Case Study

AhnLab

Strengthening Public-Sector Endpoint Security with Score-Based Management

Industry
Public Institution

Company Size
1,700~2,000 employees

Solutions
AhnLab ESA

Organization D had been applying basic security practices such as antivirus protection, patch management, and account policy enforcement to mitigate endpoint-related risks. However, as attacks abusing legitimate tools and lateral movement increased, configuration gaps such as disabled antivirus protection, missing patches, and improperly configured shared folders became key security concerns.

To address these challenges, the organization adopted AhnLab ESA to manage endpoint security posture through assessment checklists, security scores, and policy-based remediation. This enabled clear visibility across all endpoints, more systematic management of vulnerable devices, and a stronger overall security posture.

Visibility Through Checklist and Score-Based Management

AhnLab ESA evaluates endpoint security posture using approximately 70 checklist items, including antivirus installation, engine updates, patch status, password policies, and screensaver settings. Among them, 10 key items are designated as priority checks, defining the minimum security standards the organization must maintain.

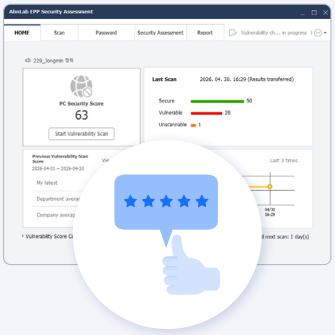
Each endpoint is assigned a security score on a 100-point scale. This score-based approach goes beyond basic configuration checks, providing a consistent and quantitative basis for managing endpoint security across the organization. Administrators can quickly identify vulnerable endpoints and prioritize remediation, while users can easily understand their device status and recognize the actions required to improve security.

Enforcing Continuous Maintenance of Core Security Controls

Attackers are increasingly combining techniques such as Living-off-the-Land Binaries, or LOLBins, with previously proven malware samples rather than developing entirely new malware. These methods are often used to disable antivirus protection or exploit known vulnerabilities. In this environment, maintaining antivirus protection, keeping engines up to date, and applying OS and software patches remain among the most fundamental and critical defense measures.

AhnLab ESA helps maintain a strong endpoint security baseline by continuously assessing and managing these core security controls. It also enables organizations to quickly identify and respond to key risk factors such as missing patches or disabled antivirus protection.

Results



Achieved a 100-point endpoint security score (average 99.9)

Managed security posture with 70+ checklist items

Gained enterprise-wide endpoint security visibility

Closing Security Gaps Through Centralized Management

Settings such as password policies, screensaver configurations, and shared folder permissions often depend on individual users, making them difficult to manage consistently. In environments where centralized management systems such as Active Directory are not fully established, security settings are more likely to be omitted or misconfigured.

AhnLab ESA helps organizations centrally assess and manage these items, reducing security inconsistencies caused by user-defined settings and maintaining a consistent security baseline across the organization.

"Before AhnLab ESA, it was difficult to manually check the security configuration of every endpoint. AhnLab ESA gives us a clear, score-based view of our overall security posture and enables automated assessment and remediation of basic vulnerabilities, helping us maintain endpoint security more reliably."

- Information Security Manager, Organization D

Improving Security Compliance Through Enforced Actions

AhnLab ESA provides a range of policy-based actions based on assessment results, including assessment reminders, user widgets, network blocking, and enforced remediation of non-compliant items.

In particular, the network blocking capability restricts external network access for endpoints that fall below the required security score, while allowing access only to necessary update servers. This enables strong policy enforcement and helps encourage security compliance without requiring direct administrator intervention. As a result, Organization D was able to effectively raise the security level across its endpoint environment.

Balancing Security and Business Availability

Strengthening security often raises concerns about business availability. However, AhnLab ESA is designed to support policy configuration tailored to each organization's environment through a structured process of assessment, scoring, and phased remediation.

Organization D actively applied network blocking policies while minimizing business impact by allowing exceptions for work-related websites. This enabled the organization to improve its security posture while maintaining operational stability.

As a result, most endpoints were able to consistently maintain essential security requirements, including antivirus protection, patch status, and account policies. The organization also significantly improved its ability to respond to attacks involving internal endpoints. In practice, Organization D maintains a monthly endpoint security score of 100 points, with an average score of 99.9 based on agents identified by its EPP solution. Employee compliance with basic security practices has also improved significantly.

"With policy-based enforcement measures such as network blocking, we can strengthen security while minimizing business impact by allowing exceptions for work-related sites. The greatest benefit has been achieving both stronger security and operational stability."

- IT Operations Manager, Organization D

AhnLab ESA (EPP Security Assessment) is a vulnerability assessment and remediation solution that evaluates the security posture of business PCs and strengthens endpoint security through automated remediation.

Operating within AhnLab EPP's integrated management environment, AhnLab ESA delivers a wide range of capabilities spanning vulnerability remediation, malware response, patch management, and personal data protection, enabling effective endpoint hardening across the enterprise.

With a single agent and unified management environment, AhnLab ESA helps reduce operational burden and enables organizations to establish a faster, more consistent endpoint security response framework.