au Kabucom

Finance firm improves performance and
efficiency for its security team

From perimeter-based security to a Zero Trust model

au Kabucom provides online brokerage services to more than 1.1 million customers across
Japan. In recent years, the company's System Risk Management Department has been
particularly focused on Zero Trust security, an approach in which all communications are
validated and access is strictly controlled for every user and device, regardless of whether
they are inside or outside the network. This move to Zero Trust is driven by the need for secure
and easy access to internal applications for remote workers, an increase in cloud services,
and the new sophisticated attacks that are testing the limits of perimeter-based security.

With regard to remote application access, Yoichi Ishikawa, Head of the System Risk
Management Department, explains, "Today, the definition of 'workspace' extends beyond
just 'the office' to include spaces like our homes and coworking sites. In these times, we
believe that a Zero Trust security environment is necessary for people to be able to work
safely anywhere, anytime, and in the same sort of environment as if they were in the office.
Security is a key focus, but we also need to take into account the ease of remote access
while still ensuring integrated identity management."

"Cyberattacks are becoming more diverse and sophisticated, and we are facing the
limits of perimeter defense," says Koju Ito, a specialist in the System Risk Management
Department. "We are also using a variety of cloud services to improve our efficiency, so we
feel we need to manage and protect each and every one of our devices very closely."

Enterprise Application Access solves VPN-related issues

One question that arose during the move to a Zero Trust architecture was how to securely
allow remote access to endpoints from outside of the office. The existing method was to
use a VPN, but Ito states, "VPN appliances need constant maintenance. Any failure in this
area could lead to threats entering the system if a vulnerability was exposed. And there
are a number of other challenges as well: redundant management for both the VPN and
Active Directory, complicated access procedures when accessing SaaS, overloading the
bandwidth, firewall hardware loads, delays, and so on."

au Kabucom Securities Co., Ltd.
Tokyo, Japan
kabu.com

Industry
Financial Services

Solutions
• Enterprise Application Access
• Secure Internet Access Enterprise

Key impacts
• Reduced application access
  complexity, improved
  performance, and increased
  security by replacing VPN

• Improved proactive malware
  prevention and reduced risk

• Increased operational efficiency
  of security team

While searching for a better solution to these VPN challenges as part of its move to a cloud-first approach, au Kabucom discovered Akamai Enterprise Application Access. "Since it was deployed, we've used Enterprise Application Access in conjunction with identity as a service (IDaaS) to efficiently connect to, and control access to, internal resources and public clouds," explains Ito. "With this setup, we don't need to run the VPN equipment that was causing issues."

Ito adds, "And because the service infrastructure is also provided by Akamai, we can eliminate any delays associated with security measures. In the case of cloud access, Enterprise Application Access can eliminate inefficient procedures and traffic flows associated with one-time client VPN access. This also saves bandwidth and reduces the required investment in hardware. We consider Enterprise Application Access to be a complementary solution that ensures safety for the types of connections which have not yet been inspected or tested for Zero Trust."

Secure Internet Access Enterprise immediately detects malware and reduces operational burden

Migration toward a Zero Trust architecture not only involves secure access, but also threat protection. In addition to improving its remote access, au Kabucom evaluated its existing approach to detecting and blocking malware and decided to deploy Akamai Secure Internet Access Enterprise service to improve its security posture. Secure Internet Access Enterprise is a cloud-based secure web gateway that uses DNS as a proactive security control point.

"Blocking the ever-growing number of threat domains with our own firewall is impossible in terms of capacity. We knew that some attackers steal information using DNS, so the thought that we might be opening ourselves up to unseen threats that could lead to data leaks was a real concern. Since adopting Secure Internet Access Enterprise, we haven't had to worry about this, as Akamai's threat intelligence data is constantly being updated in the cloud. Secure Internet Access Enterprise helps us immediately identify and block new threats that could affect our company, while significantly reducing our operational burden," says Kenta Nakamura of the System Risk Management Department.

Nakamura reports that Secure Internet Access Enterprise defends against a higher number of threats than the web-threat solutions of other companies. Looking to the future, au Kabucom expects that Secure Internet Access Enterprise will provide security for mobile devices that connect directly to the internet to use cloud services. The product offers threat intelligence–based protection for mobile devices through client software.

au Kabucom is confident that it will be able to create a secure environment that provides users access to an internet that's safe from the latest threats.

> "
> Secure Internet Access Enterprise helps us immediately identify and block new threats that could affect our company, while significantly reducing our operational burden.
>
> **Kenta Nakamura**
> System Risk Management Department, au Kabucom