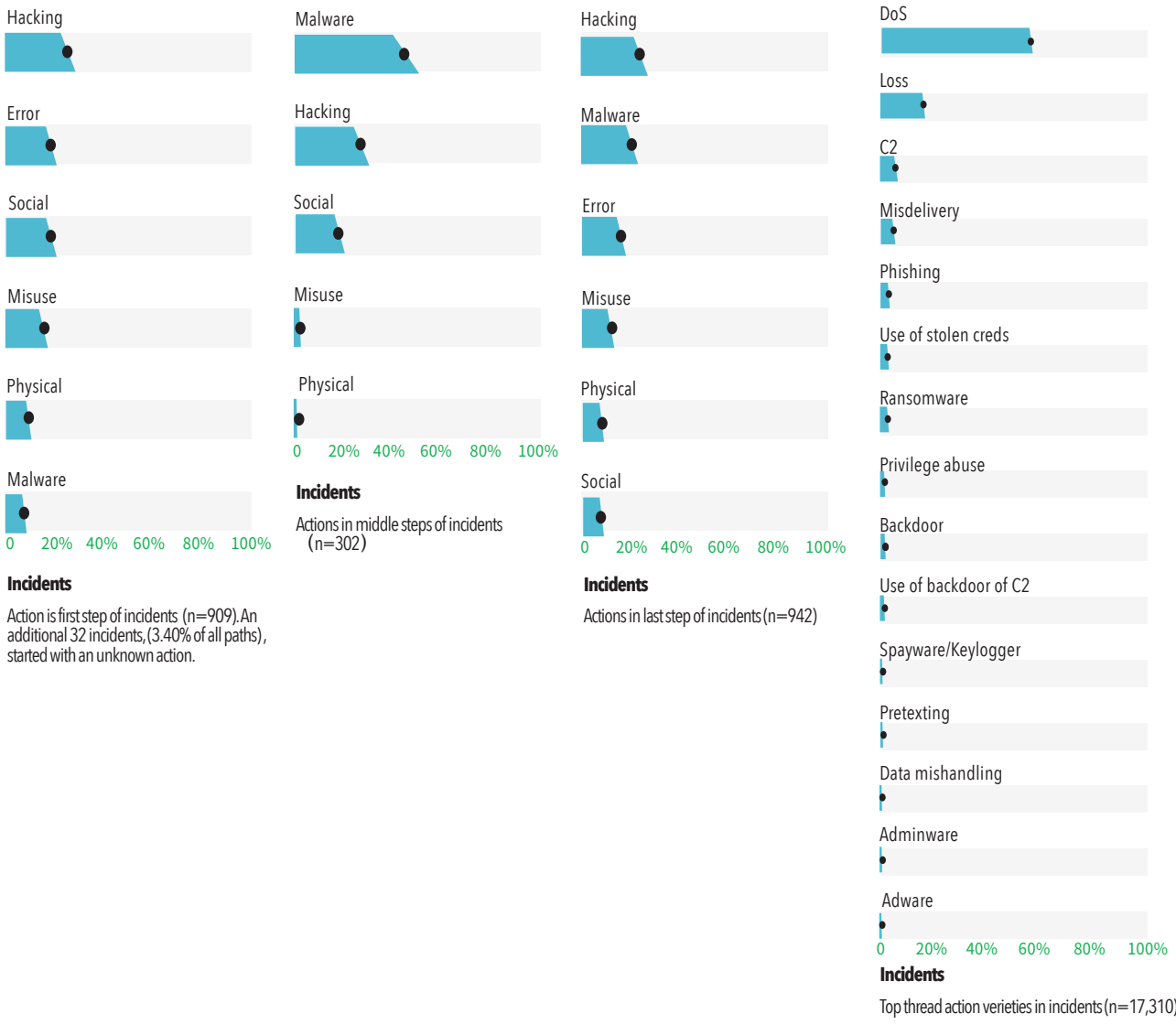


Source: Internet

Being Diversified

In 2019, American telecommunications company Verizon has released a Data Breach Investigations Report, which shows the distribution of attack types before, during and after cyberattacks. Among them, hacking, malware and misuse are now the main threats affecting the global cybersecurity market. These factors, combined with social and human errors, form a complex cyberattack environment. As for means of attack, Denial of Service (DoS) attack was the main mode in 2018, while C2, phishing and other means of attack also frequently appeared. In addition, global cybersecurity company Symantec mentioned in its Internet Security Threat Report (Issue 24) released in 2019 that Web attacks grew 56% and supply chain attacks rose 78% year on year in 2018. At the same time, cyber criminals are constantly renovating their means of attack. Attacks such as spear phishing and hijacking have also attracted extensive attention from enterprises.

Figure 2 Diversified Cyberattacks



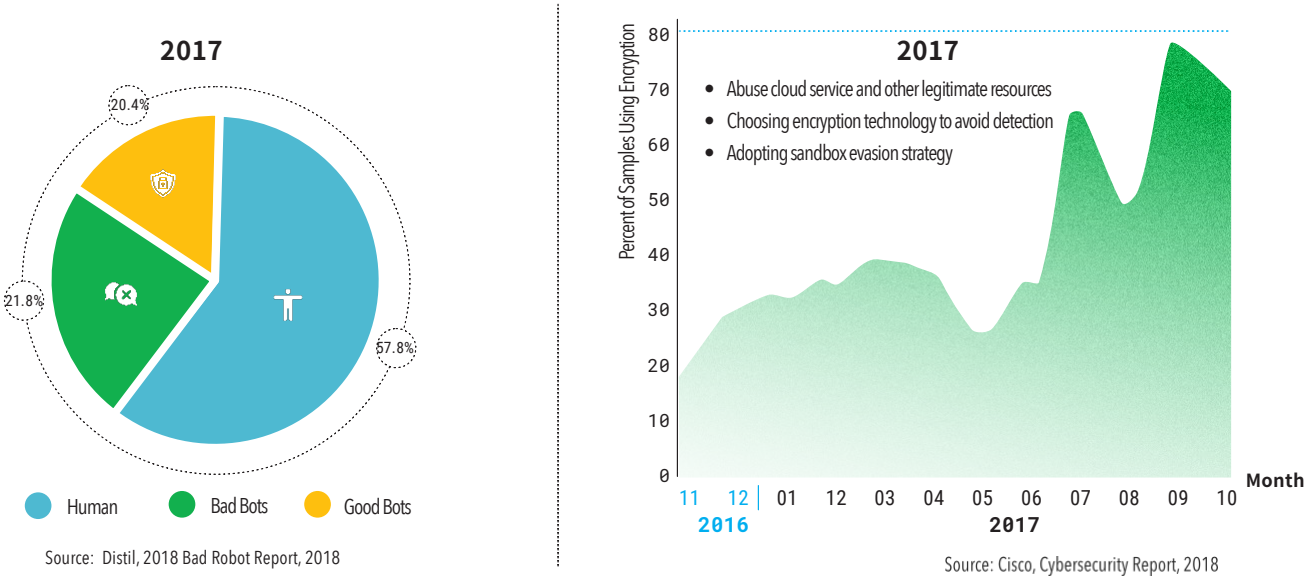
Source: Verizon, Data Breach Investigations Report, 2019

Being Highly Concealed

At the same time, cyberattacks have also become more concealed. According to the 2018 Bad Bot Report released by cybersecurity company Distil, bad bots account for 21.8% of all website traffic in 2017, up 9.5% year on year. Bad bots took 72.4% of their time by identifying themselves as web browsers such as Chrome, Firefox, IE and etc. With the rapid weaponization of data centers, 82.7% of bad bot traffic hid themselves in data centers in 2017, an increase of 37% year on year.

In its Cybersecurity Report released in 2018, global network solution provider Cisco pointed out that cybercrimes also rely on legitimate Internet services, making them their main covert way of attack, which makes most malicious traffic unrecognizable. In addition, attackers also use development and encryption technology to avoid detection, launch multiple attacks on a single domain to hide themselves and expand the destructive attack power while hiding themselves. It is the enhanced attack concealment that make enterprises find it difficult to make accurate user portraits and user behavior analysis of attackers in time, thus increasing the difficulty of cybersecurity protection for enterprises.

Figure 3 Cyberattacks Have Become More and More Concealed

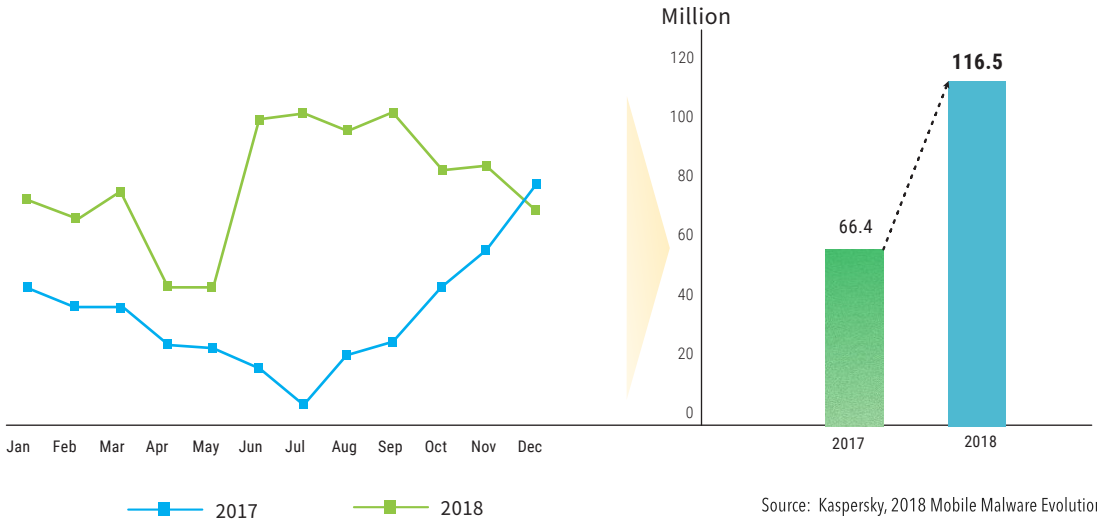


To sum up, with the popularization of the Internet and the increase of data assets, cyberattacks have been deep into all aspects of social life. The forms and means of cyberattacks are constantly updated with the improvement of technology, making the attacks and attackers increasingly hard to be detected.

1.1.2 The Number of Malware and "Zero Day" Vulnerabilities is Rising

In 2018, the number of malware worldwide rose. According to the 2018 Mobile Malware Evolution Report of Kaspersky Lab, 5,321,142 malicious installation packages were detected in 2018, of which the number of malicious mobile software attacks nearly doubled to 116.5 million.

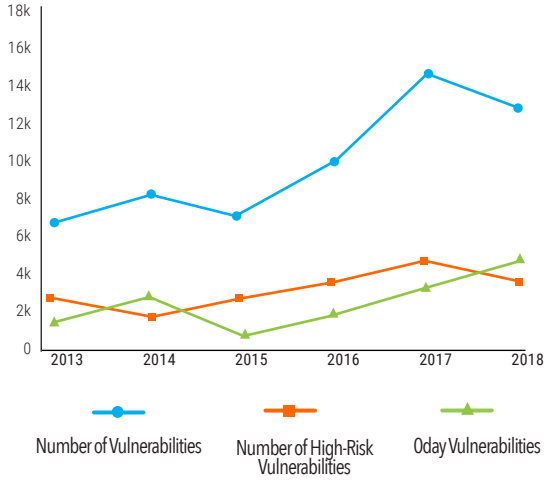
Figure 4 The Number of Mobile Malware Attacks Worldwide Rises



Source: Kaspersky, 2018 Mobile Malware Evolution Report , 2019

In China, the 2018 China Internet Cybersecurity Report released by the National Internet Emergency Center shows that despite a decline in the number of cybersecurity vulnerabilities in China in 2018, the number of "zero-day" vulnerabilities continued to rise, reaching 5,381, up 39.6% year on year, accounting for 37.9% of the total number of security vulnerabilities in the country. The increase in the number of “zero day” vulnerabilities reflects that China is still facing a very serious cybersecurity situation at present.

Figure 5 The Number of "Zero Day" Vulnerabilities in China Increases



Source: 2018 China Cybersecurity Posture Review, 2019

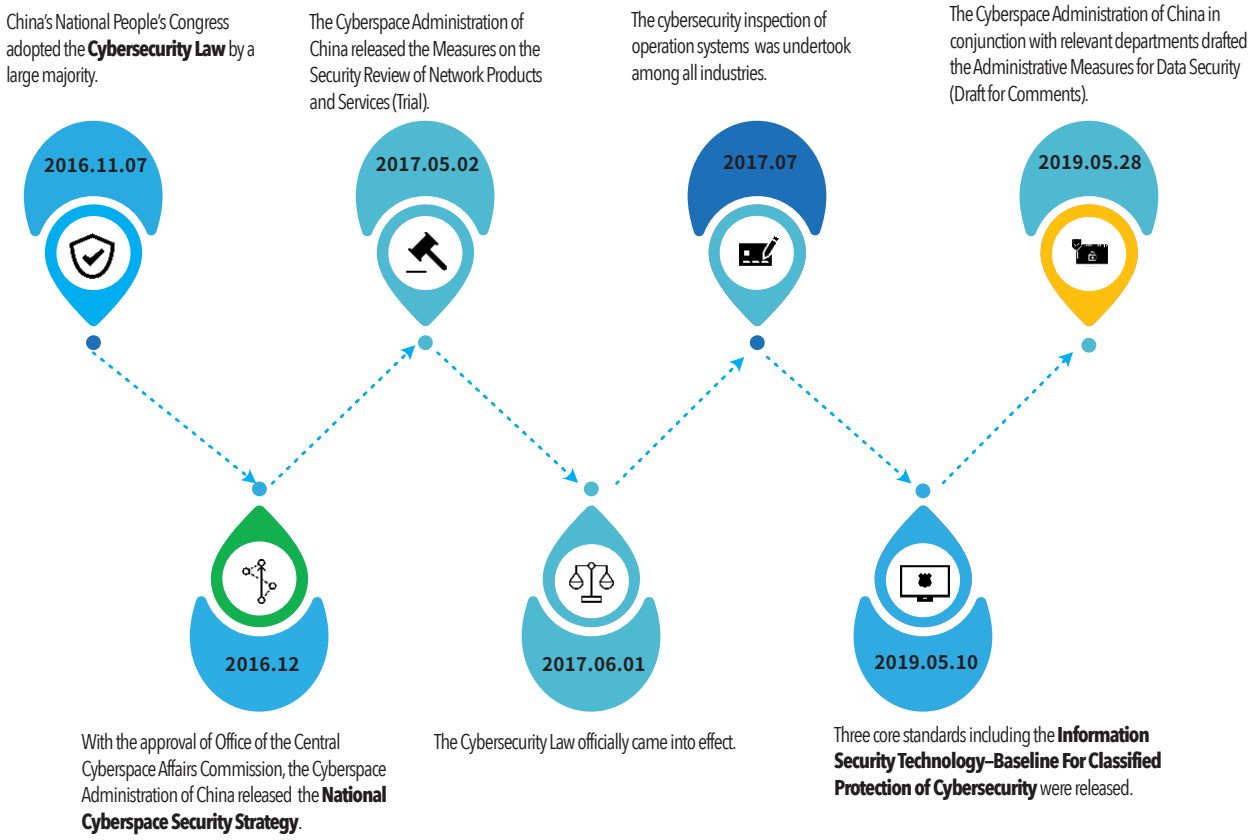
In general, the widespread, diversified and concealed cyberattacks and the continuously rising number of malicious software and "zero-day" vulnerabilities are both threats to the digital transformation of enterprise-level customers. Meanwhile, these have posed a threat to the national interests, being an issue of concern to the government and society.

1.2 Regulatory Standards Become More Stringent

Faced with the escalating threats of the digital age, various countries and regions around the world have stressed on their institutional improvement on cybersecurity. Among them, the European Union has promulgated the most stringent personal data protection regulation -- the General Data Protection Regulation (GDPR) in 2018, in an effort to strengthen the web tracking and protection of personal data. According to media reports, the Information Commissioner's Office (ICO) of Britain has started to punish, in compliance with the GDPR, a number of rule-breaching enterprises. For example, on July 8, 2019, the ICO decided to impose a maximum fine of £183 million on British Airways for the leak of information on 300,000 users in 2018. On July 10, 2019, the ICO proposed a fine of US$124 million against Marriott International over a data breach involving 383 million of its customers in 2018.

At the same time, the Chinese government is also vigorously carrying out the work of cybersecurity governance and policy construction, and constantly improving national supervision.

Figure 6 Cybersecurity Supervision in China at an All-Time High Level Now



Source: IDC, 2019

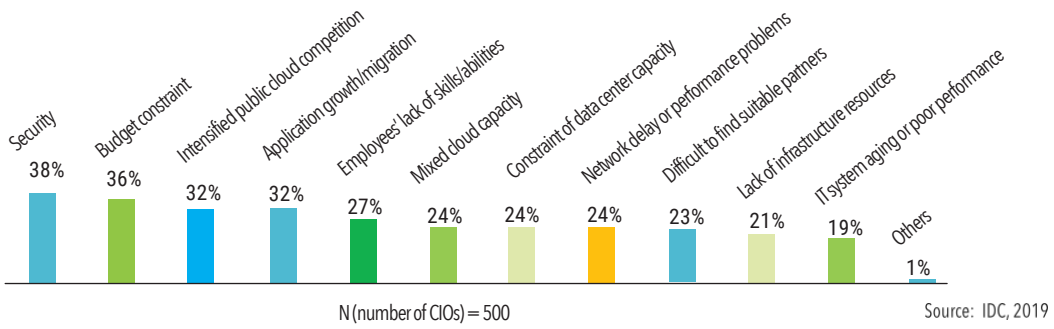
On June 1, 2017, China's Cybersecurity Law officially came into force. The law clearly defines the obligations of various entities in society, and covers the protection of key information infrastructure, network data and personal information, emergency response and monitoring of cybersecurity, and other aspects. It guarantees the space sovereignty and national security of cybersecurity, the security of network products and services, and the security of network operation, and pushes forward the cybersecurity legalization process in China, being an important milestone in the cybersecurity legalization.

On May 10, 2019, China officially released three core standards of the Information Security Technology—Classified Protection of Cybersecurity 2.0 (hereinafter referred to as "Classified Security Protection 2.0"), including the Information Security Technology—Baseline for Cybersecurity Classified Protection. Compared with Classified Security Protection 1.0, Classified Security Protection 2.0 expands the scope of objects for classified protection, incorporating cloud computing, mobile interconnectivity, IoT, industrial control systems, etc. into the standard. At the same time, it unifies the classification frameworks of the basic requirements, technical requirements for security design and evaluation requirements, and forms a triple protection architecture supported by the "secure communication network", "secure zone boundary", "secure computing environment" and "secure management center". In addition, trusted validation is included at all levels, and the execution of system programs and applications will also be subject to dynamic trusted validation according to the requirements of different levels. Through Classified Security Protection 2.0, the state has improved the protection and safeguard of key information infrastructure by various social entities. In the future, establishing Classified Security Protection 2.0 will be the obligation that network operators must fulfill to ensure the cybersecurity. The state will also severely deal with those operators and users which fail to fulfill their obligations for building Classified Security Protection 2.0 or which have major security accidents, so as to help the government and enterprises to pay more attention to cybersecurity construction, enhance their comprehensive cybersecurity protection capabilities and reduce the risk of being attacked.

1.3 Enterprises Urgently Need Powerful Cybersecurity Equipment and Solutions

As discussed above, the grave situation of global cybersecurity and compliance requirements have brought new challenges to the future development of enterprises. More and more enterprises have elevated cybersecurity construction to a strategic level. In its survey of 500 CIOs worldwide, IDC found that cybersecurity has become the biggest challenge in the digital transformation of global enterprises.

Figure 7 Cybersecurity Becomes the Biggest Challenge to Enterprises' Digital Transformation Worldwide



What threats are enterprises facing at present? Through its global market survey and research, IDC found that the main challenges faced by enterprise users in terms of cybersecurity include: sophistication of cyber miscreants growing rapidly, proliferation of security tool sets, growing number of environments and devices to protect, death of perimeter, scarcity of qualified information security professionals, continued growth of compliance regulations, and cyber crime as a business.

Figure 8 Seven Overarching Trends in Cyber Security

Source: IDC, Market Analysis: Global Management Security Service Providers, 2018

01 **Sophistication of cyber miscreants growing rapidly**

IDC has seen more and more complex technologists used by attackers. Attack codes now spread as quickly as weapons, as reflected in the following:

Rampant hackerism -- more and more attackers are turning numerous and complex technologies into cybersecurity tools to disrupt organizations that do not agree with their political or ideological views; **industrial espionage activities** -- these attacks often target insiders in an attempt to obtain sensitive data that can be sold or released to competitors; **organized cybercrime,** where attackers use mixed methods to attack their ultimate targets; **attacks against nationalities and countries,** which are usually well-funded and frequently associated with the military. These attackers often take advantage of "zero day" attacks that are not known to the public.

02 **Proliferation of security tool sets**

As business migrates to the cloud and different types of devices increase substantially in numbers, demand for different types of security tools is also soaring. In most situations, these security tools are products that solve a particular security problem. In the near future, however, these products will be incorporated into a larger product set. For example, although user behavior analysis/user and entity behavior analysis (UBA/UEBA) is a technology, it will soon become part of other products. This technology will help security management personnel to identify and address multiple top-level challenges.

03 **Growing number of environments and devices to protect**

IDC predicts that global IoT spending will reach US$1.1 trillion by 2023, and 39% of new services will be sold in a virtual form by 2019. Such a huge number of devices also form a massive number of IT environments, which also implies that many organizations will need to use hybrid security policies or security policies for specific IoT scenarios.

04 **Death of perimeter**

Over the next two years, 95% of large enterprises plan to increase their use of cloud technology. Border-based security defense methods can no longer meet the needs of security defense. Although traditional network boundary security devices such as firewalls and IPS have the ability to protect local networks, overall security methods must change to adapt to the technological evolution of the third platform.

05 Scarcity of qualified information security professionals

Enterprise-level users have growing concerns about cybersecurity. IT architecture is virtually changing on a daily basis, and demand for experienced cybersecurity professionals is constantly growing. The lack of talent leads to a general pay rise for cybersecurity personnel, and it is difficult for small- and medium-sized enterprises to pay higher expenses for this, which results in frequent security incidents in many enterprises.

06 Continued growth of compliance regulations

Countries around the world have continuously strengthened the formulation and update of their cybersecurity policies and regulations, and promoted the cybersecurity compliance of governments and enterprises. For example, with the continuous upgrade of informatization, China has promulgated a number of laws and regulations related to cybersecurity in recent years. Among them, the Cybersecurity Law elevates cybersecurity to the national strategic level, while Information Security Technology – Baseline for Cybersecurity Classified Protection further clarifies the direction of development in the new era of classified protection and Administrative Measures for Data Security (Draft for Comments)" has set forth provisions on data leakage, personal data protection and other aspects.

07 Cyber crime as a business

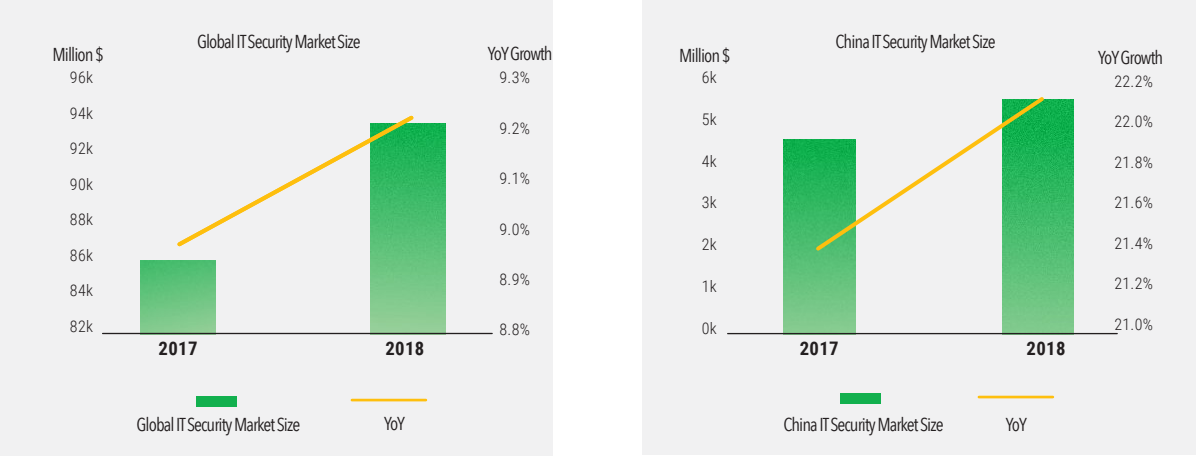
With the continuous escalation of cybercrimes, the government, enterprise-level users and individuals are no longer facing simple and single cyberattacks, but complex, highly concealed and organized cybercrimes. The core attackers in attack teams formulate phased development tasks and operational forms for other attackers. At the same time, the attack systems within the attack groups connects all sectors of society. Attacks can concurrently affect many industries, thus forming a complex cyberattack ecosystem. For example, blackmail software, which has appeared frequently in recent years, penetrates into all sectors of society through programs such as worms, so as to achieve the purpose of cyber blackmail.

All these changes require enterprises to quickly identify potential threats that are not conducive to their corporate security while developing new technologies, strengthen security construction and protect themselves from cyberattacks.

1.4 Market Response Reaches a New Pitch

As the global cybersecurity market continues to grow, the market's response to the cyber threat situation and policies has reached a new high. According to IDC Worldwide Semi-Annual Security Tracker, the global IT security market reached US$94.2 billion in 2018, an increase of 9.26% over the previous year. Overall expenditure on security solutions in China amounted to US$5.53 billion, up 22.1% year on year. Of this, security hardware still occupies the absolute dominant position in overall security solution expenditure, followed by security software and security services. It is precisely under the influence of the sustained high-speed growth of the cybersecurity industry that the government and enterprises have sped up their cybersecurity layouts and raised their cybersecurity construction level to safeguard their own digital transformation and meet the requirements of compliance.

Figure 9 Global and China IT Security Market Sizes 2017-2018



Source: IDC, 2019

02

Multiplied Innovation Drives Continuous Change in Security Construction

2.1 Security Construction Needs Continuous Innovation

With the continuous development of the digital era, all walks of life have begun to actively carry out digital transformation, using AI, IoT, cloud computing and other technologies to establish a series of IT systems that meet the own attributes of their sectors. At the same time, the continuous increase of IT systems and the continuous innovation and development of new technologies have put forward higher requirements for security construction in the cyberspace. Cybersecurity construction needs continuous innovation to adapt to the continuous development of the digital era.

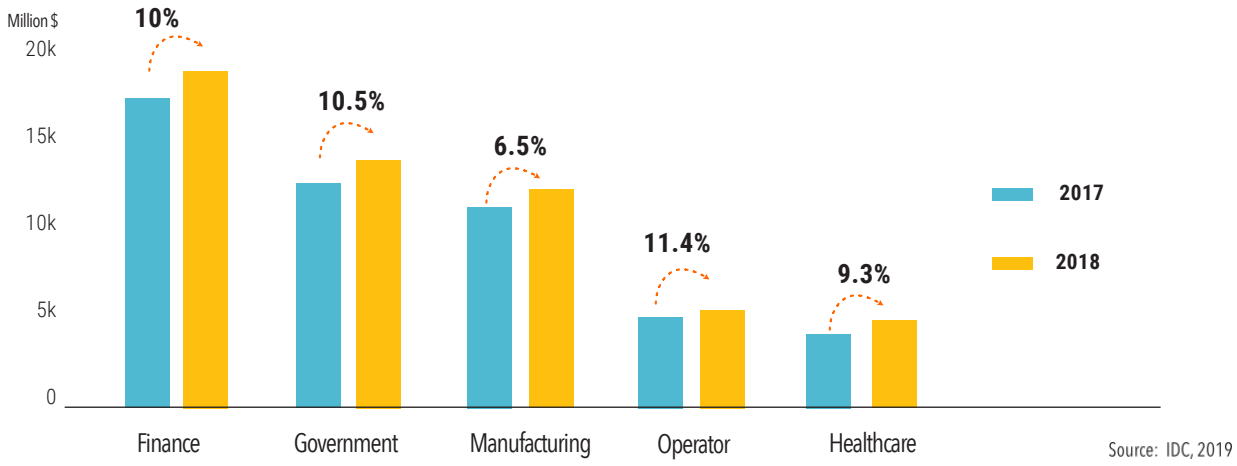
2.1.1 Potential Threats Increase as IT Systems Boost during Digital Transformation

Digital transformation has now entered the stage of multiplied innovation. Enterprise-level users in all sectors are actively leveraging their innovative advantages and building a large number of new IT systems in line with the needs of digital transformation. These systems contribute to the foundation for the development of smart cities, new finance, operators' business transformation and digital manufacturing, while also facing a lot of security problems.

	Government	Financial	Operator	Manufacturing
	· Governments around the world are actively building images of being efficient, and continuously promoting their digital transformation by applying technologies such as cybersecurity, analysis and detection, mobility, big data, cloud computing and etc. · Countries across the globe are actively building smart cities or wireless digital cities to unify social, economic and political functions. In the future, they will further promote the deep integration of AI with the economy, society and national defense, and push forward the development of new smart cities.	· Cybersecurity, physical security and policy compliance are the key strategic directions of attention for financial enterprises worldwide. · IoT automation, real-time payment and open banking will be the focal points of development in the financial industry in the future.	· The stable development of mobile big data services and emerging markets continues to drive the growth of the telecommunications industry. · Telecom operators use SD-WAN technology and SDN/NFV-based platform virtualization technology to build integrated collaboration platforms.	· Investment in digital platforms has become the basis for business transformation in the manufacturing industry. · Manufacturers in various countries actively use AI, blockchain, automation and other technologies to build new ecosystems, thereby achieving business growth. · Security, as the basis of IT/OT integration for global enterprises, plays a vital role in the reform of the global manufacturing.
	· In the work report delivered to the Nineteenth National Congress of the Communist Party of China, a call was made to raise the level of socialization, rule of law, intelligence and specialization in societal governance. "Internet + governance" has become the consensus of governments at all levels in China. Investment in digital technology will increase rapidly in the future. · Third platform technology is in "spiral-shaped" in the government sector. Data-centered platform construction, application innovation and AI intelligence are the core concerns of leaders in charge of government informatization in the next three years. · Governments at all levels should strengthen infrastructure security control, readjust operational procedures according to their own control systems, and assign appropriate technology, products, services and personnel to ensure the normal operation and security of infrastructure.	· Business model of new finance: Combine with different industries and achieve all-round digital channel coverage through science and technology. · Integration and cross-boundary: weaken the boundaries between financial services and products and bridging the boundaries between data and platforms. · Comprehensive digital channel coverage: build digital channels on virtual cloud. · Financial security: data security, and security protection of key infrastructure.	· "No revenue increase despite business volume increase" will become a normal in the telecommunications industry, and Chinese operators expect to achieve business transformation and improve industry profit margin through network transformation. · New business patterns such as SD-WAN, cloud-based UCaaS, cloud interconnectivity and communication services outsourcing will become new sources of revenue for operators. · SDN, SD-WAN, 5G and other technologies have put forward new requirements of cybersecurity construction for operators.	· Digital-centric, platform-based, cross-industry collaboration helps China's manufacturing industry to make breakthroughs to high-quality development. · Platform ecosystems centered on blockchain and AI realize enterprise process automation. · Various enterprises place data at the center of processes. Workers in manufacturing plants will be armed with AR/VR, intelligent applications and collaborative robots to increase productivity and improve the working environment.

In the above situation, various industries around the world are increasing their investment in security construction. According to IDC Worldwide Semi-Annual Spending Guide, global IT security spending in finance, government, manufacturing, operator, healthcare and other sectors was in continuous increase from 2017 to 2018 (as shown in the figure below), so as to adapt to continuously innovating emerging IT systems.

Figure 10 Global IT Security Expenditure Growth in Various Sectors



2.1.2 New Technologies are Deeply Utilized in the Black Industry

The application of AI, IoT, cloud and other technologies in smart cities, key information infrastructure construction, financial fraud prevention, manufacturing security and other new scenarios has brought great convenience to social life. But it has also generated higher cybersecurity risks. The root of such risks lies in the black industry's more active use of these technologies to make cyberattacks.

From the perspective of AI, attackers can analyze the attackees' assets, network and user data through machine learning, thus improving the accuracy and destructive power of their attacks. For example, an attacker makes an attack decision by observing and learning the anti-malware AI, and develops a "minimum detected" malware. An attacker uses machine learning to analyze a large number of stolen logs so as to identify potential victims and carry out effective targeted attacks. In addition, attackers can also use the "countermeasure sample" to avoid attacks and make their attacks more covert.

From the perspective of IoT, the continuously emerging cyberattacks make the public begin to realize that attackers can easily intrude into daily monitoring devices such as cameras and monitor everybody's daily life. IoT devices are usually networked devices by default, which are easy to be taken advantage of by attackers. Attackers will attack their observed network devices in groups and invade a large number of devices in a short time. For example, Mirai botnet is a botnet program that mainly infects IoT devices. It logs into IoT devices by default or weak password, thus turning them into "broilers" and manipulating the attacked objects to attack other network devices. Through DDoS attacks, Mirai has crashed many social networking sites, shopping sites and so on.

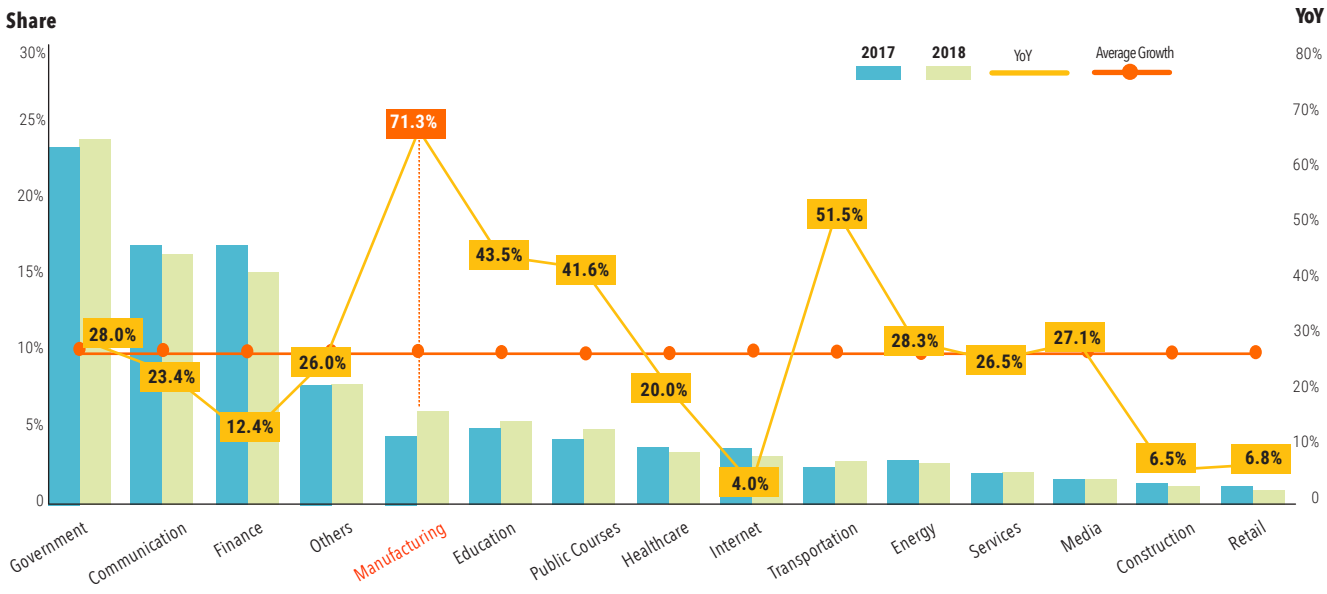
From a cloud perspective, attackers usually build their own private cloud or virtual network, steal or hijack vulnerable cloud computing systems, and then use cloud computing resources for cyberattacks. Among them, DDoS attacks are their main means of attack. At present, many cloud service providers rely on third-party platforms to accommodate and protect their information, which also puts forward higher requirements for the product design of third-party platforms. Attackers can exploit the vulnerabilities of application programs on third-party platforms to make attacks.

In short, attackers use these new technologies to carry out cyberattacks, expand the scope of their cyberattacks, improve the accuracy, concealment and destructive power of their attacks. This puts forward new requirements for enterprise-level users' cybersecurity construction.

2.1.3 Close Cybersecurity Protection Becomes a Necessity

Against the background of the continuous emergence of large numbers of new IT systems and innovative technologies, security construction has gradually become a necessity of various key industries. Taking manufacturing as an example, according to IDC statistics on security investment in various industries in 2017 and 2018, the growth rate of security investment in the manufacturing industry reached 71.3%, largely thanks to the issue of the Guiding Opinions on Deepening "Internet + Advanced Manufacturing" and Developing the Industrial Internet issued by the State Council. The first consideration for customers in the initial stages of project implementation is the security issue, because cyberattacks in the industrial control environment will bring serious risks to enterprises and may cause enterprises huge losses. In the current cybersecurity construction, in addition to the policy push, enterprises have also become aware of the serious consequences of cyberattacks, and really consider cybersecurity construction as the rigid demand for corporate development.

Figure 11 Cybersecurity Building Becomes a Necessity in China

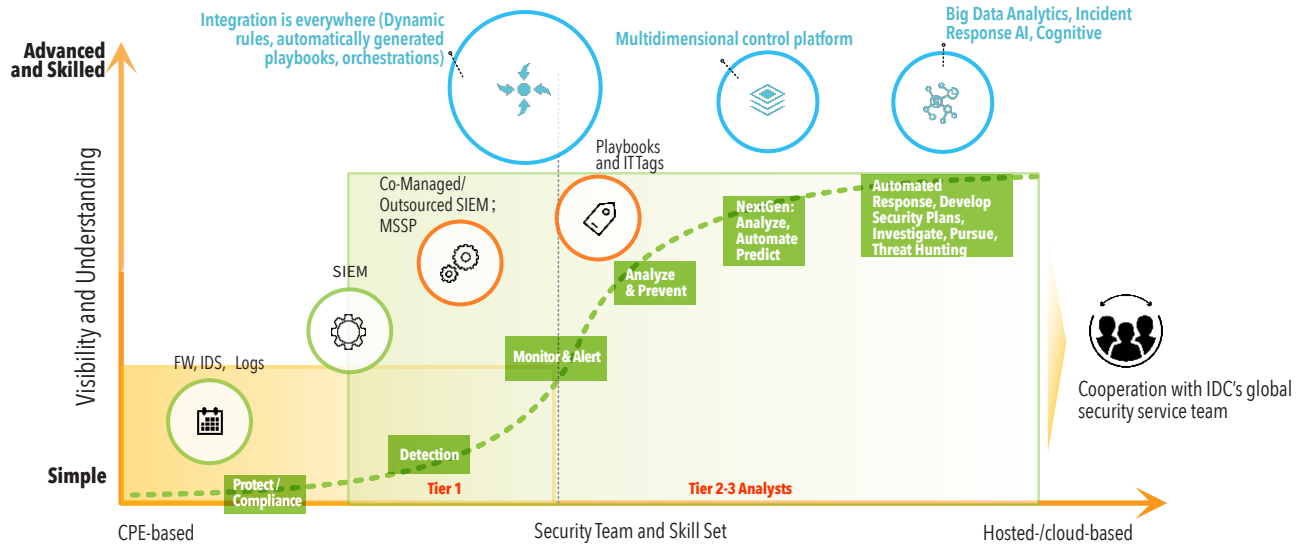


Source: IDC, 2019

2.2 New Directions of Technological Innovation and Development

From the deployment of simple firewalls and intrusion detection products at the end of the 20th century to the deployment of structured cybersecurity products today, cybersecurity technology innovation is continually evolving and changing. IDC believes that the next generation of security products will widely adopt technologies related to big data analysis, event response, AI and cognition. Cybersecurity defense systems will also focus on automatic response, development security plans, investigation, tracing, threat trapping and etc.

Figure 12 New Direction of Technological Innovation and Development

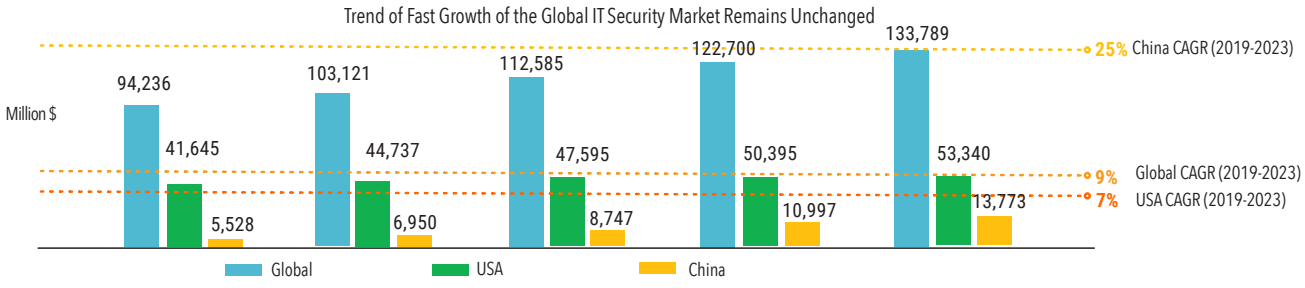


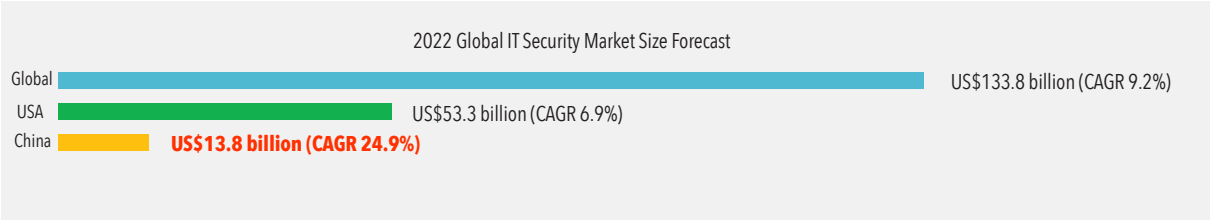
Source: IDC, 2019

By integrating multi-dimensional control platforms (including dynamic rules, automatic script generation, editing and other capabilities) in the network, enterprises can make junior cybersecurity analysts use the integrated platform to imitate and learn from the cyberattack handling capabilities of higher-level analysts in the future.

According to IDC's forecast in 2019, driven by the rapid development of technology and market demand, the global IT security market will reach US$133.8 billion by 2022, with a CAGR of 9.2% from 2019 to 2013. China's IT security market will reach US$13.7 billion, with a CAGR of 24.9% from 2019 to 2023, which is much faster than global market growth. In the future, with the improvement and upgrade of technology and solutions of security vendors, enterprise-level users will have more choices to obtain security solutions that are most in line with their current situation. Security vendors, governments and enterprises will work together to build a new environment of personal security, corporate security and national security.

Figure 13 China Leads the World in Security Market Growth





Source: IDC, 2019

03

How to Deal with Cybersecurity Threats in the Digital World

In 1972, Kenneth Arrow, a Nobel Laureate in economics, pointed out that almost all business transactions, especially those that take a long time, contain elements of trust. Therefore, it can be said that economic retrogression of the world can be explained by lack of mutual trust. Since then, research has been gradually growing on the causal relationship between trust and economic growth.

Overall, trust can drive economic growth - we do business with the people we trust; we do more business with those being more trustworthy. Economists and psychologists have linked a country's confidence index to its gross domestic product (GDP). Admittedly, economic growth is driven by other important factors, but without trust, it is likely that only temporary, low-risk, low-value transactions will occur. Such transactions will not actually boost economic growth.

IDC had found that in the age of digital transformation, demand for digital trust has increased significantly, both for individuals and organizations. For example, for consumers, many of their daily activities must rely on their trusted websites to obtain corresponding services. In the enterprise-level market, digitally transformed enterprises regularly interview and audit business partners and service providers to assess their credibility under closer strategic relationships.

Therefore, just as trust promotes economic growth in the real world, digital trust can promote the growth of the digital economy and then digital transformation.

Digital trust will be the key economic driver of the digital transformation (DX) strategy. The digital economy integrates the willingness, interest and capability of enterprises, partners and customers, enables them to mobilize and share resources for digital activities, and leverages their unique advantages to create synergies, thus pushing forward the growth of the digital economy.

IDC believes that:

Digital trust can reflect the degree of trust in each other in the decisions of multiple entities. These decisions are made based on the digital reputation of each entity and the level of assurance of the cybersecurity plan that each entity formulates for its digital activities.

It has become an inevitable trend for enterprise-level customers to build their digital trust frameworks. A digital trust framework consists of four levels, two of which are related to the technical risk management requirements of cybersecurity projects, and the others to the reputation factors of personnel and business interaction.

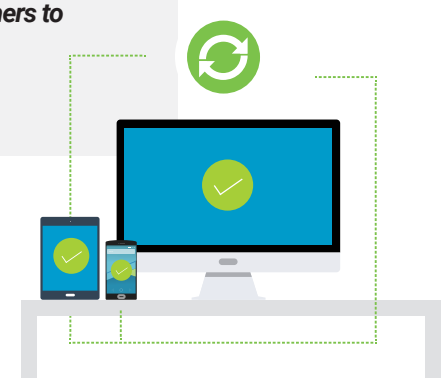


Figure 14 IDC Digital Trust Framework

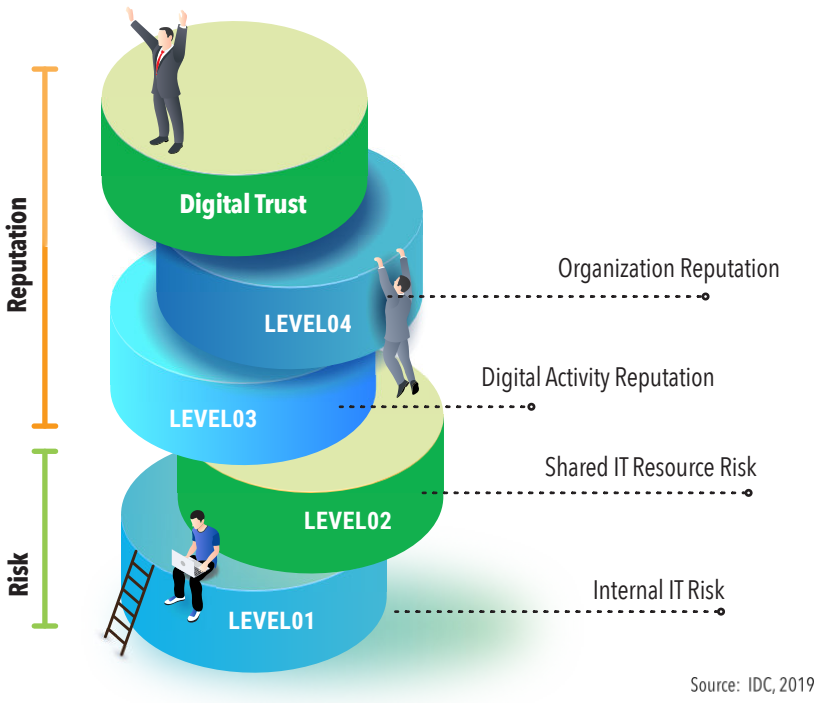


Figure 14 shows four levels of the digital trust platform, in which:

Level 1: Internal IT risk addresses internal, traditional cybersecurity posture and risk management activities of an organization.

Level 2: Shared IT resource risk addresses the managed risk of the shared technical resources for the digital activity.

Level 3: Digital activity reputation addresses the quality of an organization's reputation in providing or performing some specific digital activity.

Level 4: Organization reputation addresses the quality of an organization's overall reputation for all of its digital activities and usually all of its public actions.

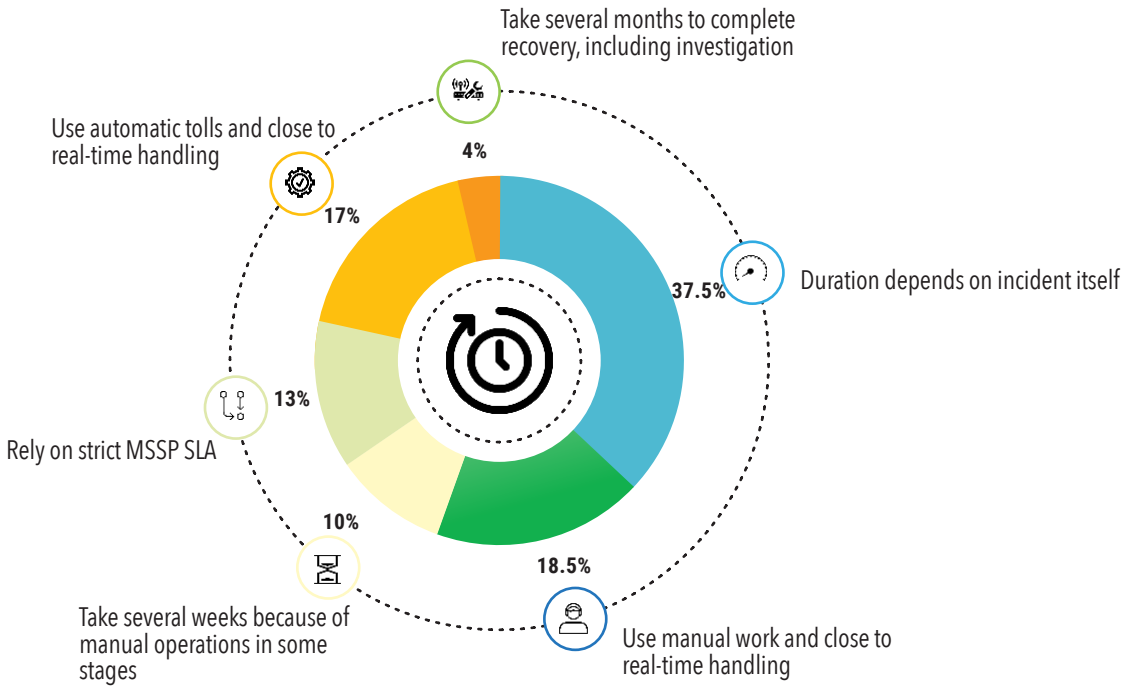
Achieving IDC's highest level of digital trust will help accelerate the pace of enterprises' digital transformation. IDC believes that the foundation for enterprises to build a digital trust framework is to establish an active security defense system.

3.1 Idea: Building an Active Defense System on the DX Platform Based on Threat Intelligence and Analysis

The idea of cybersecurity defense system building determines the final construction effect. The large-scale construction of new-generation business systems based on third platform technology greatly promotes the digital transformation of enterprises. However, due to its complexity, the systems are challenged with more and more threats. For example, enterprises rent cloud resources, which makes the traditional "castle" type of passive defense ineffective.

In the face of numerous complex business systems, it is difficult to detect and respond to unknown threats in time by only relying on manual analysis and passive defense technology. At the same time, the construction of automatic defense systems is no cause for optimism. Through its survey and research, IDC has found that only 17% of the interviewed customers could use automatic means to protect against cyberattacks.

Figure 15 Enterprises Generally Lack Automatic Defence Means

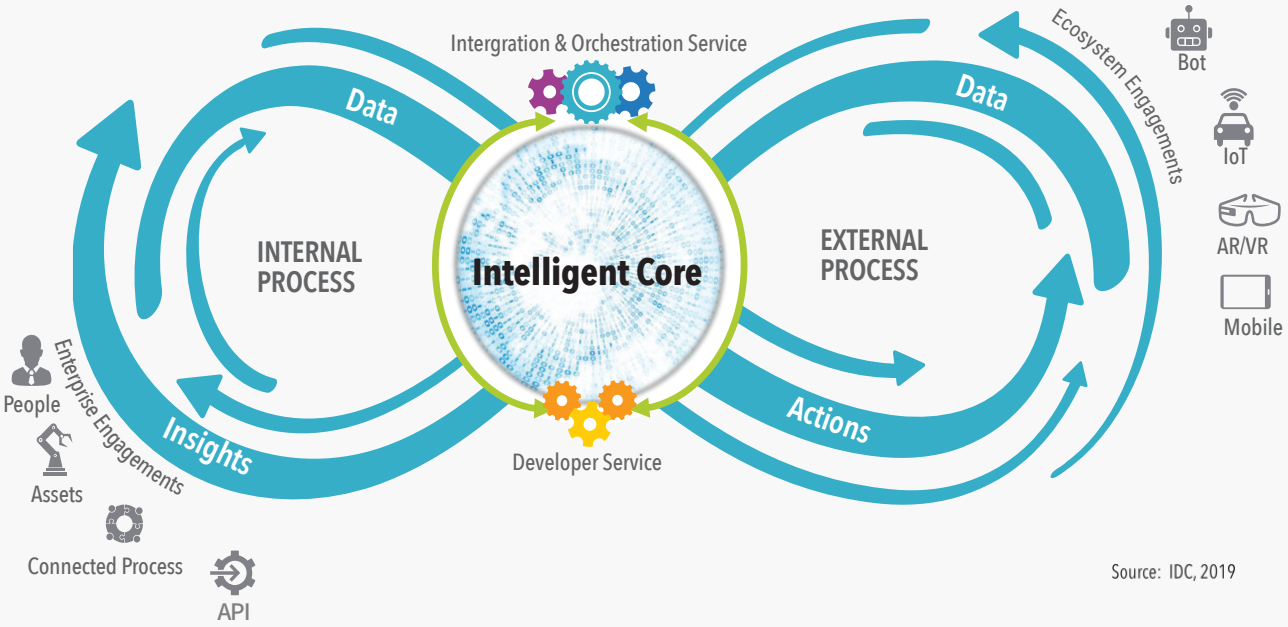


Source: IDC, 2019

In the current grave situation of cybersecurity, enterprise-level users therefore need to thoroughly update their ideas of cybersecurity system construction.

IDC has found that enterprises worldwide which have made successful digital transformation are all continuously building DX platforms, and their cybersecurity active defense systems are also built around the DX platform. **The DX platform is the future technological framework for enterprises accelerating digital transformation. The DX platform can quickly create external-oriented data products, services and experience, while actively optimizing the internal IT environment into an intelligent core system.**

Figure16 DX Platform



Among them, having an intelligent core refers to having active and sound cognitive capability and being able to use automatic decision-making means to expand traditional manual decision-making. The DX platform with an intelligent core can meet the diversified needs of customers, partners and enterprises, and integrate complex technologies and products dynamically and organically, thus providing comprehensive information governance and powerful data management.

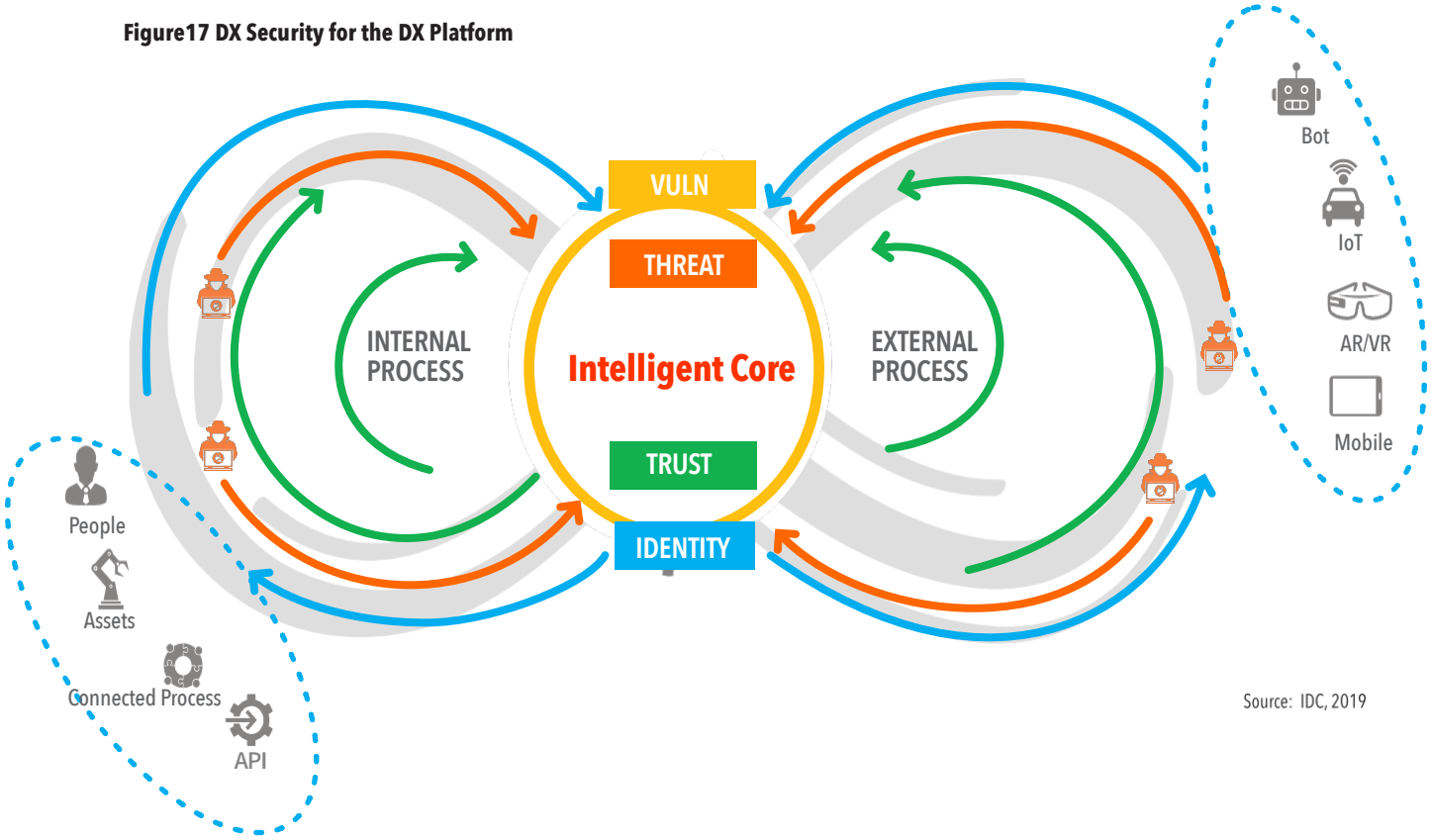
The digital platform will not only be an advanced technological platform, but also a comprehensive ecosystem building platform. Through interacting, sharing and integrating with external resources, it can help enterprises to establish a good operational ecosystem environment and ensure the healthy development of the digital transformation process. IDC predicts that by 2020, the number of organizations deploying DX platforms will double and reach 60%.

The purpose of cybersecurity construction is to ensure the smooth progress of enterprises' digital transformation. Therefore, it is necessary to make overall design based on the construction of the DX platform. Specifically, the active defense system provides security for all the links around the operation of the DX platform from the aspects of trust management, identity management, threat management and vulnerability management, and constantly optimizes its own defense measures to enhance the defense effect.

It is worth mentioning that threat intelligence has received the attention of global customers in the building of active security defense systems. The traditional cybersecurity defense system lacks awareness of new threats, thus usually unable to take rapid preventive measures against changes in the external threat environment. IDC believes that integrating threat Intelligence into active security defense systems can combine the unique security situation within enterprises with millions of security incidents, threats and vulnerabilities around the world. Through a series of professional analysis, high-priority security incidents can be found as soon as possible, thus helping enterprises to deal with unknown threats in advance.

Enterprises urgently need to build active defense systems based on threat intelligence and analysis on the DX platform, so as to cope with the continuously upgraded advanced means of attacks.

Figure17 DX Security for the DX Platform



Source: IDC, 2019

Currently, the idea of "building active defense systems based on threat intelligence and analysis on the DX platform" has won wide recognition and support from cybersecurity practitioners worldwide.

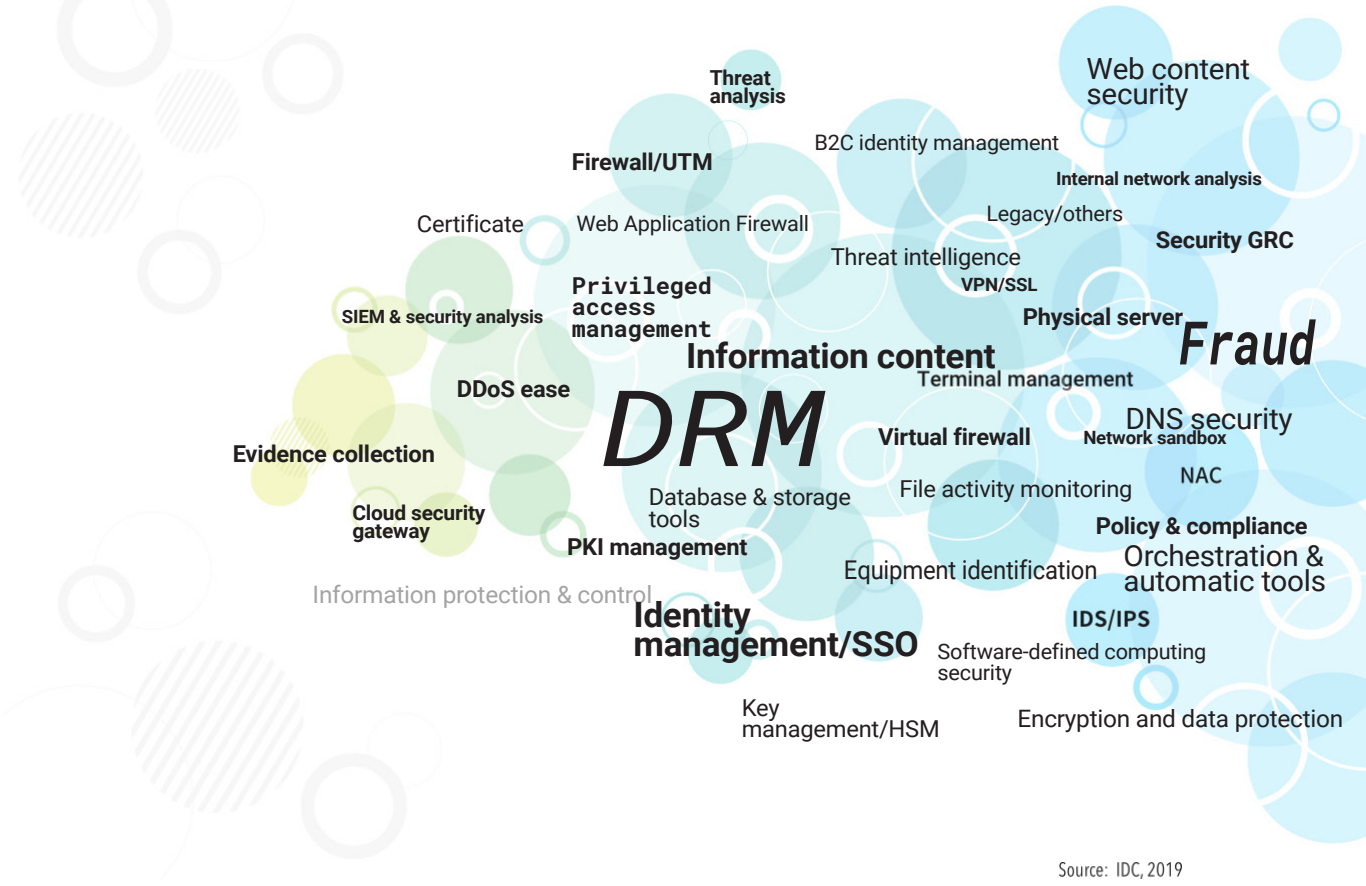
3.2 Cooperation: Building a Rich and Integrated Technological Ecosystem

3.2.1 Cybersecurity Construction Needs the Support of Various Cybersecurity Products

Specific cybersecurity construction needs to be supported by different types of cybersecurity software and hardware products, but the cybersecurity market is a fragmented one, with various types of product. A single cybersecurity product provider cannot provide all security products. Therefore, it is very important for enterprise-level customers, especially important industry customers related to key information infrastructure, to widely cooperate with all kinds of cybersecurity providers. Through cooperation, they can effectively build up technology reserve, which will help enterprises to cope with the ever-changing cyberattacks with ease.

IDC believes that cybersecurity products are mainly composed of security products at the network level, terminal level, identity and digital trust, security analysis and intelligence, response and layout, data security, App security and DevSecOps, etc.

Figure 18 Numerous and Complex Cybersecurity Products



Source: IDC, 2019

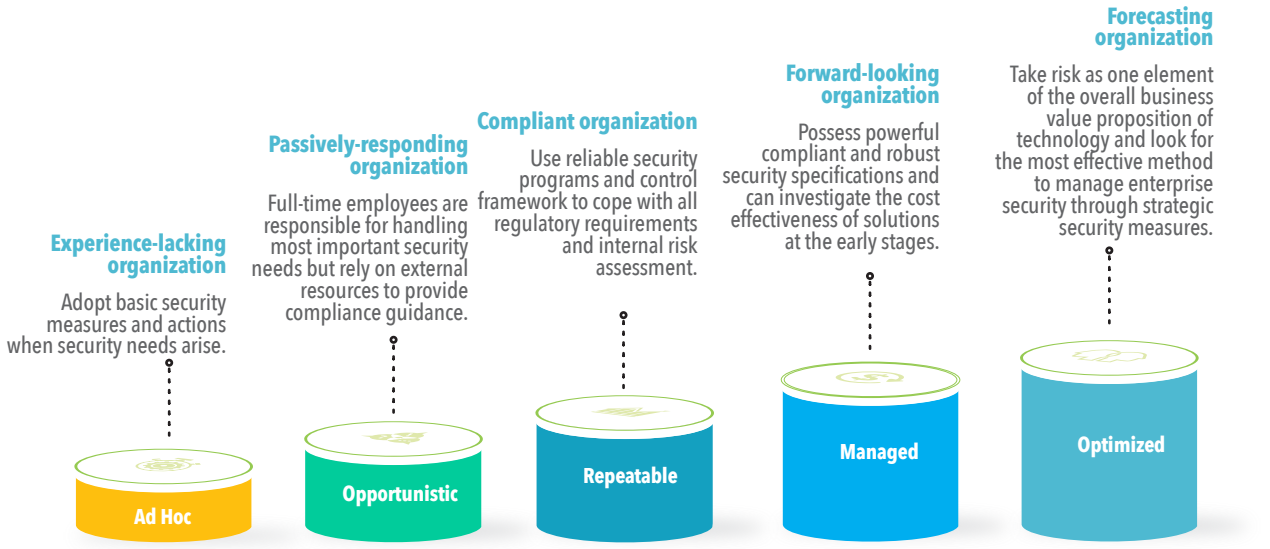
3.2.2 Phased Cybersecurity Construction Needs the Support of "External Brain"

When business managers see such complex and numerous cybersecurity products, they often face difficult choices. Although cybersecurity has become an indispensable part of enterprises' digital transformation process, what products do they need to buy? When to buy? How much investment is needed? These are still the doubts which enterprises have.

In this regard, **IDC believes that cybersecurity construction is not an overnight task. Enterprises need to integrate cybersecurity strategy with corporate development strategy. They need to make reasonable investment and scientific construction based on the need of different stages of development.**

To help enterprises clearly judge how to invest in cybersecurity, IDC has, based on its worldwide research, put forward a cybersecurity maturity evaluation model. The model defines the business development stage, scale, results and counter-measures for cybersecurity construction of various companies. These measures can effectively promote enterprises to achieve the security maturity required by competition in the third platform era.

Figure 19 IDC Cybersecurity Maturity Model



Source: IDC, 2019

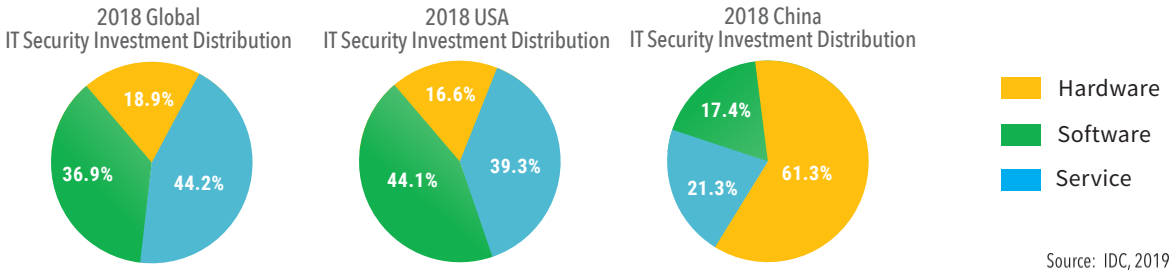
Enterprises need to select one or more of their cybersecurity solution partners to develop customized active security defense solutions for them.

3.3 Leveraging: Building Strength Through MSSP

Enterprises' cybersecurity is inseparable from security management. In the era of digital technology, enterprises' business systems will be generally placed in the cloud. At the same time, the trend of mobility is becoming more and more obvious. Enterprises are already short of ability to manage cybersecurity on their own. Security services will become an urgent supplementary service which Chinese enterprises need in the process of cybersecurity management.

Security services in China are still at an early stage of development. IDC data shows that in 2018, services and software accounted for the largest proportion of investment in the IT security industry in the United States and the world as a whole, with IT security hardware investment having the least proportion. The pattern in China was just the opposite, where IT security hardware taking up the highest proportion of investment. Chinese customers tend to recognize the value of security hardware, but do not much recognize the value of invisible security software or services. However, with the rapid development of public cloud and industry cloud, safeguarding cybersecurity for enterprises will be more dependent on cloud security software and services. From a global perspective, the amount of investment in IT security services will directly determine the actual defense effect of customers' security defense systems.

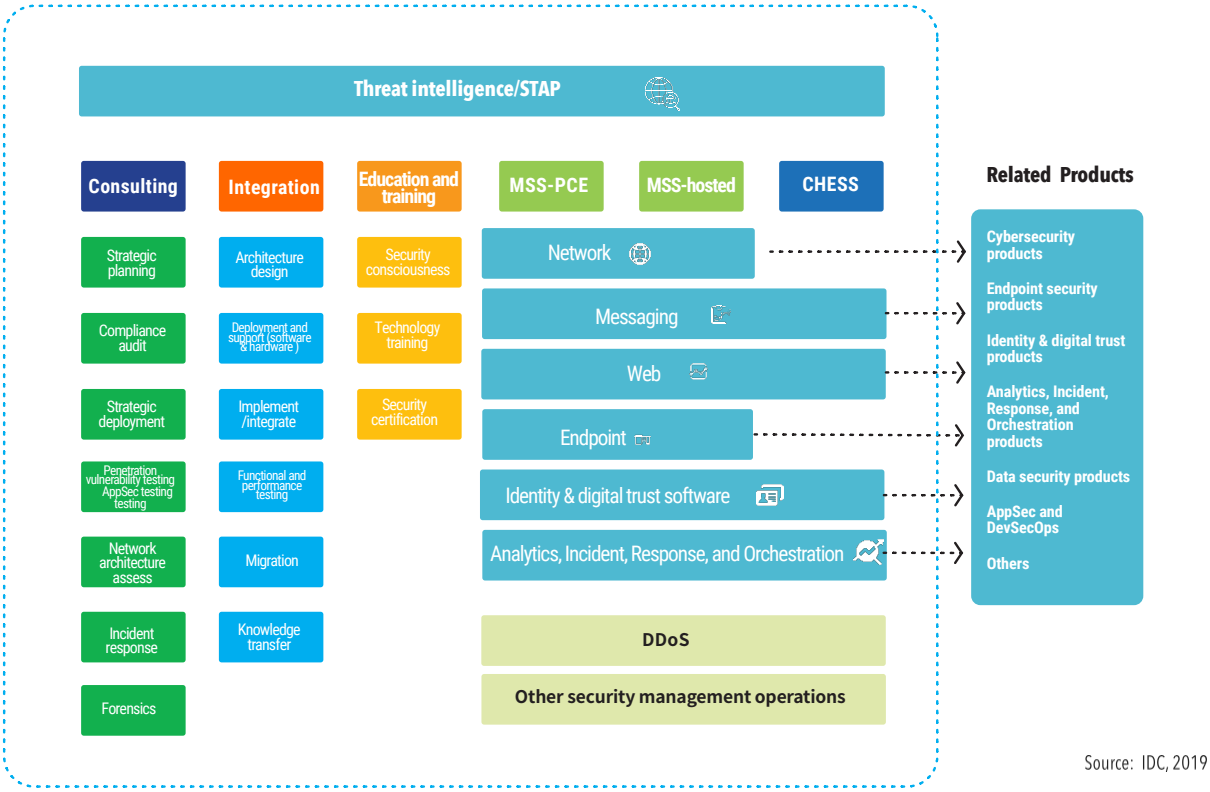
Figure 20 Comparison of Investment Structure of IT Security Industries in 2018



Source: IDC, 2019

Helping enterprises to clarify the composition of security services is good for enterprises to select the most appropriate choice of service. IDC believes that IT security services include four parts: security consulting services, security integration services, education and training, and security management services. Each part has a number of sub-categories, as shown in Figure 21.

Figure 21 Integrating Safety Management Services to Enhance the Overall Safety Defense Effect



Source: IDC, 2019

Among them, security consulting services, security integration services, education and training are related services in the early stages of IT security construction. Management security services (MSS) are most important in enterprises' IT operation process and have been widely recognized by customers worldwide. When cybersecurity incidents occur in enterprises, MSS providers (MSSPs) can provide emergency response, event handling, investigation, evidence collection and other security services for enterprise-level customers to solve their lack of professional IT security technical teams.

Specifically, security management services may include three types: MSS-CPE, MSS-Hosted and CHESS. Their characteristics and differences are shown in the following table:

Service Type	Service Location	Description
MSS-CPE Managed Security Service-Customer Premise Equipment	User premises	Customers retain ownership of security technology; MSSP can place monitoring devices on the client network or at the data center site. For example, through log management, MSSP can place log collection devices on the customer premises to collect and standardize tens of thousands of log events generated daily by servers, routers, firewalls, endpoints and other devices.
MSS-Hosted Managed Security Service-Hosted	Inside data center of operators or cloud hosting suppliers	Large operators and cloud hosting providers usually provide purified traffic to customers to protect them from cyberattacks. At present, this method has also been applied to internal deployment management and monitoring.
CHESS Cloud Hosted Enterprise Security Service	Public cloud	CHESS is a service delivered only through the cloud and managed through the cloud. Customers do not need to deploy the underlying IT security architecture internally. It is the same as security as a service.

Customers need to choose the corresponding security management services according to their IT deployment situation.

At present, the Chinese market is still dominated by MSS-CPE, and the main investment in IT security defense systems is assumed by customers. However, with the development of cloud, more MSS-Hosted will be found in private cloud or industry cloud. In public cloud, demand for CHESS will increase.

3.4 Leadership: Continuously Introduce Innovative Technologies to Enhance System Defense Capabilities

The leadership of an active security defense system is characterized by time window, that is, when the attacker adopts more advanced technology, the effect of the defender's defense system will decline. Therefore, the defending side will have to input innovative technology continuously to ensure the continuous improvement of its defensive capability.

Building active security defense systems is a task which requires long-term input. For example, when an enterprise uses third platform technology to start to make digital transformation, the active security defense system will provide effective protection for the cloud environment, mobile environment, social environment and big data environment. Therefore, it is necessary to integrate continuously emerging innovative technologies into the active security defense system so as to achieve the desired defense effect.

It is worth mentioning that AI technology has attracted great attention in the field of cybersecurity. AI technology can be integrated into different fields, and cybersecurity is one of them.

In the field of cybersecurity, according to IDC, AI is capable of providing consulting, enhanced services and semi-automated cybersecurity defense functions based on a series of structured and unstructured data (including logs, device telemetry, network data packets and other available information). Essentially, its goal is to capture and replicate the strategy, technology and decision-making process of the best security experts by creating an AI-enabled analysis platform, and complete the threat detection and repair process through automatic analysis method's. AI-enabled analysis platforms usually start with common algorithms and are gradually applied to increasingly complex application scenarios. By using a large amount of structured and unstructured data, AI-enabled security platforms can answer questions, provide suggestions and trend analysis through in-depth analysis, and formulate response measures based on existing conditions. At the same time, by taking in a lot of training content, AI-enabled platforms can adaptively learn lessons from the failures of security experts, so as to enhance the defensive capabilities of cybersecurity defense systems.

In the future, active security defense systems will face more challenges of advanced technology-based cyberattack. IDC predicts that by 2024, quantum computing will be fully developed, and 25% of the countries in the world will be able to decrypt current public key infrastructure (PKI) technologies. The ability of active security defense systems to meet new challenges will still depend on the introduction of innovative technologies.

04
Sangfor's Security Architecture

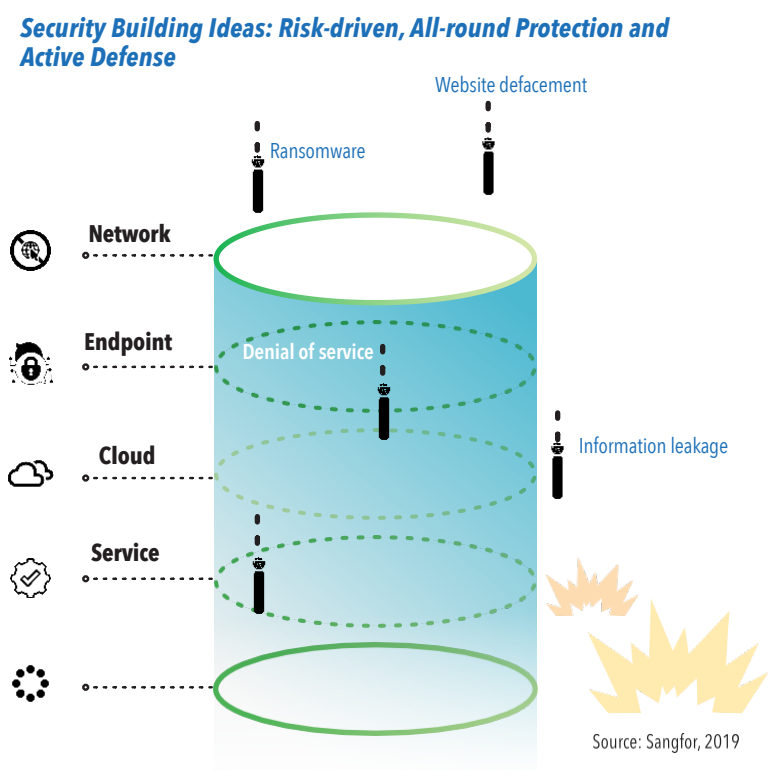
In the process of digital transformation, security protection capabilities need to evolve to adapt to changing business scenarios. To guide users to build effective protection security capabilities for the future, Sangfor has established a complete security construction methodology, which includes 3 parts: clear thinking, design model and sound framework.

Sangfor's idea of service security construction can be summarized as risk-driven, all-round protection and active defense. Based on this idea, Sangfor has designed a complete APDRO (Artificial Intelligence, Protect, Detect, Respond, Operate) capability model, including the five dimensions of artificial intelligence, protect, detect, respond, operate, to help users to achieve the security goal of "future-proof effective protection". With this intelligent security capability model as the guide, Sangfor has formed an implementation framework for security capacity building, which mainly includes technology, management and operation.

4.1 Security Building Ideas: Risk Driven, All-round Protection and Active Defense

Compared with traditional cybersecurity control measures which are over dependent on boundary defense, Sangfor believes that the idea of security construction should achieve continuous risk assessment and effective risk management through being risk-driven, all-round protection and active defense.

Figure 22 Security Building Ideas: Risk Driven, All-round Protection and Active Defense



Risk Driven: Continuous risk assessment is the prerequisite for safety control measures to be effective. Risk assessment can comprehensively assess the possibility and impact of security incidents according to the importance of business-carrying assets, taking into account the frequency of threats and the vulnerability of assets themselves.

All-round protection: Risk disposal cannot merely rely on boundary defense. Rather, it requires defense, detection and response through the levels of cloud, network, endpoint and security services. When control measures at one level are amiss, they can be supplemented by control measures at other levels, and risks can be fully dealt with in a holistic and structured way through structured and coordinated protection at all levels.

Active defense: Continuous security monitoring and risk prediction combined with threat intelligence are needed to achieve active defense. Through active defense, it is possible to make timely and precision early warnings, build a flexible defense system real time, and avoid, transfer and reduce the risks faced by an information system before intrusions affect the information system.

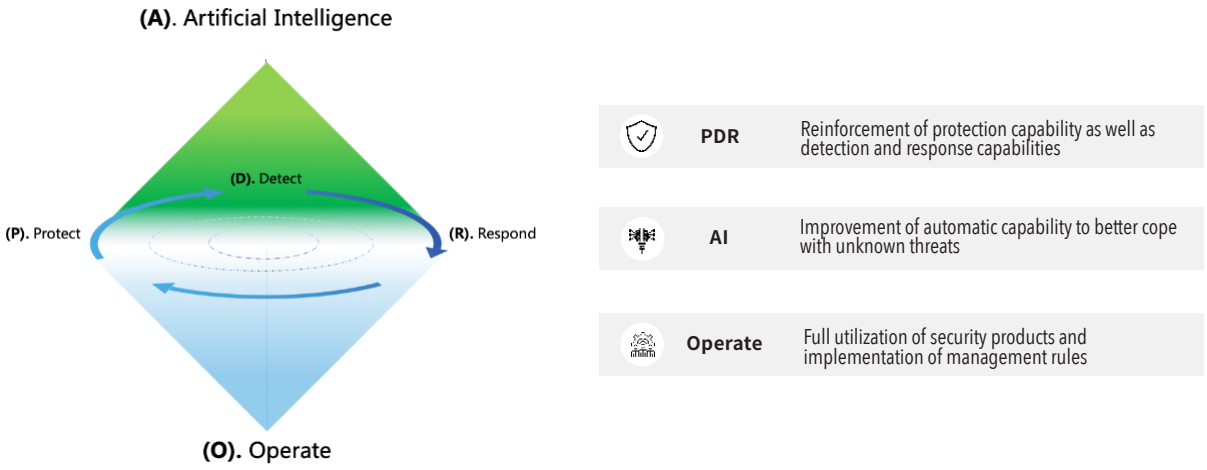
4.2 Security Capability Model: APDRO

In cybersecurity work, the commonly used models in the past are: PDR (protect, detect and respond), PPDR (security policy, protect, detect and respond), PDRR (protect, detect, respond and recover), ASA adaptive security framework (predict protect, detect and respond), etc. From these existing models, it is not difficult to find that the existing risk management models contain protect, detect and respond (PDR). It is generally believed that protect, detect and respond are three indispensable functional elements of security. As hacker attacks become more and more frequent and are accompanied by a large number of unknown threats, it is necessary to use AI-based automatic tools to improve the efficiency of PDR, and use AI to enhance the ability to detect unknown threats.

On the other hand, the essence of security is the confrontation between attack and defense. For the defending party, it is necessary to make full use, through manual operations, of all kinds of security equipment purchased, give full play to the security value of network equipment, and effectively implement the security business objectives and management regulations.

Generally, the logic of the APDRO capability model is to firstly build closed-loop security capability that integrates PDR into one body; secondly to use AI technology to enhance the automatic capabilities of PDR in face of a large number of frequent unknown threats; finally to truly put security products into operation, making PDR more effective. As shown in the figure below, the APDRO risk management model consists of five functional domains, namely Artificial Intelligence, Protect, Detect, Respond and Operate.

Figure 23: Sangfor's Security Capability Model: APDRO



Source: Sangfor, 2019

Artificial Intelligence: to intelligently enhance PDR. The intelligent functions provide data-driven, AI algorithm-based security capabilities.

Protect: to guarantee the delivery of key services. The protection function provides the ability to limit or control the impact of potential cybersecurity incidents.

Detect: to identify the occurrence of cybersecurity incidents. The detection function provides the ability to continuously detect cybersecurity incidents.

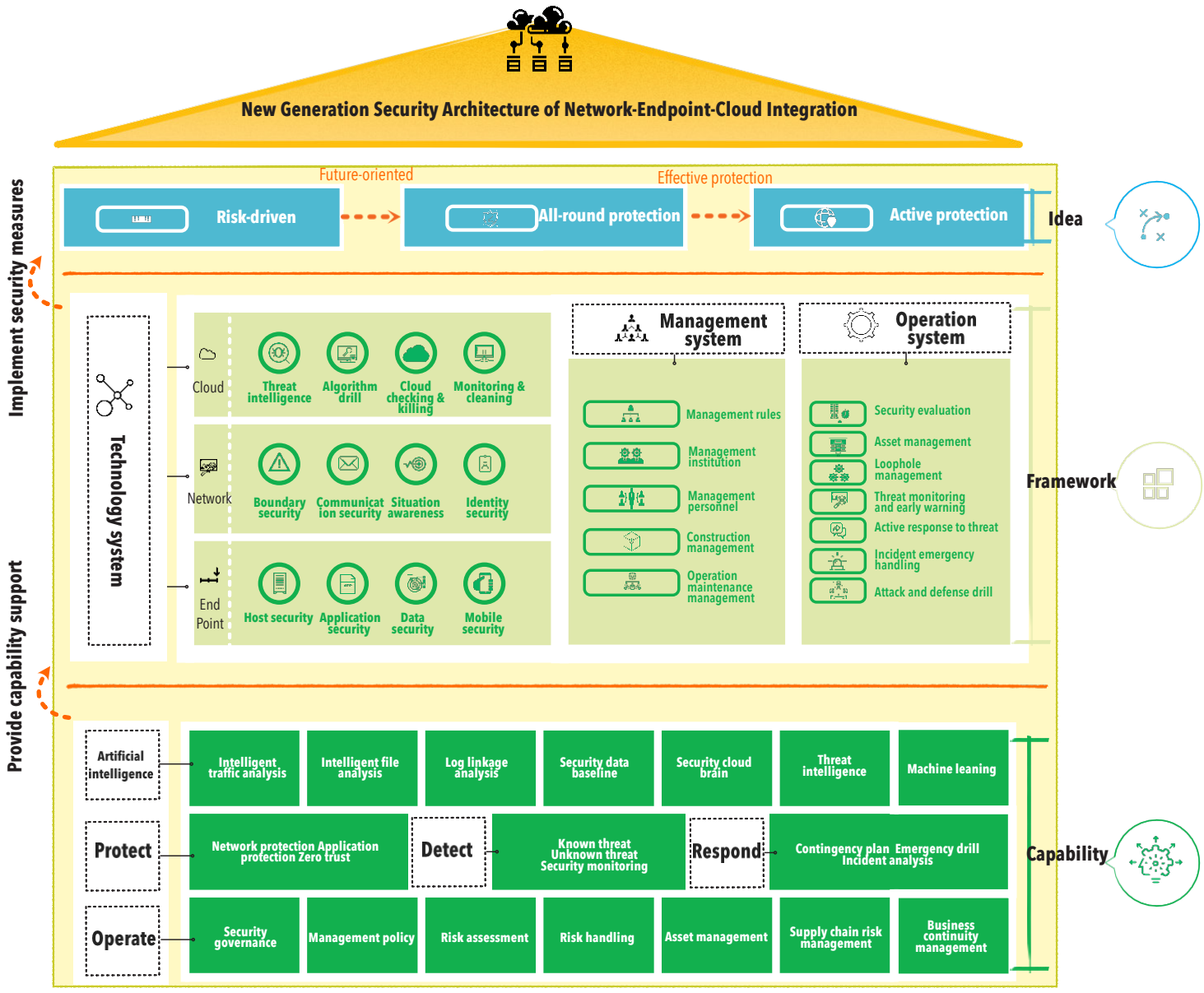
Respond: to deal with detected cybersecurity incidents. The response function provides the ability to control the impact of potential cybersecurity risk incidents.

Operate: to achieve all-weather secure operation. The operation function provides the ability to supervise, monitor enterprise security, intrusion detection and respond to cybersecurity incidents.

4.3 New-Generation Security Architecture of Network-Endpoint-Cloud Integration

In combination with the idea and capability model of cybersecurity work, Sangfor has stablished a new-generation security architecture for network-endpoint-cloud integration as a blueprint to support users' security construction. Through real-time empowering at the cloud endpoint and by the Neural-X, the architecture continuously enhances network and end terminal capabilities, achieve network and endpoint collaboration, and fast reduce closed-loop risks.

Figure 24: Sangfor's New Generation Security Architecture of Network-Endpoint-Cloud Integration



Source: Sangfor, 2019

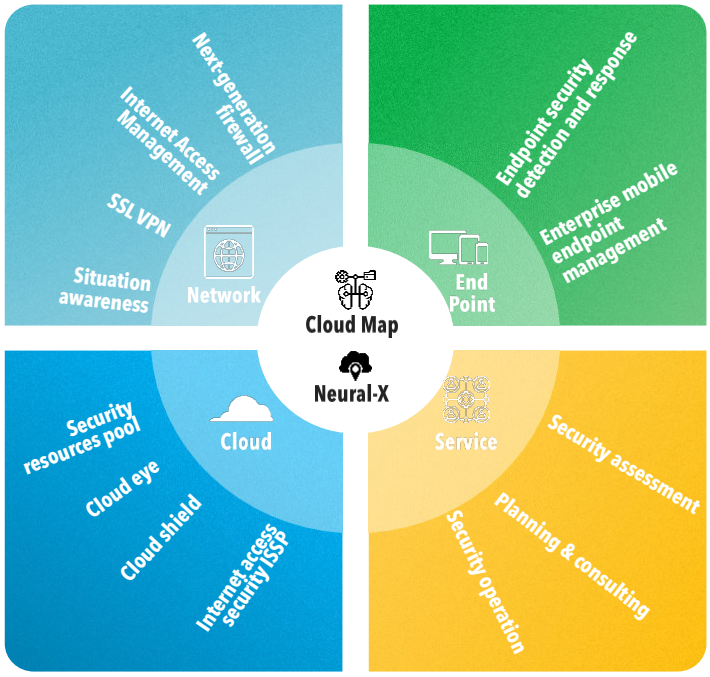
In terms of technology, the architecture evaluates the actual risks faced by organizations, and selects appropriate control measures to deal with risks at various levels such as cloud, network and endpoint.

As for management, it makes bottom-up planning in combination with Information Security Technology—Baseline for Cybersecurity Classified Protection, ISO27001 Information Security Management System Requirements, industry requirements, the requirements of the higher supervising body and the actual internal and external environment of the organization; by integrating the methods of the management system via PAS99, it runs one management system while meeting the requirements of standards at multiple levels.

Concerning operation, in combination with AI and experts, the architecture ensures efficiency and effectiveness through human-computer co-intelligence, and helps organizations and institutions to better implement security capabilities, such as strengthening security incident response capacity through event management.

4.4 Future-Proof Effective Protection

Figure 25: Sangfor's Future-Proof Effective Protection



Source: Sangfor, 2019

Of course, the final implementation of security architecture is not separable from specific risk control measures such as security products and security services. Adhering to the idea of bringing out "future-proof effective protection", Sangfor will continuously make use of Neural-X and cloud map at the cloud endpoint and cover four forms of delivery, namely network, endpoint, cloud and service, by providing security products such as next-generation firewalls, online behavior management, posture sensing and etc., as well as security assessment, planning and consulting, security operations and other services.

In addition, Sangfor provides various solutions to meet the requirement of the cybersecurity classified protection 2.0, to actively defense against blackmail viruses, cloud data center, big data platform and overall security planning from the different perspectives of compliance, risk, business and security planning, to meet the security needs of different industries under different scenarios.

ABOUT SANGFOR

Sangfor Technologies is a leading global vendor of IT infrastructure solutions, specializing in cloud computing, network security and infrastructure with a wide range of products. Sangfor is committed to carrying the foundational work in the process of users' digital transformation in various industries, so as to make users' IT simpler, safer, and more valuable. Sangfor now has over 4,500 employees with more than 50 branch offices around the world. The company has been awarded as a national high-tech enterprise and hosts the National and Local Joint Engineering Laboratory of Next-Generation Internet Information Security Technology, and Guangdong Research Center for Intelligent Cloud Computing Engineering.

Sangfor has adhered to the idea of continuous innovation to develop convenient products for users, winning wide recognition in the market and providing products to nearly 100,000 users.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com