A Forrester Consulting
Thought Leadership Paper
Commissioned By Huawei

October 2019

Artificial Intelligence Firewalls — The Intelligent Solution For Enterprise Cybersecurity

FORRESTER®

Table Of Contents

Project Director:
Diane Deng,
Market Impact Consultant

Contributing Research:
Forrester B2C Marketing Team
Forrester Security Research Team

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

Executive Summary

A digital wave is sweeping the world. Unprecedented widespread connectivity, explosive data growth, and thriving intelligent applications will profoundly change the way people live and work. Interactions between individuals, enterprises, and between individuals and enterprises are getting more frequent than ever, and the exchange of data will only boost economic development. However, in the meantime, criminals in the cyber gray zone continue their attempts of stealing personally identifiable information, corporate secrets, and even computing resources to make illegal profits. As we enjoy the convenience brought on by the digital wave, we also have to face the security risks that come along with it. In recent years, corporate security incidents have become a necessary and consistent evil, whereas the occur all the time and cause great losses. However, after the ten years since its inception, the next-generation firewall (NGFW) finds it hard to cope with the growing number of cyberattacks.

After several ups and downs, AI technologies have continued to be refined, and in recent years have become more well-developed. Many believe that AI will inject new vitality into all walks of life, and bring new opportunities for security protection. Practice has shown that AI technologies can extract insights from data, revolutionize the capabilities of threat detection, respond to incidents and security operation and maintenance, and will promote the evolution of firewalls into of artificial intelligence firewalls (AIFWs).

In July 2019, Huawei commissioned Forrester Consulting to conduct research on the trend of global cybersecurity. Forrester interviewed 200 decision makers in network security and firewall deployment for large and midsize enterprises worldwide, in order to understand the current challenges faced by the NGFW, against the backdrop of an increasingly complex network security situation, and propose strategic recommendations for the evolution of firewall technology.

AI technologies will promote the evolution of NGFW to artificial intelligence firewall (AIFW).

KEY FINDINGS

- **The network security situation is getting grim.** A greater number of important information is put on the internet, leading to diverse, sophisticated, and extensive cyberattacks. Only 2% of respondents did not experience any security incidents over the past year. Companies must invest more to defend cyberattacks.
- **Enterprises using NGFW are now challenged.** NGFW was first introduced in the PC Internet era, and is based on application detection visibility and control. With the rapid development of the mobile internet and cloud computing, a large number of web applications become exposed to the internet; and traditional firewalls no longer perform well in this confusing situation. It is hard to detect and block advanced persistent threats (APTs) or locate and respond to internal threats, posing severe challenges for operation and maintenance.
- **Artificial intelligence firewalls came into being.** The development of AI technologies will promote the evolution of NGFW to the AIFW. AI technology can tackle the shortcomings of static rule engines, thereby strengthening threat detection. It also deals with the difficulties in operation and maintenance through automation. The prosperity of the hardware ecosystem and the emergence of AI chips guarantee AI applications in the firewall field. Artificial intelligence can also help with synergies between equipment and cloud-edge collaboration, promoting the development of a secure and interactive ecosystem, and build solid security platforms to safeguard the companies.

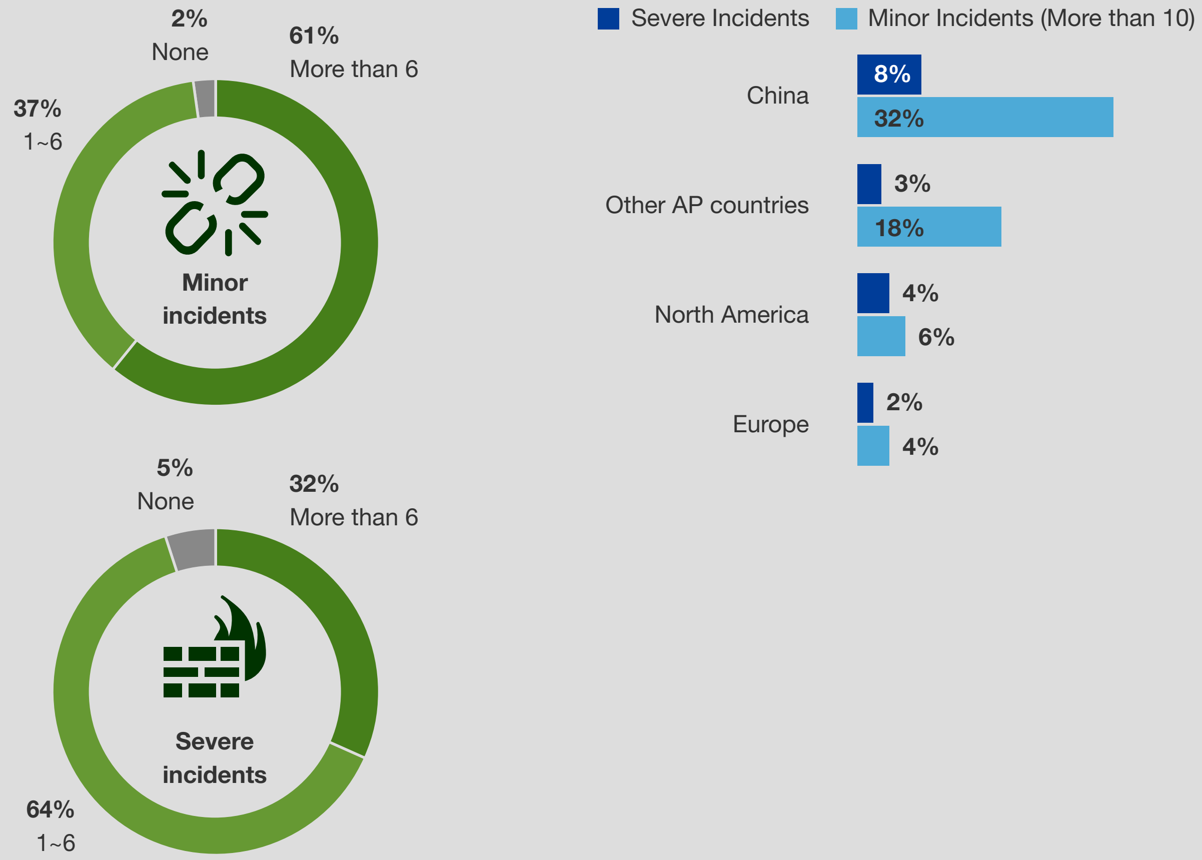
The Increasingly Severe Network Security Situation

Technology development is a double-edged sword. It benefits enterprises and individuals, but it also arms criminals. The situation of network security has gotten more severe in recent years, as intelligent and automation technologies can be conducive to new types of cyberattacks that more diverse, complex, and extensive. In this survey, nearly one-third of respondents had more than six serious security incidents in the past year, and only 2% did not encounter any security incidents (see Figure 1). Therefore, companies have to invest considerably to ensure information security. Forrester Business Technographics data shows that 88% of respondents believe they need to enhance their security control, which tops the list of 13 initiatives, including improving the data analysis capability and expanding the use of cloud computing.

Security incidents are so frequent that only 2% of security decision makers worldwide say there were no security incidents in the past year.

Figure 1: Security Incidents Are Frequent In Companies

"Approximately how many security incidents occurred to your company in the past 12 months?"



Base: 200 decision makers for network security and firewall deployment from large and midsize enterprises worldwide
Source: A Forrester Consulting independent research commissioned by Huawei

CYBERATTACKS ARE COMPLEX AND DIVERSE

As more applications are exposed to the internet, attempted attacks by cyber criminals grow rampant (see Figure 2). In 2018, CNCERT (China's National Computer Network Emergency Response Technical Team) captured nearly 140,000 ransomware attacks; and into 2019 this number has continued to rise. Targeted attacks such as the evasion technique, the zero-day exploit, credential theft, and professional phishing are all becoming more sophisticated, and variants of attacks only make things worse. GrandCrab for example evolved so fast that it had 19 modifications in 2018, alone. Widespread and continuously evolving hacking techniques and tools may explain the advancement of cyberattacks. Well-planned and organized APTs hinder security analysts of companies using NGFW from locating the problem among multiple threats in the cyber kill chain.

Figure 2: Diverse Cyber Attacks And Tools

"What issues pose serious challenges to your company's cyber security, due to diverse and perplexed cyber attacks?"

Rank	China	Other AP countries	North America	Europe
1	Malicious URL	Malicious URL	Social engineering	Malicious URL
2	Social engineering	Attack at web port	Malicious URL	Attack at web port
3	Malicious code implantation	Social engineering	Malicious code implantation	Social engineering
4	Attack at web port	Large-scale DDoS attacks	Large-scale DDoS attacks	Malicious code implantation

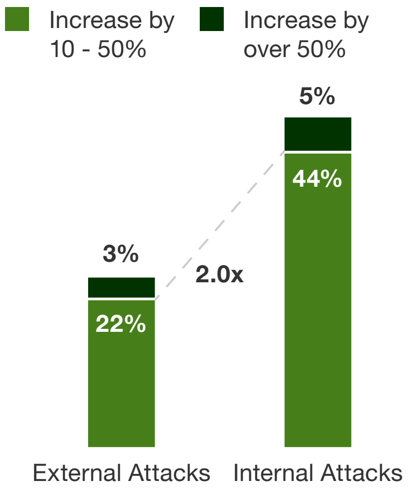
Base: 200 decision makers for network security and firewall deployment from large and midsize enterprises worldwide
Source: A Forrester Consulting independent research commissioned by Huawei

EXTENSIVE SECURITY ATTACKS

The development of cloud computing, 5G, and the consequent explosive growth of internet of things (IoT) have expanded the security boundaries of companies, leading to more extensive cyberattacks. The targets go beyond computers to all exploitable ICT devices, and the attackers originate not only from the outside but also from within, or as third-party vendors. Internal cyberthreats in particular are harder to detect than external attacks because the attackers have legitimate access to information. In the survey, 64% of respondents say they had an increased number of external attacks in the past year, and 80% experienced rising internal cyberthreats. Among them, 25% of respondents say external attacks grew by more than 10%, while 49% say internal attacks rose by more than 10% (see Figure 3). Enterprises must increase prevention and protection measures to counter extensive attacks, strengthen the defense lines against internal and external threats, and use other security products to block threats in the entire network.

Figure 3: Increasing Internal Attacks Raise Concerns Within The Company

“What are the trends of the external and internal attacks compared to three years ago?”



Base: 200 decision makers for network security and firewall deployment from large and midsize enterprises worldwide
Source: A Forrester Consulting independent research commissioned by Huawei

Enterprises Using NGFW Are Challenged

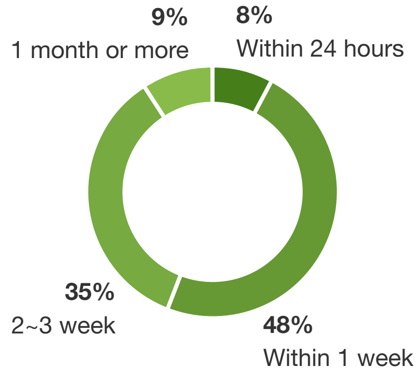
Since its inception, firewall technologies have witnessed the transition from the PC era, to the Network era, to the PC Internet era, and now the Mobile Internet era. To defeat evolving threats and attacks, firewall technologies continue upgrading actively to solve problems in performance, operation, and maintenance. When NGFW was first introduced in 2009, its application detection, IPS, and security analysis capabilities gained wide acknowledgement among companies in the PC Internet era. Nonetheless, cyber criminals have also made great technical strides over the past decade. Increasingly rampant and intelligent security attacks will severely challenge NGFW’s abilities of prevention and control as we are entering an age of intelligent connectivity.

NGFW STRUGGLES WITH RAPIDLY MUTATING THREATS

NGFW can identify application vulnerabilities more effectively than previous firewalls, but its rule engine still has significant limitations. The existing solution would generate a signature for a single threat that has been identified, but once the threat mutates, the signature no longer works. This means the NGFW needs to be continuously updating its signature database, which requires person-power to manually renew the solution. However, each local device can only accommodate limited number of signature databases, making it hard to respond to new changes, so the operation and maintenance (O&M) personnel have to change the rules constantly, in order to maintain prevention and control capabilities. Through continuous variants of threats, cyber criminals can easily put firewalls to passive responses, agreed by 57% of respondents. Only 8% of respondents believe they can configure the firewall within 24 hours, while 44% need more than a week (Figure 4). Untimely updates open a window for attackers to sneak in. Therefore, the post-event management must intelligently shift the focus from experience to data and insights, to address severe security challenges.

Figure 4: Current Firewall Can't Keep Up With The Digital Process

"How long does it take on average to configure firewall rules?"



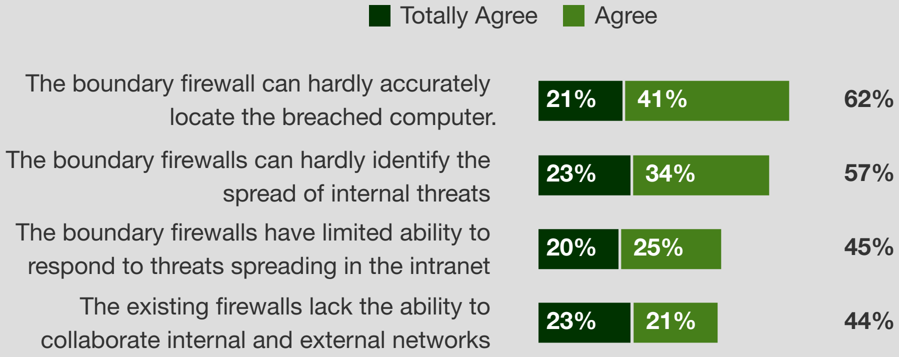
Base: 200 decision makers for network security and firewall deployment from large and midsize enterprises worldwide
Note: from workload building to the effective use of the new rule
Source: A Forrester Consulting independent research commissioned by Huawei

NGFW STUMBLES IN EXTENSIVE ATTACKS

Cybersecurity threats spread quickly in all dimensions, but NGFW can only protect the preset protocols or applications in the database, and it can do nothing to those outside the database, even if they are of the same type. For intranet attacks, it is critical to swiftly spot the threat and locate the breached computer through means like behavior analysis and abnormal traffic detection, in order to mitigate damage, stop internal diffusion, and build both a comprehensive fence against the APT attack chain and a detection network that spans the boundary of the enterprise. The current NGFW can barely cope with intranet attacks, testified by 62% of respondents who say existing firewalls fail to locate intranet breached computers in the intranet, and 57% of respondents that doubt whether they can identify the spread of internal threats (see Figure 5).

Figure 5

"To what extent do you agree with the following statement regarding challenges in intranet security?"



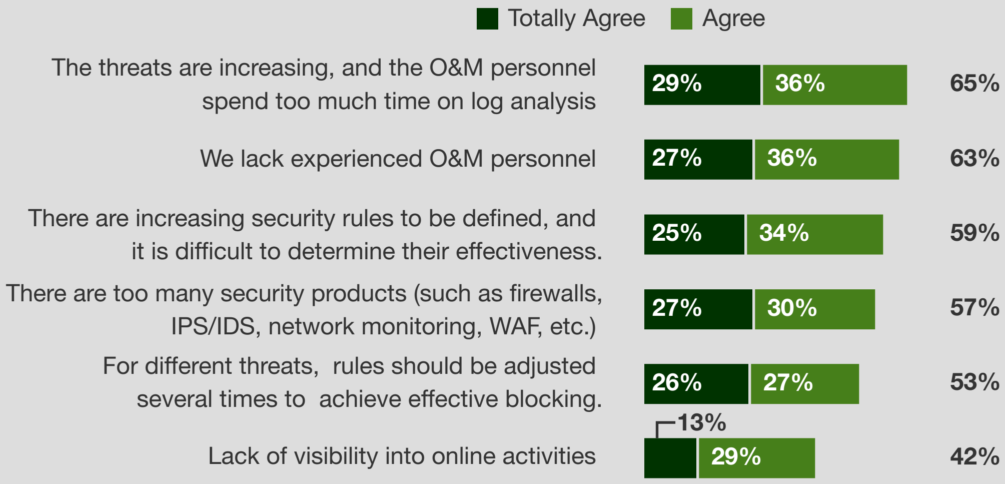
Base: 200 decision makers for network security and firewall deployment from large and midsize enterprises worldwide
Source: A Forrester Consulting independent research commissioned by Huawei

NGFW MAINTENANCE IS STRESSFUL

Routine maintenance is critical after NGFW deployment. The O&M personnel update the rules continually for threat mutations, but gradually these personnel will experience stress and be at risk of attrition. It is more prudent to delete an old rule than adding a new one, so rules keep increasing, thereby perplexing the management. A large number of rule comparisons lower the prevention and control performance. In addition, most NGFWs lack effective data analysis capabilities, requiring O&M personnel to manually analyze massive security logs. In general, the team can only review thousands of log data or hundreds of code segments per day. Their workload is heavy and demanding, but the effect cannot be guaranteed. Log analysis relies heavily on the experience of security personnel, which undoubtedly increases the company's investment in operation and maintenance, as well as risks caused by staff turnover. Sixty-five percent of respondents believe their O&M personnel spend too much time on log analysis, and 63% say that they lack experienced security staff (Figure 6).

Figure 6

"With the deepening of the digital transformation, how much do you agree with the following trends in security operation and maintenance?"



Base: 200 decision makers for network security and firewall deployment from large and midsize enterprises worldwide
Source: A Forrester Consulting independent research commissioned by Huawei

Artificial Intelligence Brings Important Opportunities

After various ups and downs, AI has gained widespread attention again in the past decade. New technologies like deep learning can make full use of big data in the Mobile Internet era to achieve breakthroughs in accuracy, outperforming human beings in many tasks. Given the severity of security situations, and the challenges faced by NGFW, AI technology can map massive amount of information to high-dimensional spaces with better information abstraction capabilities, bringing new opportunities to security protection with its generalization and inferential capabilities.

A firewall equipped with local AI can cope with unknown threats that were deemed difficult in the past, greatly improving both the efficiency of detecting mutating attacks and the subsequent work of O&M personnel, thereby advancing enterprise security to a new level.

AI DISRUPTS THE PREVENTION AND CONTROL OF CYBERATTACKS

Threat prevention and control are two primary tasks for any firewall. AI provides more accurate APT detection, more powerful event analysis, and a closed defense loop that spins faster, which greatly enhance the firewall's ability to prevent and control threats. Specifically, AI can:

› **Defend new threats effectively.** Traditional solutions, based on signatures or rules, are relatively static and struggle to catch up with rapidly mutating threats in proactive defense. AI technology goes beyond the limitations of human beings' low-dimensional cognition and can better understand the behavioral patterns of threats and attacks at a deeper level. In practice, supervised and unsupervised learning are used to spot frequent variants of malware, locate breached hosts and zombies, detect the theft of encrypted outgoing messages, and identify malicious behaviors like low frequency or distributed brute force attacks. AI learning taps into massive data to generate defense models based on scenario analysis; it upgrades the models continuously according to the real-time data to achieve self-evolution.

- **Strengthen intelligent analysis of security incidents.** Various attacks do leave traces in security logs, but it requires a lot of person-power to detect the threats (from countless logs of operating systems, threats, and network protection) and refine insights to continuously enhance prevention and control capabilities. Therefore, most companies have never fully taped into the security data they have. AI can revolutionize event analysis of cyberthreats. For example, AI knowledge mapping can sort local knowledge such as attack and defense database and threat events, and use them with environmental, behavioral, and intelligence data to dig into data and better detect and defend from threats targeted at critical assets.

- **Support quicker response to APT attacks.** When an intrusion is detected, it is vital to quickly locate and separate the problem and carry out sensible defense. The AI-based APT defense model is more lightweight than traditional solutions and can be easily integrated to the local firewall. Compared with the collaborative external detection in the past, the AI-based APT defense model shortens the exposure time of APT attacks and helps minimize the losses. In the survey, 82% of respondents express concern over the speed of response to cyberattacks (see Figure 7).

AI EMPOWERS INTEGRATED SECURITY PROTECTION

AI improves security data analysis and provides better threat detection and prevention capabilities than static rule engines, equipping enterprise firewalls for cyberattacks. AI can also connect equipment in the network for joint machine learning, in order to optimize the defense model on a regular basis.

- **Federal learning continually optimizes the defense.** Restricted by industry sensitivity and policies in some countries, many companies are still uncertain about in-depth sharing of security data with each other. Through encrypted exchanges of parameters, federated learning can improve the sharing model without moving the data, thereby enriching the training data sets for AI to build distributed AI collaborative defenses. AI firewall can also utilize the threat intelligence in the entire network to sustainably and swiftly update the detection and response model to maintain effective defense.

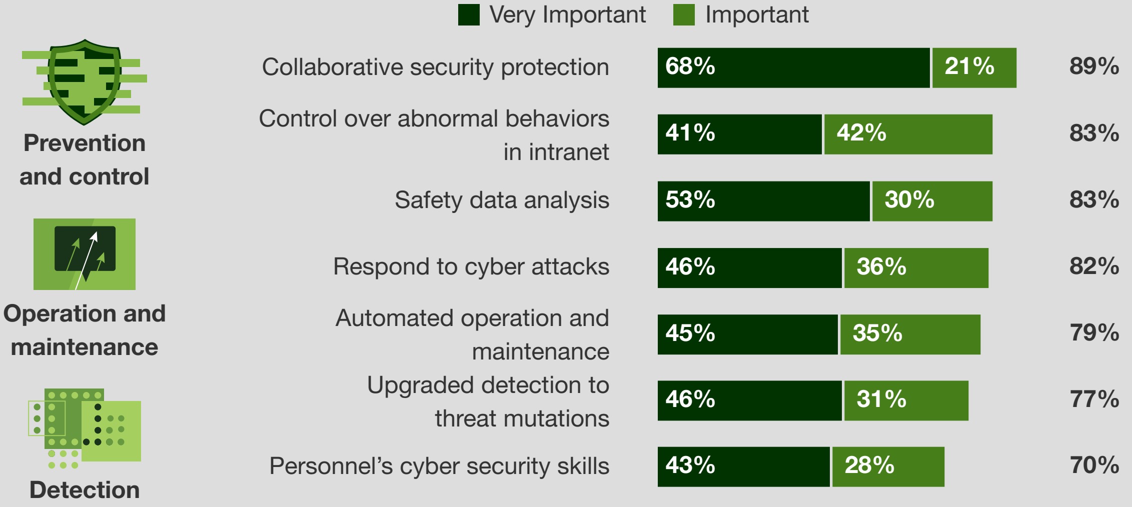
- **Deploy intranet defense and enhance collaborative detection.** A firewall can set built-in traps that will form a safety net for internal threats, using AI-based traffic analysis to identify malicious or illegal traffic for collaborative detection in the intranet. Eighty-three percent of respondents believe that the control over abnormal behaviors in the internal network is an essential function of the firewall. An AIFW can intelligently identify and collaborate with other APT defense systems to better safeguard and realize automated closed defense loops through open interfaces. Eighty-nine percent of respondents value collaborative security protection (see Figure 7).

AI PROVIDES NECESSARY TOOLS TO IMPROVE O&M EFFICIENCY

The shortage of senior security O&M personnel is a consensus in the industry. Improving O&M capabilities is one of the most important challenges for the existing prevention and control technology. AI can efficiently analyze massive logs, sparing more time for the O&M personnel. It can also reduce redundancy in security rules through intelligent tuning or even automated generation, reducing the pressure on O&M personnel to maintain huge databases. AI models digitally sort the experience/knowledge and powers automation of safety operation/maintenance, thus filling the gap of talent shortage. In the survey, 79% of respondents believe that automated O&M is of great importance (Figure 7).

Figure 7

"How important are following capabilities of firewalls used by your company?"



Base: 200 decision makers for network security and firewall deployment from large and midsize enterprises worldwide
Source: A Forrester Consulting independent research commissioned by Huawei

AI Firewall Is An Inevitable Choice

In the era of intelligent connectivity, NGFW is severely challenged by increasingly complex security situations, while AI brings new opportunities for enterprise firewalls. Therefore, NGFW should embrace AI and evolve into the AIFW to strengthen prevention and control, to build integrated protection capability, and to improve operation and maintenance efficiency. To give full play to AI and maximize the prevention and control performance of AIFW, dedicated AI chips, cloud-edge collaboration, and security ecosystem are indispensable for firewall evolution, the reliable safeguard of enterprises, and progression for the entire industry.

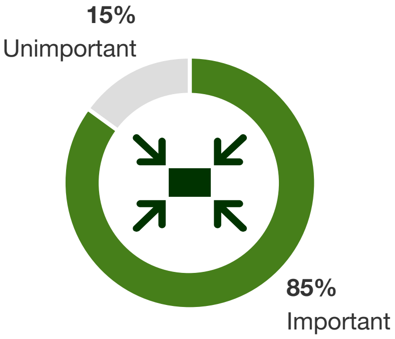
NGFW should fully embrace AI and evolve into the AIFW to strengthen prevention and control, to build integrated protection capability, and to improve operation and maintenance efficiency.

AI CHIPS FUEL THE ENGINE FOR LOCAL APT DEFENSE

To build localized defense against APTs, AIFW needs a built-in AI detection engine to respond to threat mutations through self-evolution. Encryption and decryption, packet detection, and traffic forwarding already consume a lot of the computing power of a firewall, but the AI detection engine also demands massive computing power to process mass data and AI inference. Therefore, AI chips are a must-have to enhance computer power for detection, effective emergency response, and other functions of the firewall, providing shorter response time than the cloud's big data solutions. In principle, the selection of chips should vary due to the diversity of computational tasks, thus dedicated security chips, co-processors, and AI chips will become increasingly important for AIFW. In this survey, 85% of respondents believe they need a dedicated chip to accelerate AI calculation and inference, in order to have better defense against APTs (see Figure 8).

Figure 8

"What do you think about the importance of using dedicated chips to enhance computing power and hardware acceleration in your security strategy?"



Base: 200 decision makers for network security and firewall deployment from large and midsize enterprises worldwide
Source: A Forrester Consulting independent research commissioned by Huawei

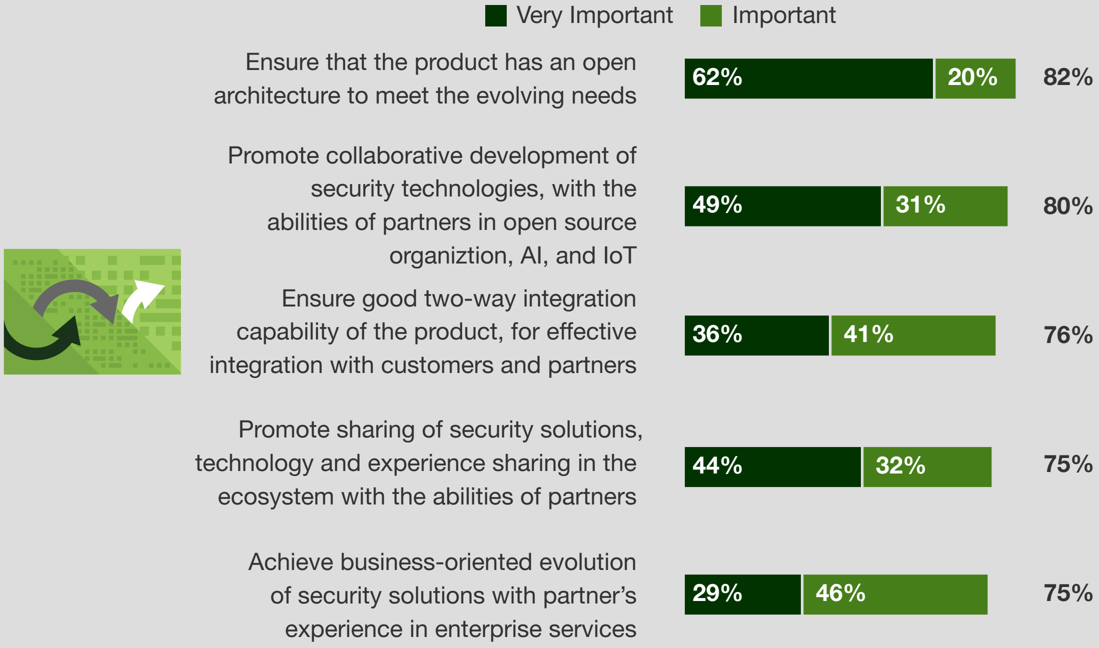
BUILD YOUR CYBERSECURITY PLATFORM UPON EXTENSIVE COLLABORATION

The growth of IoT applications will extend the security boundaries of enterprises and impact the form of the firewall. Boundary defense requires a collaborative threat detection of AIFWs and other APT defense equipment and clouds.

In the long run, comprehensive security prevention and control also requires extensive alliance in the ecosystem to remain proactive against cyberattacks. Firewalls will need to be open to share or exchange local intelligence for closer collaboration. In the survey, 82% of respondents expect the open architecture of AIFW for continuous evolution (see Figure 9). Companies need to leverage the advantages of partners to share security solutions and experience, which can also promote the development of technologies like AI and IoT and form a virtuous circle. Multiparty collaboration will be critical to securing the victory in the ongoing battle against cyber criminals.

Figure 9: Companies Expect Products To Have Open Architecture And Provide Better Security Without Compromising On Performance

"How important do you think about the following aspects of continuous upgrade in a collaborative ecosystem?"



Base: 200 decision makers for network security and firewall deployment from large and midsize enterprises worldwide
Source: A Forrester Consulting independent research commissioned by Huawei

Key Recommendations

As we enter the age of intelligent connectivity, cyberattacks are becoming more diverse, sophisticated, and extensive than ever, posing inevitable challenges for companies. Through our survey with 200 cybersecurity decision makers from large and midsize companies worldwide, who are interested in or already using AI in their practices, Forrester recommends that:

AI empowers the next generation of firewalls — the AIFW. As a general-purpose technology, AI will be applied widely in various business scenarios, including cybersecurity. For cyberattacks already armed by intelligent technologies, firewalls based on rule engines are obviously outdated. Enterprises should turn to AIFW for comprehensive local defense against APTs. Adopt AI chips to accelerate task processing and collaborate with AI capability centers on the cloud to continuously update security models and ensure cybersecurity in all aspects.

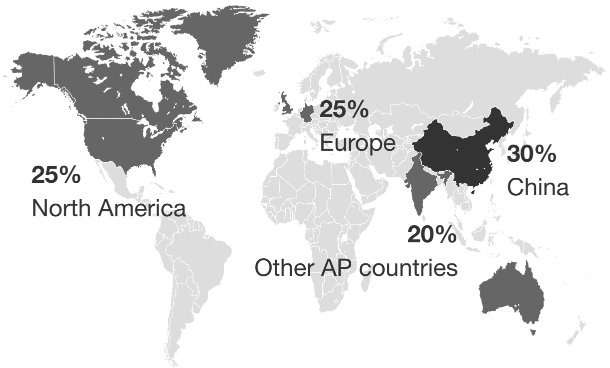
Embrace intelligent applications to improve the O&M efficiency. Intelligent and automated operation and maintenance is the choice of the times. AI-enabled applications like traffic analysis, threat detection, and behavior identification reduce the workload of O&M personnel. The AI-driven intelligent tuning of security rules solves the problems of manual updates, and greatly improves O&M efficiency. As AI detection of unknown threats gets more accurate, false alarms will be significantly reduced, bringing on another leap in O&M quality.

Build your cybersecurity platform upon extensive collaboration. Cyber criminals only exploit a single breach at one time, but the company needs comprehensive defense for being at a disadvantage. As attacks go rampant, companies must collaborate and embrace an extensive ecosystem, share security intelligence, and utilize information from the entire network to build increasingly powerful security models and to jointly win the battle against cyber criminals.

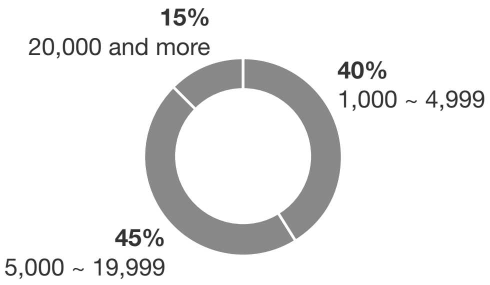
Appendix A: Methodology

In July 2019, Huawei commissioned Forrester Consulting to conduct a research on the trend of global cybersecurity. We have interviewed 200 decision makers for network security and firewall deployment from large and midsize enterprises worldwide. The survey was completed in August 2019.

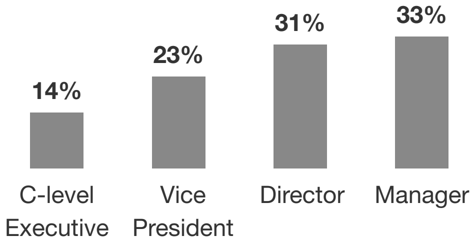
Appendix B: Demographics/Data



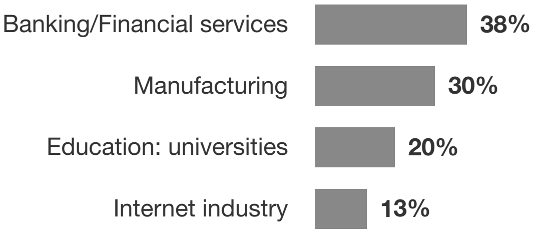
COMPANY SIZE



POSITIONS



INDUSTRY



Base: 200 decision makers for network security from large and midsize enterprises worldwide
Source: A Forrester Consulting independent research commissioned by Huawei