Case Study

AhnLab

A network Security Strategy for Visibility and Control

Industry
IT

Company Size
Enterprise

Solutions
AhnLab TrusGuard

As company J expanded its cloud-based work environment with increased use of SaaS applications, the limitations of its existing network security architecture became clear. As HTTPS-encrypted traffic and CDN environments became more prevalent, it became harder to identify services and monitor user behavior, making existing policies less effective. As a result, company J needed to establish a network security framework centered on visibility into encrypted traffic and user behavior-based security controls.

Key Results

- Full visibility into traffic
- Implementation of behavior-based security controls
- Application identification and control
- Maintaining a balanced and stable security operations framework

Key Challenges

Company J faced more than a simple performance issue with its security appliances. Its existing security model could no longer adequately address the demands of a changed work environment.

1) SaaS Identification in CDN Environments

Many global SaaS applications rely on CDN infrastructure and share the same IP addresses and domains. As a result, traditional policies based on IP addresses and FQDN could not distinguish business services from non-business services, making it difficult to apply differentiated policies to individual services.

2) Limited Visibility into HTTPS Traffic

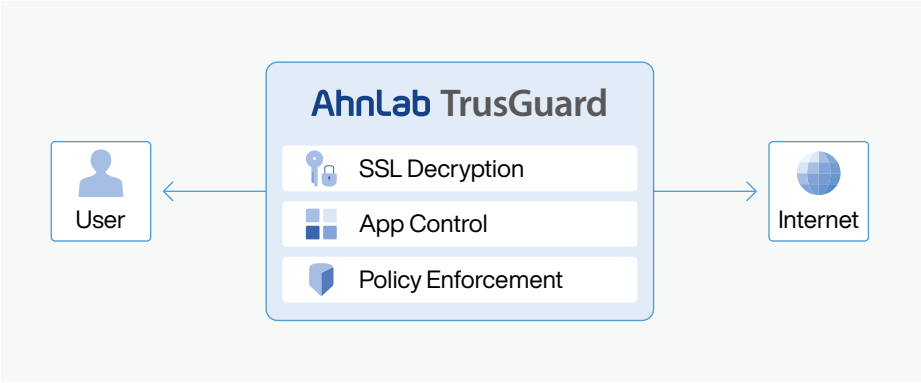
As most business traffic shifted to HTTPS-based collaboration tools, existing security appliances could no longer inspect traffic content or identify user actions. This limited visibility and control over internal data flows, creating security blind spots.

3) Lack of Behavior-Based Policies

Company J's policies were based on IP addresses, ports, and URLs, making it impossible to control specific user actions such as file uploads, email attachments, and external sharing. This significantly limited the organization's ability to respond to data leakage and unauthorized activity.

Solutions

Company J moved beyond the traditional network-centric security model and redesigned its network security architecture around three pillars: visibility, behavior-based control, and operational stability.



1) Securing Visibility Through SSL Inspection

AhnLab TrusGuard decrypts HTTPS traffic and analyzes request information, content, and traffic flows within encrypted sessions. This gives company J visibility into hidden application activity and data flows within SaaS applications.

2) Application-Based Behavior Control

The application control engine analyzes traffic decrypted by TrusGuard and identifies user actions based on URLs, headers, file types, and request methods.
For example, it can identify file uploads, email attachments, and external sharing attempts, then apply policies accordingly. This enables behavior-based security policies that go beyond simple access control.

3) Maintaining Service Stability Through SSL Exception Policies

SSL decryption can cause authentication errors or service disruptions in some applications. TrusGuard addresses this with exception policies that selectively exclude those services from decryption, helping maintain both security and service availability.

Business Outcomes

By deploying TrusGuard, company J was able to transform its security operations.

1) Establishment of a Behavior-Based Control Framework

Company J moved beyond simple network access control and began applying policies based on actual user actions within applications. This reduced the risk of data leakage and strengthened the organization's ability to respond to unauthorized activity.

Operational Flow

1. User accesses an HTTPS-based SaaS service
2. Traffic passes through TrusGuard for SSL session reconstruction
3. Traffic is decrypted for content inspection
4. Content and behavior is analyzed by the application control engine
5. Policies allow, block, or terminate sessions
6. Exception policies let specific services pass without decryption

2) Greater Control over CDN-Based SaaS Environments

By overcoming the limitations of IP and domain-based policies, Company J achieved application-level control even in CDN environments through content-based analysis.

3) Visibility into Encrypted Traffic

By analyzing HTTPS traffic, company J gained visibility into hidden traffic flows and user activities, which significantly improved the accuracy and scope of security monitoring.

4) Balancing Security and Business Continuity

Through SSL exception policies, company J maintained stable operations without service disruption while enforcing strong security policies where needed.

Company J's case shows that simple network access control is no longer enough for enterprise security. In environments centered on SaaS and HTTPS, organizations need a security model that combines visibility with behavior-based control.
Through SSL Inspection, application control, and flexible exception policies, AhnLab TrusGuard addresses these requirements in a practical way and delivers a next-generation security operations model that enables meaningful control even in encrypted environments.

Key Improvements

Before	After
IP-based control	Behavior-based control
Limited visibility into HTTPS traffic	Full traffic visibility
No control over SaaS applications	Granular application control
Service disruptions	Stability through exception policies