Historia de cliente de Akamai

Novant Health protege las API que impulsan una atención innovadora

Detección y mitigación de los riesgos de las API con visibilidad, protección de datos y pruebas "shift-left"

Identificación de las vulnerabilidades de seguridad

Mitigación de los riesgos de forma proactiva

Mejora de la eficiencia de los desarrolladores

¿Cuántas vidas puede mejorar el sistema de salud mediante una atención integral y centrada en la comunidad? Para Novant Health, la respuesta es impactante e incluye:

- 6,8 millones de visitas médicas
- 155 964 pacientes hospitalizados atendidos
- 602 590 visitas de urgencias
- 22 082 partos

Cifras como estas también nos ayudan a hacernos una idea de quién y qué necesita una institución sanitaria para protegerse frente al abuso de las API y evitar la filtración de datos confidenciales.

¿Qué está en juego?

Novant Health es un sistema integrado sin ánimo de lucro de 16 centros sanitarios y más de 1900 médicos que abarca más de 900 ubicaciones. Con más de 36 000 miembros en el equipo y médicos asociados, la organización con sede en Winston-Salem opera en Carolina del Norte y Carolina del Sur.

A través de una serie de iniciativas digitales, Novant hace posible que la atención al paciente sea más efectiva, personalizada y eficiente. Las API se encuentran en el centro de esta innovación y permiten un intercambio continuo de datos de pacientes entre diferentes aplicaciones, dispositivos y sistemas. De hecho, resultan tan imprescindibles que Novant creó un centro de excelencia (COE) que engloba personas, conocimiento y recursos con el fin de garantizar el desarrollo de los mejores productos de API.

NOVANT HEALTH

Ubicación

Winston-Salem, Carolina del Norte
novanthealth.org

Sector

Ciencias de la salud y de la vida

Solución

API Security

Akamai

Tras haber buscado información sobre cómo los ataques a las API afectan a los profesionales sanitarios, el equipo tuvo claro desde el principio que la seguridad de las API era su máxima prioridad. Las estadísticas del sector que fueron descubriendo sobre la marcha también resultan impactantes, pero no en el buen sentido. Por ejemplo, el coste promedio de una filtración de datos sanitarios es de 9,7 millones de USD. Además, el 79 % de las organizaciones sanitarias han sufrido un incidente de seguridad de API en los últimos 12 meses.

Identificación del problema

Como primera medida, el COE antes mencionado determinó que era necesario mejorar la seguridad de las API en toda la organización de Novant. La única solución con la que ya contaban era un firewall de aplicaciones web (WAF). Estas herramientas ofrecen protección contra ataques ya conocidos, pero las organizaciones sanitarias actuales requieren un enfoque integral para proteger las API. Para ello, este enfoque debe incluir:

- Visibilidad sobre cuántas API existen dentro del entorno de TI de una organización.
- Información acerca de los atributos de riesgo de cada API, como los tipos de datos que gestiona.
- Análisis en profundidad de la estrategia de seguridad de API de una organización, incluidos los errores de configuración que aprovechan los atacantes.
- Protección frente a los ataques que aprovechan defectos en la lógica empresarial de las API.

Además, el equipo del COE de Novant identificó una serie de lagunas en las iniciativas de la organización para detectar problemas en las fases iniciales o integrar la seguridad en las primeras etapas de desarrollo. Ya disponían de herramientas para probar los contenedores de Docker, pero necesitaban una solución para el desarrollo de las API. Teniendo en cuenta que gestionan datos confidenciales, como los historiales de los pacientes, coincidieron en que necesitaban encontrar un proveedor cuyo personal y cuyos productos se centraran al 100 % en proteger las API.

Descubrimiento de momentos reveladores

El COE de Novant empezó a reunirse con Noname Security (que actualmente es una empresa de Akamai) tras conocer su enfoque integral para proteger las API. Juntos, llevaron a cabo un análisis en profundidad de la gestión de la estrategia de cada API en el entorno de TI de Novant. Mediante la plataforma de seguridad de API de Noname (que ahora forma parte de Akamai API Security), el equipo identificó una vulnerabilidad de Azure que conllevaba graves implicaciones de seguridad.

> Gracias a Akamai, en Novant Health pudimos subsanar una brecha importante y obtuvimos una mayor visibilidad sobre uno de los activos que más suelen atacar los agentes maliciosos. Los hallazgos que se han hecho hasta la fecha con respecto a las vulnerabilidades existentes de nuestro ecosistema de API ya han demostrado su valor. La seguridad de los activos de datos es nuestra principal prioridad. Akamai comparte esta visión y se ha convertido en un pilar fundamental dentro de nuestra infraestructura general de seguridad de datos.
>
> – Justin P. Byrd
> Vicepresidente de Plataforma de Datos e Integración, Novant Health

Akamai

La solución de gestión de la estrategia de las API de la plataforma reveló que algunas de las solicitudes dirigidas a las API del entorno de nube de Novant llegaban pasando *alrededor* de su herramienta WAF, en lugar de a través de ella. Los atacantes evitaban el WAF a través de una "puerta abierta" que el WAF no había podido proteger y atacaban de forma repetida las API de Novant, dejando así a la compañía expuesta sin que fueran conscientes de ello.

La información que aportó Akamai fue impactante y resultó útil de inmediato. La capacidad de Novant Health para desarrollar y mantener API de forma segura pasa por tener un espacio de trabajo en la nube totalmente protegido. El vicepresidente de Novant, Justin P. Byrd, y su equipo quedaron impresionados por la voluntad del equipo de Akamai de arremangarse y aplicar su solución de gestión de la estrategia de las API para detectar y mitigar las deficiencias de seguridad que se habían descubierto.

A partir de sus descubrimientos iniciales, el equipo del COE ya pudo empezar a utilizar las funciones automatizadas de la solución de gestión de la estrategia de las API de Akamai. Estas funciones se encargan de analizar continuamente las API y detectan errores de configuración y riesgos ocultos para que la organización pueda tomar medidas para mitigarlos de forma proactiva. Esto incluye la posibilidad de identificar cuáles son las API y los usuarios internos que pueden acceder a los datos confidenciales.

Para una organización como Novant, que administra datos sanitarios y que establece millones de interacciones con pacientes, saber cuáles son las API que interactúan con información confidencial resulta fundamental para generar confianza en los pacientes, proveedores y organismos reguladores, así como para mantenerla.

Seguridad y valor empresarial

Para el COE de Novant, formado por expertos en ingeniería con mucha experiencia, otra prioridad era la de integrar la seguridad en las pruebas de API de la organización. La velocidad de desarrollo es esencial para todas las API, y más en una organización como Novant, cuyas API desempeñan un papel crucial en la atención al paciente. Sin embargo, los desarrolladores deben crearlas a contrarreloj, lo que hace que sea más fácil que una vulnerabilidad o un defecto de diseño pasen desapercibidos.

Para ello, el COE buscó capacidades de prueba de API fiables con el objetivo de evaluar las medidas de seguridad implementadas en cada API. Esto implica realizar pruebas exhaustivas para identificar vulnerabilidades en variables como mecanismos de autenticación, controles de autorización, integridad de los datos y protocolos de cifrado.

Como pasa con cualquier implementación de una nueva herramienta de seguridad, el éxito no depende solo de su funcionalidad, sino también de la implicación de las principales partes interesadas. Los desarrolladores son conscientes de la importancia de la seguridad, pero debido a su ritmo de trabajo, suelen desconfiar de cualquier herramienta desconocida que pueda acarrear una ralentización.

Eso fue lo que ocurrió en Novant Health al principio.

A medida que el equipo de Novant fue interactuando más con Akamai, indicó una serie de funciones que podrían ayudar a los desarrolladores a realizar su trabajo de forma segura y eficaz. Por ejemplo, la solución Active Testing de Akamai API Security les ayudó a desvelar de forma proactiva algunos errores que se podrían haber convertido en graves problemas y cuya resolución habría supuesto mucho tiempo.

Además, dicha solución también permitió al COE ofrecer a los desarrolladores algunos consejos rápidos para mejorar la eficiencia, lo cual fue una agradable sorpresa para los miembros del centro, que no se habían percatado de que la solución también hacía comprobaciones de control de calidad no relacionadas con la seguridad. Por ejemplo, pudieron determinar si las especificaciones de API coincidían con lo que las API desarrolladas estaban proporcionando en realidad. Los desarrolladores, que al principio eran reticentes, no tardaron en darse cuenta de los beneficios para la seguridad y la eficiencia, y estuvieron encantados de trabajar con Akamai API Security.

"Desde el primer día, Akamai ha sido un asesor de confianza para detectar, proteger y probar nuestras API en todas las fases, desde la codificación hasta la producción. Nuestro centro de excelencia ha demostrado a toda la organización que la eficiencia y la seguridad son perfectamente compatibles", explicó Byrd. Esta colaboración no se limita a los productos. Las personas del equipo de Noname [que ahora forma parte de Akamai] entienden nuestro mundo y los factores comerciales que hay detrás del desarrollo de las API.

El equipo directivo de Novant también estuvo de acuerdo y resaltó la capacidad de Akamai API Security para "detectar riesgos antes de que se conviertan en un problema". Además, ayudó a consolidar la seguridad de las API en las iniciativas de la organización por detectar problemas en las fases iniciales.

La seguridad de API como motor de cambio

En la actualidad, Novant utiliza Akamai API Security para proporcionar una "protección automática" a sus API y a todas las iniciativas digitales que impulsan. Tras ver los resultados de Novant en términos de detección, inventario, evaluación y pruebas de API, el equipo del COE empezó a aplicar la protección integral de la plataforma a las nuevas API que Novant desarrollaba. El equipo cree que, a medida que los desarrolladores de Novant vayan desarrollando API basadas en las prácticas recomendadas, todas ellas recibirán protección de forma automática.

De cara al futuro, prevé ampliar el uso de Akamai API Security a otros equipos de la empresa. Con el objetivo de crear un modelo de colaboración entre empresas para la protección de las API, el COE tiene previsto que el equipo de seguridad de Novant Health y el equipo de la estructura básica de la organización se unan a él y utilicen Akamai API Security.

NOVANT HEALTH

Novant Health es un sistema integrado sin ánimo de lucro de 19 centros médicos y más de 2000 médicos que abarca más de 900 ubicaciones, así como numerosos centros de cirugía externa, centros médicos, programas de rehabilitación, centros de diagnóstico por imágenes y programas de prevención sanitaria para la comunidad. Los casi 40 000 miembros del equipo y médicos asociados de Novant Health cuidan a pacientes y comunidades de Carolina del Norte y Carolina del Sur.

| Publicado en enero de 2025

Akamai