Tenable and AhnLab

Leveraging Network Intelligence to Stop Malware Cold

Key Challenges

The breaching of organizations large and small occurs all too frequently, damaging the confidentiality, availability and integrity of the critical data assets that organizations rely on. Also at risk is hard-earned reputation.

Most organizations focus on the perimeter of their networks, and neglect the intranet – ignoring threats that circumvent the based defenses and inject themselves directly into the core of the infrastructure. Additionally, most organizations are unprepared to deal with advanced malware threats that go undetected by traditional anti-malware technologies. Finally, the complex nature of today's software results in vulnerabilities that appear at an alarming rate, increasing the threat surface that attackers can leverage.

A solution is required that:

- Addresses the network universally rather than just at the edge
- Can deal with advanced malware threats using non-traditional analysis methods
- Can detect and help to manage vulnerabilities that exist within the entire infrastructure on all device types

Tenable Network Security has teamed up with AhnLab to deliver just such a solution.

Solution Overview

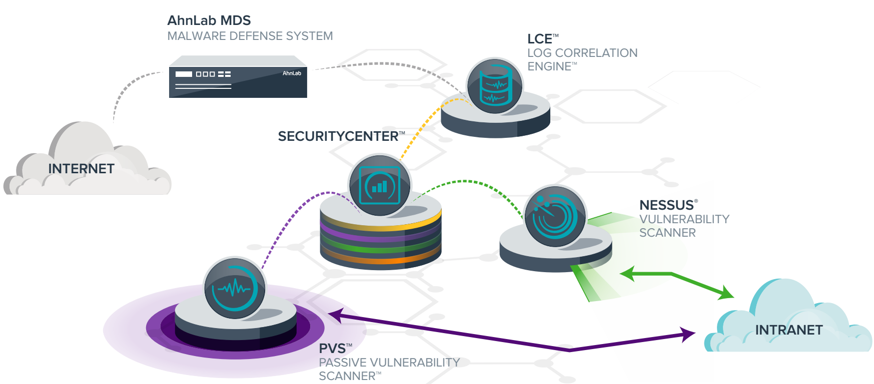
The solution combines Tenable's SecurityCenter Continuous View (SCCV) solution with AhnLab Malware Defense System (MDS) to provide a system that actively blocks malware bearing content, malicious traffic, and outbound C&C traffic. This is done within the AhnLab MDS at the network edge, using a hybrid behavior and signature based approach.

Within the intranet, Tenable's Passive Vulnerability Scanner (PVS) monitors network segments to detect vulnerabilities, C&C traffic, policy violations, and signs of malicious activities.

Tenable Nessus Vulnerability Scanner provides active and credentialed scans of key assets, identifying vulnerabilities, misconfigurations and the presence of active malware that may have been missed by other solutions. With the information provided by Tenable PVS and Nessus devices, vulnerabilities can be identified and mitigated, before an attacker can leverage them.

The AhnLab MDS communicates with Tenable's Log Correlation Engine (LCE) and SCCV devices when an active attack is detected. This enables the active identification of any systems within the intranet that may be vulnerable to the detected attack, allowing administrators to mitigate the vulnerability immediately.

How It Works – Tenable + AhnLab Solution



Solution Components

- Tenable SecurityCenter Continuous View
- Tenable Nessus Vulnerability Scanner
- Tenable Passive Vulnerability Scanner
- Tenable Log Correlation Engine
- AhnLab Malware Defense System

Key Benefits

- Real-time blocking of malicious content and traffic at the network edge using both behavior based and signature based techniques
- Real-time detection of attacks and correlation of attacks with vulnerabilities
- Detection of botnet traffic, malicious traffic, and suspicious traffic from deep inside the intranet to help you find compromised devices early
- Automated scanning for vulnerabilities helps to minimize viable attack surface

The AhnLab MDS is attached to the Internet, actively filtering malware-laden content and filtering active attacks. The AhnLab MDS communicates information about attacks to the LCE, allowing this data to be correlated with active vulnerabilities known to exist within the Intranet. This provides actionable data that allows for the mitigation of active vulnerabilities within the Intranet before they can be leveraged by an attacker.

Tenable PVS continuously monitors the Intranet for vulnerabilities and signs of malicious activities that could be indicative of serious breaches such as an Advanced Persistent Threat. Tenable PVS also discovers unknown assets within the Intranet, such that they can be brought under control and properly managed or removed.

Nessus performs active scans and in-depth credentialed scans allowing for the detection of both vulnerabilities and the presence of active malware. Again, this provides actionable data that can be used to remove vulnerabilities and active threats before they can be leveraged and turned into serious breaches by malicious actors.

Finally, Tenable's flagship Security Center serves as the central management and analysis console, providing countless easy to use dashboards and reports, as well as active alerts for very serious vulnerabilities or events.

Integration Benefits

The benefits of the Tenable + AhnLab joint solution are manifold, combining both active and passive technologies to produce a system that universally detects and blocks security issues.

One of the key benefits is that the solution deals with threats at the perimeter as well as vulnerabilities and threats within the core intranet. This means that malware that enters the network through "out-of-band" paths is detected and caught. This is a very real possibility with today's highly mobile workforce.

For example, at the perimeter, the Ahnlab MDS applies fast malware recognition and remediation with real-time blocking of malicious network traffic and dynamic disruption of active security breaches. Combining the MDS with the Tenable Solution, correlation of actual attacks with vulnerabilities that exist within the infrastructure is possible. The benefit is that system administrators can react quickly to emerging threats and mitigate known vulnerabilities immediately when an attack is detected.

Another benefit of the combined solution is that unusual traffic, indicative of the presence of malware originating within the Intranet, can be identified by Tenable PVS. This means that the sources of this traffic can be tracked and eliminated quickly. Vulnerabilities can be detected early, between scans, providing early warning that mitigation is required. The AhnLab MDS also serves a role here, by blocking the traffic from transiting from the Intranet to the Internet, rendering the malware impotent.

Yet another benefit is that the vulnerabilities that exist within the infrastructure can be detected early in their lifecycle, before an attacker can detect and leverage them. Using Tenable SecurityCenter Continuous View, a regimen of "Continuous Vulnerability Management" can be embraced and deployed. Automated by SecurityCenter, detection of vulnerabilities is performed by the popular Tenable Nessus Vulnerability Scanner. An additional benefit is that Nessus can detect malware as well, so if all other defenses fail infected machines can be identified and remediated.

About Tenable

Tenable Network Security is relied upon by more than 20,000 organizations in over 100 countries, including the entire U.S. Department of Defense and many of the world's largest companies and governments, to stay ahead of emerging vulnerabilities, threats, and compliance-related risks. The award-winning Tenable Nessus and SecurityCenter solutions have received the highest-possible rating in Gartner's MarketScope for Vulnerability Assessment and continue to set the standard for identifying vulnerabilities, preventing attacks, and complying with a multitude of regulatory requirements. For more information about Tenable, please visit www.tenable.com.

About AhnLab

AhnLab creates agile, integrated Internet security solutions for corporate organizations.

Founded in 1995, this global leader in security research and product development delivers comprehensive protection for networks, transactions and essential services. By combining cloud analysis with endpoint and server resources, AhnLab generates best-of-breed threat prevention that scales easily for high-speed networks.

This multidimensional approach combines with exceptional service to create truly global protection against attacks that evade traditional security defenses. That's why more than 25,000 organizations rely on AhnLab's award-winning products and services to make the Internet safe and reliable for their business operations. For more information about AhnLab, please visit www.ahnlab.com.

For More Information

Questions, purchasing, or evaluation:
sales@tenable.com or 410.872.0555, x500
Twitter: @TenableSecurity
YouTube: youtube.com/tenablesecurity
Tenable Blog: blog.tenable.com
Tenable Discussions: discussions.nessus.org
www.tenable.com