AKAMAI CUSTOMER STORY

KKLab introduces Akamai's Zero Trust solution, combining flexibility and protection for both internal and external networks

100
Emails automatically blocked per day with malicious behaviors

Set up a proof of concept in just 30 minutes

Strengthens security while still maintaining flexibility

Around 2015, the R&D unit of KKBOX, which became the innovative research company KKLab in 2019, started to take a closer look at information security. The R&D team conducted different experiments and hired an external team of professionals to perform hacker intrusion drills and penetration tests to discover potential breaches to systems that could be refined and improved. The unit decided to implement multi-factor authentication, and also introduced Akamai Enterprise Threat Protector to prevent targeted attacks and Enterprise Application Access to ensure application system access security. With the introduction of these two cloud-based information security services, the company realized Zero Trust security.

Moving toward a Zero Trust architecture reinforces the vulnerabilities of traditional VPNs

KKLab AVP Hung-Yi Chen said that KKBOX Group has always been technology oriented. He joined the group while completing his studies in 2005 and has focused on technology R&D for 15 years. As the group grew, he helped introduce many interesting and challenging new technologies. This included the establishment of a site reliability engineering team in 2010, the introduction of CI/CD, and the deployment of a hybrid cloud architecture. He later joined KKLab, a cloud-based technology service provider that uses its foundation of research into the cloud and artificial intelligence to help companies promote technological transformation.

KKLab
Taipei, Taiwan
www.kklab.com

Industry
Media

Challenge
Move toward Zero Trust security with multi-factor authentication, application system access security, and further prevention of targeted attacks

Solutions
- Enterprise Threat Protector
- Enterprise Application Access

KKLab supports technology services for various businesses within the group, such as KKBOX, KKTV, KKStream, KKTIX, and theFARM. It also works with external companies through its focus on artificial intelligence and machine learning (AI/ML) tool chains, big data high-speed computing platforms, multiple hybrid cloud construction, and consulting services. The company expanded its digital support to provide services to enterprises in fields such as high-tech manufacturing, retail logistics, media and entertainment, and finance and insurance.

While providing technical services, KKLab also includes information security as a key goal. The company specially introduced third-party information security testing capabilities and used hacking intrusion drills to reveal potential security weaknesses in its systems. Many people at the company were confident that it had a high level of information security and would easily withstand the test. But it was discovered via a database attack test that many accounts and passwords could be compromised by hackers. It made the KKLab team realize that the traditional information security framework and concept of accessing intranet resources through a VPN is actually quite dangerous. Once a hacker obtains an internal account password, they may follow the VPN to enter the intranet and steal information at will, exposing the group to great operating risks.

To counteract the risks, KKLab adopted two-stage security reinforcement measures. First, multi-factor authentication is enforced. Everyone must enter the account password and OTP code at the same time before being allowed to connect to the VPN. In addition, KKLab is actively planning a Zero Trust architecture, which will continuously check and verify whether each visitor is really a legitimate user. The ultimate goal for KKLab is to create a more flexible and safe working environment based around Zero Trust.

> “Akamai Enterprise Threat Protector is mainly responsible for filtering and analyzing connections from the intranet and accurately determining whether the destination has a malicious IP address or domain. The key lies in the big data database.
>
> **Hung-Yi Chen**
> AVP, KKLab

Constructing a protective net with Enterprise Threat Protector/Enterprise Application Access to block every suspicious connection

Chen noted that KKBOX Group, which focuses on entertainment media and streaming technology services, hopes that it can take advantage of the flexibility and block malicious behavior immediately. The company does not want to take excessive control measures that will inhibit the creativity of colleagues, which is why KKLab recommends adopting the Zero Trust model. The solution must be easy to deploy and maintain while affecting the user’s workflow as little as possible. Based on these requirements, the company decided to work with the solutions from Akamai.

“Akamai Enterprise Threat Protector is mainly responsible for filtering and analyzing connections from the intranet and accurately determining whether the destination has a malicious IP address or domain. The key lies in the big data database.” He added that Akamai has a high market share. The first reason why KKLab chose Akamai is the solution’s foundation built around CDN and anti-DDoS services, from which a large amount of malicious behavior data is collected. These powerful resources serve as a vital cornerstone to support the effective operation of Enterprise Threat Protector.

Second, the deployment requirements are different when looking at similar solutions to Enterprise Threat Protector on the market. Some require the installation of an agent on each endpoint device, and some require the installation of a connector on the corporate backbone network. Akamai supports simultaneous connections. The Akamai Connector is a lightweight virtual machine (VM) image, and only a few network settings need to be adjusted. In 2018, KKLab completed the proof of concept in just 30 minutes. It confirmed that with the rich intelligence database, Enterprise Threat Protector with the Akamai Connector could meet its needs, and the company decided to work with Akamai.

In addition to filtering internal and external connections, KKLab introduced Enterprise Application Access in 2020 to control the behavior of employees accessing intranet resources from any location. It deployed the connector using the Docker image. So far, KKLab has connected more than 100 internal application systems through Enterprise Application Access. While many partners used more complicated VPN channels to connect to the intranet system, now they can use the Enterprise Application Access model, which saves them from taking more IT maintenance risks and saves colleagues the extra maintenance burden.

Since deploying Akamai, KKLab has grown to become something more than just a customer. KKLab has deep experience in corporate customer service, and it provided many suggestions and use cases that are helpful to customers, such as adding deeper information in reporting. For example, in addition to knowing the statistics of events such as Trojan horses or phishing during a certain period, KKLab wanted to know who and what device triggered these events. It also suggested adding data visualizations, such as pie charts, bar graphs, and line graphs, in addition to text and numbers on reports. Akamai quickly responded to these suggestions, adjusting its reports and providing greater benefits to global users.

Nowadays, under the protection of Akamai's Zero Trust solution, KKBOX Group automatically blocks a daily average of about 100 emails that are trying to connect users to sites with malicious advertisements, malicious programs, or phishing behaviors. KKLab can easily understand any suspicious connection behavior and prevent issues before they cause harm. The company can then review issues in the architecture or user behavior and make improvements, promoting continuous improvement of information security at KKBOX Group. Looking to the future, KKLab plans to establish a model for the Zero Trust journey experience and provide it as a service to companies outside the group, so that a variety of companies can benefit from it.

Original article published by iThome, Dec 7, 2020, https://www.ithome.com.tw/pr/141499

KKLab Keke Experimental Co., Ltd. was established in 2019. It develops pioneering technology, accelerates industrial development, assists in digital transformation of enterprises, and can simultaneously provide "AI artificial intelligence and machine learning, cloud platform construction and operation, and website reliability engineering (SRE).)" and other one-stop services. KKLab also has an innovative service/IP development acceleration team to assist in the development of new business opportunities. At present, the scope of services spans many industries such as media, entertainment, telecommunications, medical care, and plasticization. We continue to improve technology and deepen the industry, and strive to create more value for customers and the industry.