Cisco Systems and the Migration from Network Access Control (NAC) to Endpoint Visualization, Access, and Security (EVAS)

By Jon Oltsik, Senior Principal Analyst

October 2014
Contents

Executive Summary .............................................................................................................................................3

A Brief History of Network Access Control ..................................................................................................3
  2010 and Beyond: NAC Transforms into EVAS ..........................................................................................4
  EVAS Functionality .....................................................................................................................................5

EVAS and Threat Management .......................................................................................................................7
  EVAS Use Case: Before an Attack ..................................................................................................................7
  EVAS Use Case: During an Attack ..................................................................................................................8
  EVAS Use Case: After an Attack ....................................................................................................................8

Cisco Systems: An Early EVAS Leader .............................................................................................................9

The Bigger Truth ..............................................................................................................................................10

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.

© 2014 by The Enterprise Strategy Group, Inc. All Rights Reserved.
Executive Summary

Network access controls are nothing new. Many organizations have used technologies like RADIUS servers and 802.1X supplicants for years to allow guest access to corporate LANs or identify corporate devices as they access wireless networks.

While network access controls (NACs) are not a new concept, many security professionals still equate them with a series of NAC technologies that first appeared a decade ago. This common perception is well behind the times because NAC has gone through a profound evolution and has become a much more comprehensive and useful security technology. This white paper concludes:

- **NAC has evolved into a new segment called endpoint visibility, access, and security (EVAS).** The original NAC technology was fairly binary in nature as it granted or denied network access depending upon the configuration and security profile of an endpoint. EVAS expands network access control with granular and contextual access policy enforcement based upon business requirements like user role, location, business process considerations, and risk management. EVAS also extends beyond PCs, providing granular network access to mobile and IoT devices.

- **EVAS has become an enterprise requirement.** IT initiatives like BYOD, cloud computing, and mobile application deployment have made information security policy creation, enforcement, and monitoring much more cumbersome. To address this situation, many CISOs are turning to EVAS to help them manage and secure the complex matrix of connections between users, devices, internal networks, and cloud services. In this way, EVAS can support business, security, and compliance requirements.

- **EVAS can help organizations prevent, detect, and respond to security attacks.** Organizations are using EVAS to harden endpoints and networks before attacks occur. EVAS can also help during an attack by helping security analysts quickly define the scale and scope of an incident. Finally, EVAS provides value after an attack by accelerating the remediation process and fine-tuning security controls.

- **EVAS has become an integration hub.** EVAS systems collect, process, and store a wealth of information about endpoint configurations, connection history, and network activities. Given the value of this data, it is not surprising that EVAS systems share this data with advanced malware detection/prevention technologies, SIEM platforms, MDM, and other networking and security tools.

A Brief History of Network Access Control

Network access controls provide fundamental security protection and have been a part of networking since the early days of Ethernet and IP. Nevertheless, few organizations opted for sophisticated network-layer protection in the past, and relied on Windows authentication as their primary means for controlling who gets on the network. These minimalist network access controls were sufficient in the early 2000s but became inadequate soon after. Why? Users with compromised Windows PCs plugged Ethernet cables into switch ports and then infected corporate networks with an assortment of Internet worms (i.e., SQL Slammer, MS Blaster, Code Red, etc.), causing business interruptions and time-consuming IT fire drills. The multitude of worms combined with poor PC hygiene in the early 2000s led to a constant cycle of network worm infection and costly remediation actions.

Over time, NAC technology and associated vendors proceeded through a number of industry and technology phases (see Table 1).
Table 1. NAC Timeline

<table>
<thead>
<tr>
<th>Timeframe</th>
<th>Primary Driver</th>
<th>Functionality</th>
<th>Limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>2003-2004</td>
<td>Internet worms</td>
<td>Basic device (PC) inspection</td>
<td>Complex technology and a lack of standards.</td>
</tr>
<tr>
<td>2005-2006</td>
<td>Guest access, wireless access</td>
<td>Basic device (PC) inspection, 802.1X authentication</td>
<td>Complex technology, high cost, confusing market landscape, and competing standards that confused the market.</td>
</tr>
<tr>
<td>2007-2008</td>
<td>Device (PC) authentication</td>
<td>802.1X authentication for wired and wireless access networks</td>
<td>Complex technology, multiple 802.1X supplicants, and scalability.</td>
</tr>
<tr>
<td>2008-2010</td>
<td>Device (PC) authentication, guest access, wireless access (802.11N)</td>
<td>802.1X authentication, common wired/wireless policy management</td>
<td>Global recession impacts funding for NAC deployment. Some startups failed or were acquired, causing market confusion. NAC is ineffective at preventing/detecting APTs, diminishing its usefulness.</td>
</tr>
</tbody>
</table>


2010 and Beyond: NAC Transforms into EVAS

NAC technology experienced a renaissance of sorts after 2010, driven by advances in Wi-Fi networking, a decrease in laptop pricing, and the onset of a plethora of alternative devices (i.e., Macintosh PCs, smartphones, tablets, etc.). Organizations needed control over corporate-owned and personally owned devices, and the ability to enforce security policies for mobile and cloud-based access as well as critical corporate or compliance-driven application use. At the same time, new threats like APTs and targeted attacks were regularly circumventing traditional security defenses, driving the need for greater visibility into who and what was on the network at any given time. Finally, IT auditors required more detail about endpoint configuration and status to support evolving governance and compliance needs.

As these changes occurred, NAC came to occupy a valuable piece of real estate on more extended and open networks. NAC was in the right position to inspect devices, monitor activities, and enforce endpoint compliance policies in a growing number of GRC and business use cases such as granular access policy enforcement for specific users, mobile computing devices, IoT sensors/actuators, etc.

Given these changes, NAC has evolved beyond its original limited use case into a new segment called endpoint visibility, access, and security (EVAS). EVAS is defined as:

*Network security technologies that provide policy-based intelligence, enforcement, risk mitigation, and real-time monitoring of all network device access, configuration, and activities for any node attached to an IP network.*

In this way, EVAS gives the security team the right view to be able to visualize its network topology through a cybersecurity lens and then react immediately with proactive controls.

As of 2014, EVAS is no longer a concept but rather an established network security technology in the enterprise. According to ESG research, 40% of enterprise organizations use EVAS extensively while another 44% say they use EVAS somewhat. When asked to identify the factors driving greater use of network access controls overall, enterprise security professionals point to EVAS drivers such as addressing IT risk, enabling mobile users and devices, and aligning network security with the increasing use of Wi-Fi for network access (see Figure 1).¹

EVAS Functionality

While NAC was used to inspect a finite number of endpoint properties, EVAS is designed for more comprehensive visibility with new levels of context and dynamic control such as (see Table 2):

- **Endpoint profiling.** EVAS is designed to monitor the status of all endpoints (i.e., PCs, servers, printers, mobile devices, Internet of Things [IoT] sensors and actuators, etc.) on the network. In fact, leading EVAS solutions capture and store this information for future use in compliance audits, security investigations, and policy assessments. EVAS systems regularly collect, process, and store endpoint-centric information like system type, configuration, applications installed, patch levels, etc.

- **Granular policy enforcement.** While NAC was used to grant or deny network access, EVAS can be configured for more granular access policies based upon identity attributes like user role, device type, network location, time of day, etc. As an example, EVAS can provide the CFO access to sensitive M&A
documents from her PC connected to the corporate LAN but deny access when she tries to access the same content using her iPad on a public network.

- **Integration.** Large organizations want integrated intelligence, policy management, and context and control to improve risk management, incident detection/responses, and security automation. EVAS is architected for these imperatives because it is designed for continuous monitoring, endpoint profiling, data capture, and interoperability with SIEM, firewall/VPN, identity management, vulnerability scanning, trouble ticketing, IT-GRC, MDM, web security gateways, etc.

**Table 2. NAC Versus EVAS**

<table>
<thead>
<tr>
<th>Function</th>
<th>NAC</th>
<th>EVAS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint profiling</td>
<td>Basic inspection of configuration and presence of endpoint security software. PC-only support. No data collection.</td>
<td>Advanced inspection of endpoint software and hardware configuration. Support for PCs, mobile devices, IoT, etc. Extensive data collection and processing.</td>
</tr>
<tr>
<td>Policy enforcement</td>
<td>Grant or deny network access based upon PC configuration and security status. Access policies for information security only.</td>
<td>Granular access controls for network access based upon device, user, network location, time of day, data sensitivity, etc. Access policies for business, security, compliance, etc.</td>
</tr>
<tr>
<td>Integration</td>
<td>Some integration between NAC and networking devices like Ethernet switches and wireless access points (APs).</td>
<td>Extensive integration with SIEM, vulnerability scanning, MDM, advanced malware detection/prevention technologies, IoT/operations technology, etc.</td>
</tr>
</tbody>
</table>

By offering this functionality, EVAS acts as a logical evolution, represents what NAC was meant to be, and plays a vital role in a number of business, information security, and IT functions. For example, continuous monitoring can be used for risk management and mitigation by the security and IT operations team. Endpoint profiling can help security, operations, and help desk personnel identify risky devices, restrict access to unauthorized resources, and prioritize remediation activities. Finally, business, IT, and security managers can work collectively to create security policies that enable new mobile computing-based business processes without adding undue IT risk (see Figure 2).
EVAS and Threat Management

As part of its maturation, EVAS gained increasing intelligence about endpoints, networks, and IT assets. This intelligence has become essential for creating, enforcing, and monitoring security policies for enterprises, helping CISOs balance day-to-day business operations with IT risk mitigation.

As an example, EVAS has become a valuable technology that can help enterprise organizations improve threat prevention, detection, and response. EVAS can mitigate risk in three phases (see Table 2):

1. Before an attack, to decrease the threat surface.
2. During an attack, for threat detection and attack mitigation.
3. After an attack, for further risk mitigation and remediation.

EVAS Use Case: Before an Attack

The EVAS threat prevention role before an attack provides added value over legacy NAC utilization. CISOs can use various EVAS capabilities to decrease the overall network and endpoint attack surface by:

- **Identifying risky assets.** EVAS is responsible for monitoring all assets connected to the network at any time. This can help organizations identify risky and potentially vulnerable assets at a moment’s notice. Identifying non-compliant users, devices, OS, applications, etc., and correlating that information with third-party vulnerability assessment tools allows for a more rapid IT response. For example, when a critical vulnerability is identified, the security operations team can immediately identify all systems with software configurations representing the highest risks (i.e., non-compliant, no antivirus updates, etc.).

- **Improving risk mitigation.** With continuous monitoring and a database of assets and activities, the security team can use EVAS for gathering actionable intelligence. This can help them improve workflows, streamline operations, and prioritize remediation activity to remain in lockstep with constant changes to IT risk.
• **Enforcing granular network access policies.** As previously described, EVAS provides contextual information for granular policy creation and enforcement. Once again, this can help decrease the attack surface by limiting access to sensitive content, assets, or network segments.

**EVAS Use Case: During an Attack**

When anomalous or suspicious behavior is detected, EVAS can help security analysts determine and limit the scope of an attack. This is accomplished by:

• **Integrating into advanced network-based threat defense systems.** Network-based threat defense systems can analyze network behaviors and malicious activity, but they lack contextual knowledge about the presence or state of actual endpoints on the network. EVAS can fill this gap with its robust database on network endpoints. By sharing contextual knowledge with the threat defense systems, when malicious activity is detected, attack data can be correlated with endpoint connections, configurations, and behavior patterns over time. This can help organizations accelerate their detection and response processes.

• **Blocking “kill chain” tactics emanating from compromised systems.** Attacks tend to follow a “kill chain” where a compromised system reaches out to other network assets to steal credentials, escalate privileges, and exfiltrate valuable data. EVAS granular access controls can help mitigate this risk by blocking kill chain activities as they occur. For example, granular access policies may preclude a system from connecting to sensitive network segments or systems housing sensitive data. Beyond blocking these malicious activities, EVAS can also send the data on to SIEM systems for further analysis or to generate immediate security alerts.

• **Taking remediation actions to limit the scope of an attack.** When an attack is discovered, the security operations team can use EVAS policies to minimize the potential impact. When a system exhibits anomalous behavior, it can be removed from the network, quarantined, or connected to a remediation VLAN or context-based segmentation. EVAS can also integrate with PCAP tools. Once a capture is taken and the additional context is provided as part of this PCAP, an administrator could decide to mirror network traffic coming from the suspect system to a honeypot/honeynet for further forensic analysis.

**EVAS Use Case: After an Attack**

After an attack is detected, EVAS can be used for:

• **Assessing endpoint profiles for vulnerabilities.** Information from the EVAS database can be shared with vulnerability analysis tools to better and more quickly discover compromised systems. Vulnerability analysis tools can then assign a “high-priority” trouble ticket classification so that IT operations can prioritize a fix.

• **Remediating compromised systems.** Many EVAS systems are integrated with MDM, patch management, and endpoint security systems. Once vulnerable systems are identified, EVAS can act as part of the fabric to automate fixes and monitor progress.

• **Fine-tuning access policies and security controls.** Based upon attack analysis or threat intelligence, EVAS can be used to fine-tune access policies for blocking attack vectors or preventing the spread of attacks. For example, EVAS can work with networking and security equipment to segment application traffic or add new firewall rules or IPS signatures.
Table 3. EVAS Use Case Before, During, and After an Attack

<table>
<thead>
<tr>
<th>Time</th>
<th>EVAS Use Case</th>
<th>Benefits</th>
</tr>
</thead>
</table>
| Before attack | • Identify risky assets  
• Improve risk mitigation  
• Enforce granular network access policies | Decrease attack surface and fine-tune security controls based upon new threat intelligence. Reduce the number of unknown/unmanaged devices connecting to the network. |
| During attack | • Integrate with advanced malware detection  
• Block “kill chain” tactics  
• Enforce immediate remediation actions | Accelerate incident detection and minimize the impact of an attack.                                   |
| After attack  | • Assess endpoints for vulnerabilities  
• RemEDIATE compromised systems  
• Fine-tune security controls | Use attack tactics and forensic knowledge to harden the network and endpoints.                        |


Cisco Systems: An Early EVAS Leader

EVAS is a broad and growing security segment made up of lots of vendors and technologies. While some EVAS tools may be considered best-of-breed, many CISOs want integrated enterprise solutions rather than an army of disparate EVAS point tools.

Cisco Systems is one of few vendors offering an enterprise-class EVAS solution that can actually meet CIO requirements for an integrated EVAS architecture. Cisco’s EVAS is actually made up of a number of products that can interoperate to form a comprehensive EVAS architecture. This includes:

- **Cisco Identity Services Engine (ISE).** ISE is used as the network access nexus for consistent security across wired networks, wireless networks, and VPNs. Security and network operations teams can use ISE to create, enforce, and monitor granular business-centric network access policies. ISE provides visibility, context, and control across the entire attack continuum.

- **Cisco AnyConnect.** AnyConnect is used to enable secure network access between a variety of endpoints (PCs, smartphones, tablets, etc.) and network-based assets (i.e., per application VPN access). AnyConnect can be used to scan devices for proper hygiene and enforce corporate endpoint configuration policies before granting network access. AnyConnect also provides device authentication, a critical component of granular access policy enforcement. Finally, AnyConnect monitors network traffic to block malware, inappropriate sites, and content at the corporate gateway. This improves security and network bandwidth utilization.

- **Cisco TrustSec.** While enterprises want to create and enforce granular network access policies, it is often difficult to align business process needs with static network segmentation technologies. Cisco TrustSec was designed to alleviate this problem. In essence, TrustSec transforms the network into a contextual firewall by categorizing user roles, tagging devices and assets, and then enforcing ACLs based upon business and risk management considerations.

- **Cisco Ecosystem Partner Integrations Powered by pxGrid.** Cisco has developed a program to integrate with technology partners to provide better security and improved network forensics capabilities. Cisco has also recently developed Cisco Platform Exchange Grid (pxGrid) technology, which introduces a new way to share contextual data about users, devices, connections, etc. to improve visibility for network and security administrators, but also to provide remediation of threats by dynamically changing access policies. To
maximize its value, Cisco is working with several partners to provide enterprise organizations with additional functionality such as:

1. Faster remediation of threats via work with SIEM vendors.
2. Extension of access policy and posture compliance to mobile devices with MDM vendors.
3. Enhanced single sign-on (SSO) on mobile device for secure access to sensitive data.
4. Internet of Things (IoT) security for the industrial sector and operations technology (OT).
5. Simplified network troubleshooting and forensics.

When all products are deployed in concert, the Cisco EVAS architecture can be used in the before, during, and after attack use cases, helping enterprise organizations lower risk, accelerate incident detection/response, and streamline security operations.

The Bigger Truth

To this day, security professionals equate NAC with its original concepts and form factor from over ten years ago. This perception is misguided and ignores the fact that NAC technology maturity has led to a new category—EVAS. EVAS extends security protection, profiles endpoints for continuous monitoring, provides for granular access controls, and aligns cybersecurity with business processes.

Aside from network access alone, EVAS can also help organizations prevent, detect, and respond to attacks in a timely manner. In fact, EVAS can be used to help organizations reduce the endpoint and network attack surface, define the scale and scope of an attack, remediate problem resolution processes, and further harden the network after an attack has occurred. EVAS also integrates with other security technologies to share data and automate remediation activities.

As organizations embrace cloud computing and mobile applications, EVAS is becoming increasingly important because it can balance business enablement, end-user productivity, and strong security. As CISOs recognize this and seek the best EVAS solutions, they would be well served by contacting Cisco and discussing how its enterprise-class EVAS architecture can help them discover and control rogue devices, reduce the attack surface for threats, and improve downstream security operations while enhancing productivity for authorized users by enabling and securing access to critical business resources.