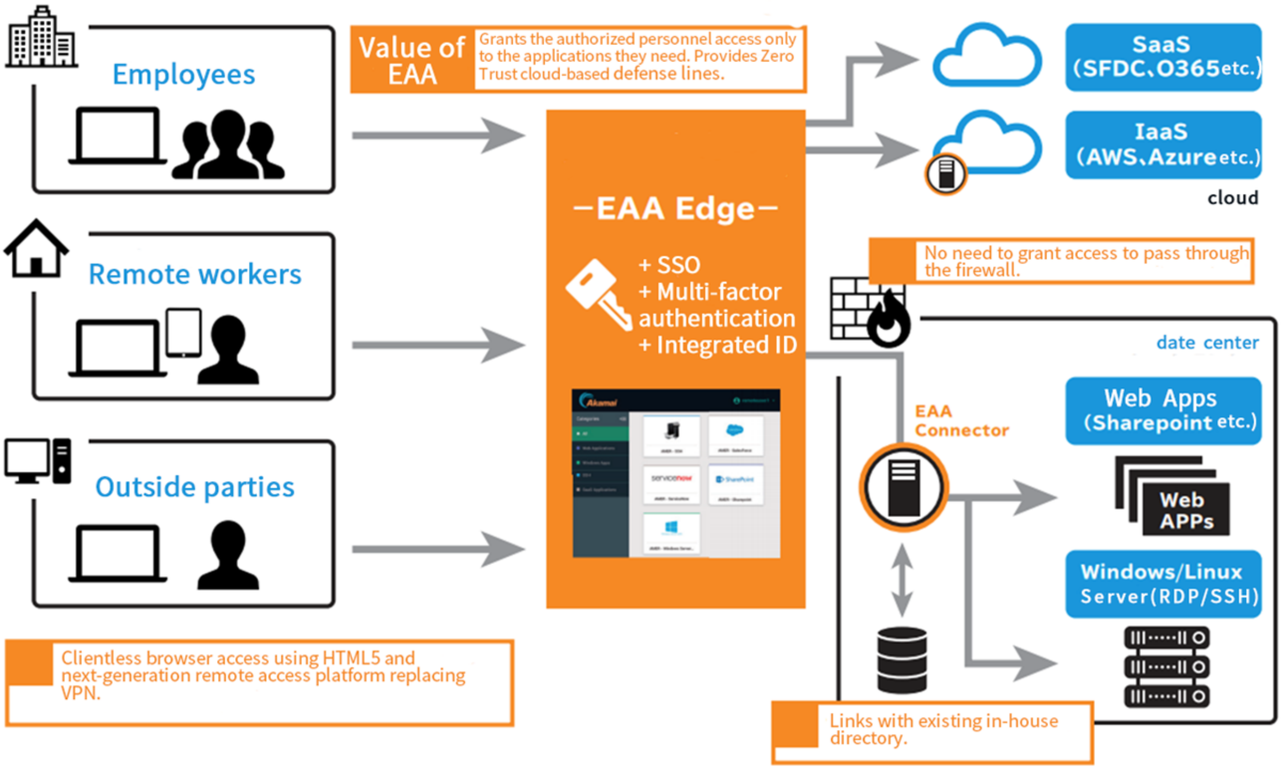
2019.5.15 News Release

Broadmedia Corporation
Broadmedia Technologies

Broadmedia Technologies Launches “Enterprise Application Access,” Akamai’s Next-Generation Access Service to Improve the Efficiency of Multi-Cloud Tasks and Work-Style Reform

Broadmedia Technologies Co., Ltd. (head office: Minato-ku, Tokyo, President: Toshihito Kubo), a subsidiary of Broadmedia Corporation, started providing Enterprise Application Access (hereafter, EAA), a solution of Akamai Technologies GK (head office: Chuo-ku, Tokyo, President & CEO: Osamu Yamano).


Employees
Remote workers
Outside parties
Value of EAA
Grants the authorized personnel access only to the applications they need. Provides Zero Trust cloud-based defense lines.
−EAA Edge−
+ SSO
+ Multi-factor authentication
+ Integrated ID
SaaS (SFDC、O365etc.)
IaaS (AWS、Azureetc.)
cloud
No need to grant access to pass through the firewall.
date center
EAA Connector
Web Apps (Sharepoint etc.)
Web APPs
Windows/Linux Server(RDP/SSH)
Clientless browser access using HTML5 and next-generation remote access platform replacing VPN.
Links with existing in-house directory.

EAA is a cloud service which provides fast and safe connections to enterprises’ applications for their employees via Akamai’s service platform on the Internet. EAA can be easily introduced at low cost and it offers a stable and secure network environment regardless of country and location. Currently, many Japanese enterprises’ information and communication technology (ICT) departments are facing the challenges of managing resources that are widely distributed across multiple cloud services, and increasing numbers of remote workers. With EAA, these challenges can be solved, making enterprises’ ICT operations faster and reducing costs. Moreover, EAA contributes to establishing a Zero Trust security model which greatly reduces the cyber security risks that many enterprises are facing.

[Description of Enterprise Application Access]

Recently, many enterprises have moved their office software and many other internal applications to the cloud. Due to the wide use of Software as a Service (SaaS) and Infrastructure as a Service (IaaS) business models, conventional network configurations and security execution are becoming inefficient. Given this trend, EAA enables access and use of cloud-based internal applications from anywhere in the world, via Akamai's distributed computing platform.

By using EAA, administrators can also centralize control of network connections, including authentication and permissions for enterprise applications. Multi-factor authentication, user directories, single sign-ons, network connections, application access control, server load balancing, and management visibility and control can be all integrated into a unified service.

[Description of the Zero Trust Security Model]

Perimeter-based security is common on internal LANs and intranets in many enterprises, and it refers to "trust but verify" practice of verifying only at the perimeter, e.g. at the Internet entrance. However, in recent years, there are many cases where terminals which had been infected with malware or other threats arising from stolen IDs/passwords have already been inside the company, hindering perimeter-based security.

Confronting this situation, a Zero Trust security model, which is based on the principle of "always verify and never trust," has been attracting a lot of attention, especially in the U.S. Whether inside or outside of the network, Zero Trust authenticates and authorizes every device and user before granting access to applications or data. In addition, Zero Trust incorporates the concept of adaptive security, so that it always analyzes logins and behaviors even after granting access and automatically eliminates devices and users with suspicious activity. By introducing this security model, enterprises' ICTs whose resources are spread on the cloud and mobile devices can be made safer.

End