EVAS, la evolución de NAC para afrontar los nuevos retos de seguridad en T.I.

Henrry Oswaldo Rodríguez Rodríguez
Universidad Piloto de Colombia
Especialización de Seguridad Informática

***Resumen*—En el año 2004 Cisco introdujo una nueva tecnología llamada Control de Admisión a la Red, ahora más comúnmente conocida como Control de Acceso a la Red o NAC (Network Access Control). En su momento NAC fue una solución a la ola de gusanos de Internet que podían infectar un PC, el cual registrándose en una red corporativa podía subsecuentemente infectar toda la red. Pero las cosas han cambiado y NAC ya no se trata solo de control de acceso, se trata de proveer visibilidad en los usuarios finales y seguridad contextual, por esto NAC evoluciona a EVAS (Endpoint Visibility, Access and Security), una plataforma que habilita seguridad contextual, y alimenta información a otras plataformas mientras hace cumplir las políticas que esas plataformas dictan; las organizaciones quieren una manera dinámica, rápida y más eficaz para identificar los sistemas, anticiparse a las exposiciones y contener amenazas.**

***Abstract*— In 2004, Cisco introduced a new technology called Admission Control Network, now more commonly known as Access Control Network or NAC (Network Access Control). NAC at the time was a solution to the wave of Internet worms that could infect a PC, which log on a corporate network could subsequently infect the entire network. But things have changed and NAC it's no longer just about access control, it's about to provide endpoint visibility and security context. So, NAC evolves to EVAS (Endpoint Visibility, Access and Security), a platform that enables contextual security, feeding information to other security platforms while enforcing the policies those platforms dictate; Organizations want a dynamic, fast and more effective way to identify systems, preempt exposures and contain threats**

***Index Terms*—Aplicación de Políticas, Automatización de Seguridad, BYOD (Bring Your Own Device), EVAS (Enpoint Visibility, Access and Security), Monitoreo Continuo, Movilidad, NAC (Network Access Control), Seguridad Contextual.**

I. Introducción

LASempresas día a día están aprovechando las nuevas tecnologías en virtualización, movilidad, conexiones inalámbricas y computación en la nube para mejorar su productividad y fortalecer el core de negocio. Estas tecnologías potencian la prestación de servicios, pero pueden incrementar el riesgo operacional y en seguridad ¿Por qué? El acceso a recursos corporativos y datos, así como el tipo de dispositivos y aplicaciones, se ha vuelto más diverso y dinámico. Sucesivamente, los perímetros y límites son cada vez máspermeables e imprecisos, lo cual afecta la aplicación de políticas de seguridad de TI, y a su vez la administración del riesgo. Según el reporte de Gartner de Octubre de 2011, en la mayoría de compañías, solo se tiene control sobre el 80% de los dispositivos conectados a la red, por lo tanto queda un porcentaje considerable de dispositivos no administrados, desprotegidos y desconocidos [1].

Debido a esto han surgido en el mercado tecnologías como MDM (Mobile Device Management) y NAC (Network Access Control), con el fin de tener control y gobernabilidad sobre todos los dispositivos conectados a la red.Las primeras soluciones de NAC ejecutaban chequeos de salud en los dispositivos de usuarios para asegurase que estuvieran libres de infecciones y protegidos por un software antivirus antes de permitirles acceso a la red, posteriormente implementaron chequeos para actualizaciones y parches además de verificar una apropiada configuración.

Ahora las soluciones NAC se están convirtiendo en plataformas EVAS, con el fin de satisfacer las demandas de las compañías para una mejor seguridad contextual, ya queeste tipo de plataformas se pueden integrar con otros sistemas de seguridad, permitiendo tener visibilidad de un grupo de dispositivos más amplio que las tradicionales soluciones NAC, la cuales solo se enfocaban en PC's.

II. ¿Qué es NAC y cómo funciona?

El concepto original de NAC, que data de 2004, era el de evitar la propagación de malware evitando a computadores infectados el acceso a la red a través de aplicación de políticas de autorización y autenticación. Las primeras implementaciones de NAC se basaron en 802.1X, el estándar IEEE para autenticar las comunicaciones entre la red y los dispositivos administrados para ofrecer NAC basadoen puertos. Publicado por primera vez en 2001, 802.1X especifica un medio para validar un dispositivo que se conecta a través de un software cliente (normalmente referido como un agente o solicitante) con un autenticador, típicamente un switch con capacidad para 802.1X. La sesión consta de un dispositivo que solicita acceso a la red, y el switch, que a su vez reenvía la solicitud a un servidor de autenticación. Dependiendo de los resultados del proceso de validación, la conexión al respectivo puerto de red ya se producción o de acceso a invitados, será

H. O. Rodriguez, Ingeniero Electrónico de la Escuela Colombiana de Ingeniería y aspirante a Especialista en Seguridad Informática de la Universidad Piloto de Colombia, Bogota – Colombia. Actualmente es Analista Master de Infraestructura Tecnológica en Servientrega S.A. (e-mail: horodriguez85@gmail.com)

concedida o denegada [2].

Fundamentalmente, NAC ofrece un mecanismo para la aplicación de políticas consistentes que comienza con el descubrimiento en tiempo real, la autenticación y clasificación de los dispositivos que intentan obtener acceso y los que ya están en la red. Un motor de reglas NAC puede basar sus decisiones en políticas predefinidas relacionadas con el usuario, ubicación, hora, tipo de dispositivo, configuración y atributos de seguridad. Con este nivel de automatización de la política, NAC es útil para identificar fácilmente cuando dispositivos nuevos y desconocidos o delincuentes están intentando acceder. El uso de la inspección de dispositivos basado en roles, la política granular sobre la configuración de dispositivos y el cumplimiento de la seguridad, se pueden aplicar tanto a equipos conocidos como desconocidos que intenten acceder a la red. En la Figura 1 se puede observar el diagrama de un sistema típico de NAC [3].

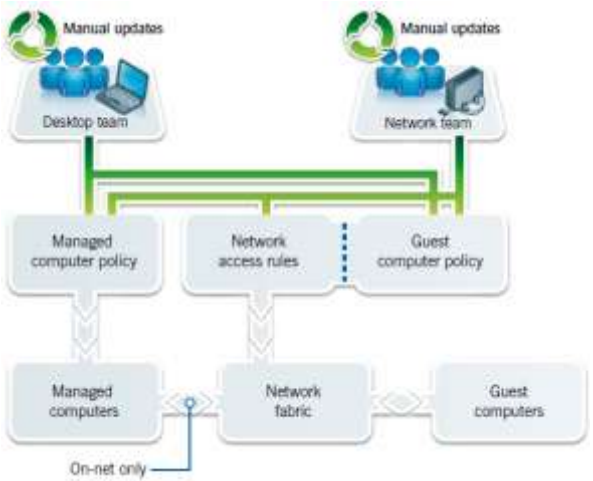

Figura 1. Diagrama de un sistema NAC básico. Se puede observar Cómointeractúan los módulos en un sistema NAC. Tomado del documento "NAC 2.0: A new model for a more secure future" de Sophos Plc.

En la práctica, esto significa que se requiere que cada dispositivo se identifique cuando se conecta, y en cada caso será examinado por su cumplimiento de las políticas de seguridad. En una red típica, hay dispositivos que:

- No pueden proporcionar una identidad en vigor y quedan completamente excluidos de la red (o, alternativamente, podría haber acceso restringido a Internet, y nada más)
- Se autentican con éxito, pero no pasan la prueba de adhesión a la política y se les da acceso a un proceso de remediación, y nada más.
- Se autentican con éxito y se consideran que cumplen con la política y se les da acceso a los recursos de red que corresponden a su identidad.

En la Figura 2 se puede observar el diagrama de flujo de las acciones mencionadas anteriormente [4]:

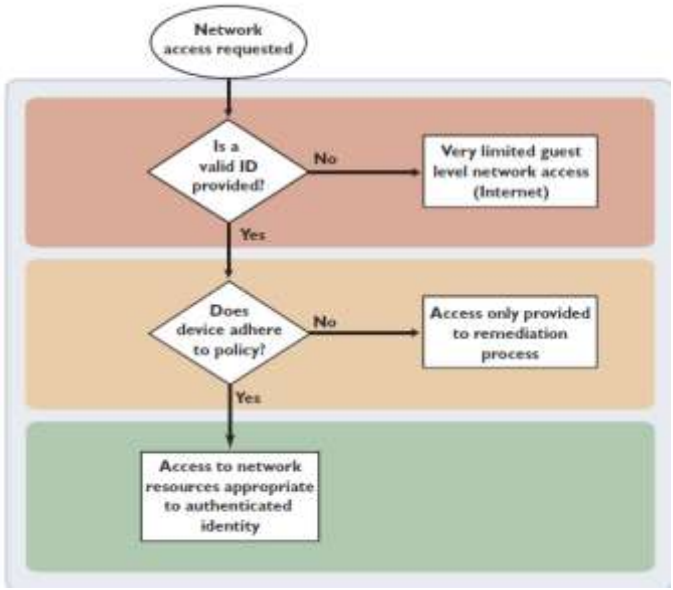

Figura 2. Diagrama de flujo de petición de acceso a la red. Se puede observar todo el flujo que tiene un dispositivo que se conecta a la red. Tomado del documento "Allied Telesis provides advanced edge security for enterprise networks" elaborado por Allied Telesis Inc. Disponible: http://alliedtelesis.com.br/media/pdf/Advanced_Edge_Security_with_NAC_revA.pdf

Como resultado de las implementaciones de NAC, las compañías lograron tener una herramienta capaz de manejar un amplio rango de problemas de seguridad como:

- Proveer acceso a la red a invitados.
- Controlar donde pueden estar conectados empleados y contratistas en la red.
- Aplicar políticas de seguridad (antivirus, niveles de parchado, aplicaciones y procesos).
- Generar reportes de auditoria acerca de cumplimiento sobre los dispositivos de usuario.
- Administrar almacenamiento portable.
- Prevenir actividades maliciosas.

III. LOS PRIMEROS PASOS HACIA LA EVOLUCIÓN DE NAC

Las soluciones NAC evolucionaron para satisfacer los enormes cambios en el panorama de IT que han tenido lugar desde 2003. Estos cambios, los cuales se resumen en la Figura 3, son los siguientes:

A. El crecimiento explosivo de la complejidad de la red de conectividad de múltiples tecnologías, múltiples tipos de usuarios y múltiples ubicaciones.
B. El aumento de la diversificación y sofisticación de los dispositivos de usuario final.
C. El aumento (y mutación) del ambiente de amenazas.

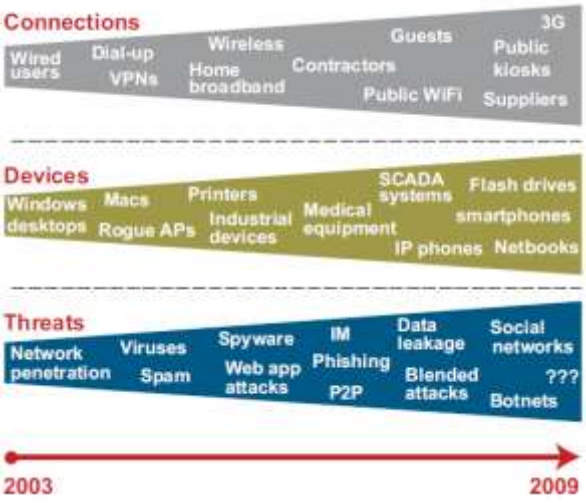

Figura 3. Factores involucrados en la evolución de NAC. En el grafico se observan los distintos cambios en tecnología y factores que han conllevado la evolución de NAC entre 2003 y 2009. Tomado del artículo "The Evolution of Network Access Control", por Infonetics Research, Inc. Disponible: http://www.infonetics.com/whitepapers/2009-Infonetics-Research-The-Evolution-of-Network-Access-Control-FINAL-112309.pdf

Se comenzó a ver la necesidad de que las redes debían estar abiertas, y en muchas de ellas incluir dispositivos invisibles, no administrados, y sin protección, como los teléfonos inteligentes, lo que creo una importante demanda de soluciones de seguridad como NAC.

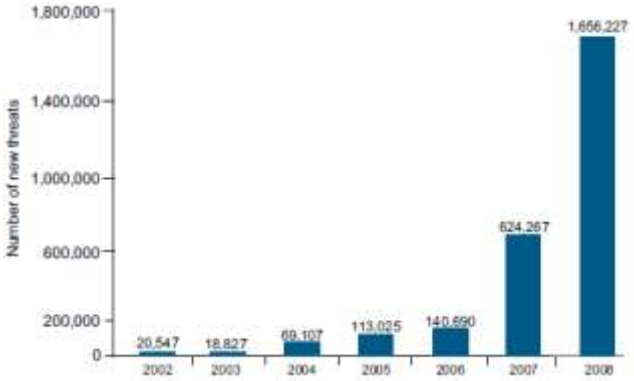

Figura 4. Detección de nuevos códigos maliciosos entre 2002 y 2008.Tomado del artículo "The Evolution of Network Access Control", por Infonetics Research, Inc. Disponible: http://www.infonetics.com/whitepapers/2009-Infonetics-Research-The-Evolution-of-Network-Access-Control-FINAL-112309.pdf

La Figura 4 muestra el número de amenazas de códigos maliciosos detectados desde 2003 hasta 2008, el número de amenazas creció 60% entre 2006 y 2007; el 60% de todas las amenazas detectadas fueron vistas (y posiblemente creadas) en 2008. La rápida expansión de las amenazas fue resultado de la transformación que el hacking tuvo desde el cambio de milenio. El hacking ya no era un hobby, fue convirtiéndose en un gran negocio. Teniendo en cuenta el ritmo acelerado del desarrollo de amenazas, las soluciones NAC tuvieron que evolucionar para mantenerse al día. Para hacer frente a amenazas de código malicioso, las soluciones NAC tuvieron que ampliar la cantidad de datos que se extraían sobre el software que se ejecutaba en un dispositivo determinado. Otros vectores de amenazas condujeron evoluciones paralelas.

Proveedores de NAC visionarios se han dedicado a la evolución de la tecnología NAC en respuesta a las amenazas mencionadas anteriormente. Elpunto clave de la evolución es la capacidad de reunir una gran cantidad de conocimientos acerca de los usuarios, dispositivos, redes, software y periféricos, y almacenar esos datos en perfiles. Estos datos son útiles, accionables y auditables, y los perfiles organizan los datos de modo que las políticas de seguridad se pueden aplicar a individuos y a grupos [5].

IV. NAC SE TRANSFORMA EN EVAS

A principios del 2008 el entusiasmo de la industria alrededor de NAC disminuyó y el mercado que estaba consolidado comenzó a venirse cuesta abajo. A pesar de esto los fabricantes restantes, continuaron innovando con el fin de que las funciones de NAC se alinearan con las necesidades de las compañías. Los proveedores de NAC comenzaron a tomar ventaja de los avances en hardware y software, virtualización, y estándares de seguridad para lograr expandir el impacto de los sistemas NAC.

A medida que los restantes fabricantes de NAC mejoraron sus productos, los requerimientos de las compañíastambién se inclinaron a favor de NAC. Las primeras soluciones de NAC se centraron en el control de acceso para computadores Windows, pero las grandes compañías fueron abriendo sus redes a una diversidad de dispositivos alternativos (Macintosh, smartphones, tabletas, etc.) para el 2010. Este cambio dio lugar a un uso más generalizado de la red inalámbrica, que a su vez aumentó la necesidad de una mayor aplicación de políticas de acceso granular. Las compañías necesitaban el control tanto de los dispositivos de uso personal como los corporativos, y la aplicación de políticas de seguridad para dispositivos móviles y el acceso a la nubeasí como el uso de las aplicaciones. Al mismo tiempo fueron surgiendo nuevas amenazas que podían sobrepasar la seguridad tradicional, lo cual genero la necesidad de tener una mayor visibilidad de quién o qué estaba conectado a la red en cualquier momento. Por último, los auditores de TI necesitaban más detalles sobre la configuración de los dispositivos y su estado para apoyar la evolución de las necesidades de gobierno y cumplimiento de las políticas de seguridad.

NAC comenzó a ocupar un lugar muy importante en compañías con grandes redes y redes abiertas. NAC estaba en la posición correcta para inspeccionar dispositivos, monitorear actividades y hacer cumplir las políticas de seguridad a todos estos dispositivos. La combinación de las nuevas necesidades de las empresas y la investigación y el desarrollo de proveedores, expandió en gran medida el alcance y el papel de la tecnología NAC. NAC ha entrado a su segunda década, y su

evolución va másallá de su función original de control de acceso a la red, y ahora tiene muchas más funciones. De acuerdo a esto se puede considerar que NAC está evolucionando más allá de su mercado original, el cual es limitado, a un nuevo mercado dentro de un nuevo segmento llamado EVAS (Endpoint Visibiliti, Access and Security).

ESG (Enterprise Strategy Group) define EVAS como: Tecnologías de seguridad en redes que proveen inteligencia basada en políticas, aplicación de las mismas, mitigación de los dispositivos que acceden a la red, configuración y actividades para cualquier nodo conectado a una red IP [6].

V. LAS NOVEDADES QUE OFRECE EVAS

EVAS se construye sobre las bases de NAC y ofrece mejoras como las siguientes:

A. Mayor cubrimiento y visibilidad de dispositivos

NAC fue diseñado originalmente con la noción de que todo era Windows, pero ahora las compañías soportan toda clase de dispositivos. Esto le da a EVAS la capacidad de crear y aplicar políticas corporativas sobre dispositivos tales como Máquinas virtuales, smartphones, tabletas, impresoras, teléfonos IP, equipos médicos, e incluso dispositivos no administrados como la tableta de un empelado. Además se ha determinado quedispositivos como impresoras, sistemas SCADA y sensores pueden ser objetivos interesantes para ataques sofisticados. EVAS está construido desde cero para soportar todo tipo de dispositivos en la red.

B. Múltiples factores de forma para sistemas EVAS

Infraestructuras de TI modernas están basadas en dispositivos físicos, máquinas virtuales y recursos en la nube. EVAS se adapta a esto y puede ser implementada como un dispositivo físico, virtual o incluso en la nube.

C. Un enfoque sobre la integración

Hoy en día las compañías desean tener arquitecturas de seguridad integrales; quieren integrar inteligencia, administración de políticas y control centralizado para mejorar la administración del riesgo, la detección y respuesta a incidentes y automatización de la seguridad. EVAS está diseñado para estas necesidades, con una interoperabilidad estrecha con firewalls, administradores de identidad, escáneres de vulnerabilidades, MDM, etc.

EVAS además simplifica la implementación de NAC, consolidando una compleja infraestructura de dispositivos en un solo equipo con administración unificada. Finalmente EVAS es un moderno superconjunto de NAC construido para satisfacer todos los requerimientos de la seguridad de la información, operaciones de red y administración de dispositivos en una empresa, así como muchas otras tecnologías de TI. En la Figura 5 se observa cómo se vislumbra el funcionamiento de EVAS y su interacción con tecnologías de IT y seguridad.

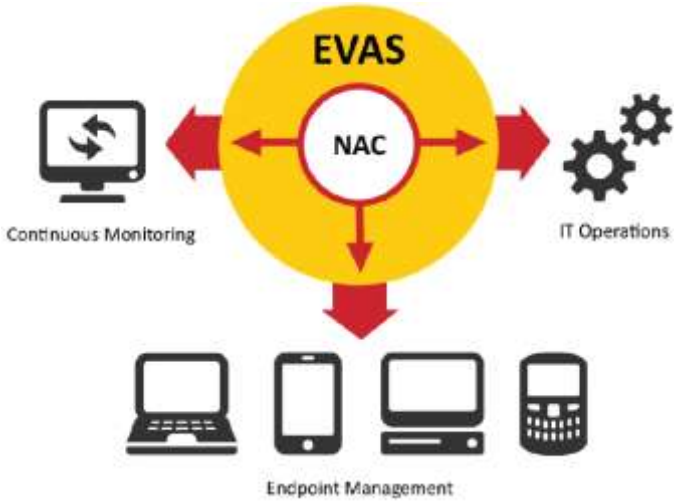

Figura 5. EVAS es un superconjunto de NAC que interopera con otras tecnologías de IT y Seguridad. Tomada del reporte "The Endpoint Visibility, Access and Security, (EVAS) Market: The Evolution of Network Access Control (NAC)". De Enterprice Strategy Group, Inc.

VI. EVAS SE VUELVE FUNDAMENTAL

Justo como los IDS abrieron el camino para que los Firewalls se transformaran en WAF (Web Application Firewall) y NGFW (Next Generation Firewall), NAC ya ha evolucionado hacia EVAS, y se convertirá en un tema fundamental para las tecnologías de seguridad en IT, generado por cinco puntos fundamentales:

A. *Movilidad de usuarios y BYOD*

Se espera que el número de empresas que prohíben los dispositivos BYOD y que requieran el uso de dispositivos entregados por la compañía se reduzca del 62 por ciento actual al 22 por ciento en cinco años.

B. *Una transición hacia el monitoreo y mitigación continua.*

Muchas organizaciones hoy en día carecen de visibilidad y control de los dispositivos de usuario final y las aplicaciones conectadas a la red y están migrando a herramientas para el control y la mitigación continua.

C. *La imperiosa necesidad por automatizar operaciones de seguridad*

Presión, presupuesto y disponibilidad de profesionales calificados de TI, así como la dinámica y el avance natural de las amenazas sobre las redes, crean necesidades urgentes para una mayor automatización que por supuesto ofrece la tecnología EVAS.

D. *El impulso hacia políticas de "seguridad contextual" y su aplicación.*

EVAS permite un uso más eficaz de otras tecnologías de seguridad al proporcionar el conocimiento en tiempo real acerca de quién, qué, dónde, por qué y cuando un usuario o dispositivo está conectado en la red.

E. *Software como servicio como un elemento básico de TI*

Las implementaciones de SaaS (Software as a Service) crecerán en los siguientes años y así mismo se implementaran nuevos tipos de aplicaciones. A medida que aumente el despliegue de SaaS, EVAS será parte de una infraestructura de aplicación de políticas y control de aplicaciones, y siendo así las implementaciones de EVAS basadas en computación en la nube tendrán fuerza en el mercado [7].

VII. EL FUTURO DE EVAS EN EL MERCADO

La funcionalidad de EVAS, la integración de seguridad TI y los nuevos requerimientos en seguridad de la información, ya están teniendo un impacto sobre los ingresos de la industria. En este punto el estancamiento del mercado de NAC es cosa del pasado, mientras que las ventas de EVAS han tomado fuerza. Por otra parte, las adquisiciones de EVAS, se han apalancado a través de proyectos como BYOD, cumplimiento de políticas en dispositivos, monitoreo continuo y análisis de seguridad. En la Figura 6 se observa la estimación de crecimiento en ventas del mercado EVAS entre 2013 y 2017 realizado por ESG, el cual indica que para el 2017 se alcanzaran ventas superiores a los 700 millones de dólares.

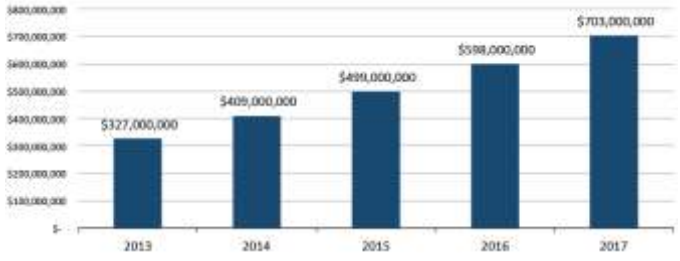

Figura 6. Estimación del crecimiento en ventas del mercado EVAS entre 2013 y 2017. Tomada del reporte "The Endpoint Visibility, Access and Security, (EVAS) Market: The Evolution of Network Access Control (NAC)". De Enterprice Strategy Group, Inc.

Como parte de la renovación del mercado EVAS, la competencia crecerá nuevamente, lo que lleva a nuevas adquisiciones, funciones adicionales e integración de módulos, ofertas de paquetes y la baja de los precios de un mercado maduro. No obstante, el crecimiento continuará, aunque a un ritmo decreciente en el tiempo. La Figura 7 muestra cómo será el comportamiento del mercado hasta 2017 y los factores que promoverán dicho crecimiento [6].

	Growth Rate	Drivers	Market Dynamics
2013	NA	Mobile/BYOD, Early continuous monitoring	Market share leaders include Bradford Networks, Cisco, Forescout, and Juniper
2014	25%	Mobile/BYOD, continuous monitoring, contextual security policies; integration bundles/ large enterprise adoption	Competition from MDM vendors and wired/wireless integration; Aruba gains share with WiFi sales; MDM vendors enhance mobile gateways providing some EVAS functionality
2015	22%	New cybersecurity framework, continued large deployments from expansive enterprise, SDN, and SCADA integration	Price erosion due to increased and new competition; competition from MDM vendors, wired/wireless infrastructure integration and systems management vendors
2016	17.5%	SDN integration, changes to regulatory compliance, broader mid-tier adoption	Price erosion, new functionality, additional hardware/cloud packaging
2017	10.25%	EVAS part of network/security infrastructure	Network/security staple, incremental price erosion

Figura 7. Dinámica del mercado EVAS entre 2013-2017. Tomada del reporte "The Endpoint Visibility, Access and Security, (EVAS) Market: The Evolution of Network Access Control (NAC)". De Enterprice Strategy Group, Inc.

VIII. CONCLUSIÓN

Tecnologías novedosas como NAC, tienden a surgir y desaparecer, muchas veces basadas en suposiciones y cuando la tendencia del mercado muestra una baja, las compañías suelen fijarse en la siguiente "estrella" de la tecnología.

Ciertamente algo así sucedió con NAC, y su ciclo de vida fue tomando forma de hipérbole hasta casi desaparecer, sin embargo algunos fabricantes no dieron su brazo a torcer y después de una recesión mundial NAC se transformó en EVAS y actualmente su impacto en el mercado es enorme. Tendencias del mercado como movilidad y BYOD, monitoreo continuo y automatización de procesos de seguridad, llevaron a EVAS a ser un aliado para las compañías en el manejo de nuevos riesgos y requerimientos.

Las soluciones EVAS están disponibles hoy en día y rápidamente se están convirtiendo en tecnologías esenciales que pueden soportar el negocio, la seguridad de la información e iniciativas de gobierno y cumplimiento. Indudablemente se puede tener la certeza de que los profesionales en seguridad de la información tomaran ventaja de todas las capacidades de EVAS para desarrollar las estrategias de seguridad de la información y afrontar los retos que las nuevas tendencias de tecnología puedan traer.

REFERENCIAS

[1] L. Orans and J. Pescarore, "Strategic Road Map for Network Access Control" Gartner, Inc., Stamford, CT, Rep. G00219087, Oct. 11, 2011. [Online]. Disponible: http://www.arubanetworks.com/pdf/Gartner-Roadmap-for-NAC.pdf

[2] G. Mark Hardy, "The Critical Security Controls: What's NAC Got to Do with IT?", SANS Institute, Bethesda, MD, Abr. 2013. [Online]. Disponible: http://www.sans.org/reading-room/whitepapers/analyst/critical-security-controls-what-039-s-nac-it-35115

[3] Sophos, "NAC 2.0: A new model for a more secure future" Sophos Plc, Boston, MA, Jul. 2008.

[4] Allied Telesis, "Allied Telesis provides advanced edge security for enterprise networks" Allied Telesis Inc., North Creek Parkway, WA, 2008. [Online]. Disponible: http://alliedtelesis.com.br/media/pdf/Advanced_Edge_Security_with_NAC_revA.pdf

[5] J. Wilson, "The Evolution of Network Access Control", Infonetics Research, Inc., Silicon Valley, CA, Nov. 2009. [Online]. Disponible: http://www.infonetics.com/whitepapers/2009-Infonetics-Research-The-Evolution-of-Network-Access-Control-FINAL-112309.pdf

[6] J. Oltsik, "The Endpoint Visibility, Access and Security, (EVAS) Market: The Evolution of Network Access Control (NAC)". Enterprice Strategy Group, Inc., Milford, MA, Jul. 2013.

[7] D. Montner, "Network Access Control (NAC) Evolves Into Endpoint Visibility, Access and Security (EVAS) Market Says ESG", ForeScout Technologies, Inc. Cupertino, CA, Rep 203-226-9290, Jul. 30, 2013. [Online]. Disponible: http://www.forescout.com/wp-content/media/ForeScout_ESG_Research_July-30-2013_final.pdf