História do cliente da Akamai

Novant Health protege APIs que impulsionam cuidados inovadores

Encontrar e atenuar riscos de API com visibilidade, proteção de dados e testes "shift-left"

Vulnerabilidades de segurança identificadas

Redução proativa de riscos

Aumento da eficiência do desenvolvedor

Quantas vidas um sistema de saúde pode melhorar por meio de cuidados abrangentes e focados na comunidade? Para a Novant Health, a resposta é surpreendente, incluindo:

- 6,8 milhões de atendimentos em clínicas médicas
- 155.964 internações
- 602.590 visitas ao pronto-socorro
- 22.082 partos

Números como esses também oferecem uma visão clara de quem e o que uma instituição de saúde precisa proteger contra agentes mal-intencionados que visam dados confidenciais por meio de violações de API.

Saber o que está em jogo

A Novant Health é um sistema integrado sem fins lucrativos com 16 centros médicos e mais de 1.900 médicos, abrangendo mais de 900 locais. Com mais de 36.000 membros da equipe e parceiros médicos, a organização baseada em Winston-Salem presta assistência na Carolina do Norte e na Carolina do Sul.

Por meio de uma série de iniciativas digitais, a Novant torna o atendimento ao paciente mais eficaz, personalizado e eficiente. As APIs estão no centro dessa inovação, permitindo uma troca perfeita de dados de pacientes entre aplicativos, dispositivos e sistemas. Na verdade, as APIs são tão essenciais que a Novant construiu um COE (center of excellence, centro de excelência) que compreende as pessoas, o conhecimento e os recursos para garantir o melhor desenvolvimento de produtos de API da categoria.

NOVANT HEALTH

Localização

Winston-Salem, Carolina do Norte
novanthealth.org

Setor

Saúde e ciências biológicas

Solução

API Security

Akamai

Após pesquisar como os ataques focados em APIs afetam os provedores de serviços de saúde, a equipe considerou, com razão, a segurança de APIs como prioridade máxima desde o início. As estatísticas do setor que eles descobriram ao longo do caminho também são surpreendentes, mas não em um sentido positivo. Por exemplo, o custo médio de uma violação de dados no setor de saúde é de US$ 9,7 milhões. E 79% das organizações de saúde sofreram um incidente de segurança de APIs nos últimos 12 meses.

Identificar o problema

A primeira medida do COE de APIs determinou que era necessário elevar o nível de segurança das APIs em toda a organização da Novant. A única solução existente era um firewall de aplicativos da Web (WAF). Essas ferramentas oferecem proteção contra ataques já conhecidos, mas as organizações de saúde atuais exigem uma abordagem mais abrangente para proteger APIs, incluindo:

- Visibilidade de quantas APIs existem no ambiente de TI de uma organização
- Informações sobre os atributos de risco de cada API, como tipos de dados manipulados
- Análises detalhadas da postura de segurança específica da API de uma organização, incluindo descobrir configurações incorretas que os invasores exploram
- Proteção contra ataques que exploram falhas na lógica de negócios da API

Além disso, a equipe do COE da Novant identificou lacunas importantes nos esforços da organização para instaurar uma abordagem “shift left” ou incorporar a segurança nas etapas iniciais do desenvolvimento. Havia ferramentas em vigor para testar conteinêires do Docker, mas era preciso uma solução para o desenvolvimento de APIs. Com dados confidenciais em jogo, como prontuários de pacientes, a equipe do COE da Novant concordou que precisava encontrar um fornecedor cujo pessoal e produtos estivessem 100% focados na proteção de APIs.

Descobrir "momentos de revelação"

O COE da Novant começou a se reunir com a Noname Security (atualmente uma empresa da Akamai) após conhecer sua abordagem abrangente para a segurança de APIs. Juntos, eles realizaram uma análise aprofundada de gerenciamento de postura de cada API no ambiente de TI da Novant. Usando a plataforma de segurança de APIs da Noname (agora parte do Akamai API Security), a equipe identificou uma vulnerabilidade do Azure que teve grandes implicações de segurança.

> “A Akamai preencheu uma lacuna considerável para nós na Novant Health, proporcionando maior visibilidade sobre um dos ativos mais visados por agentes maliciosos. As descobertas que tivemos até o momento sobre vulnerabilidades de segurança acionáveis em nosso ecossistema de APIs já demonstraram seu valor. Na Novant Health, a proteção de nossos ativos de dados é nossa principal prioridade. A Akamai está alinhada com esses valores e se estabeleceu como um recurso fundamental em nossa pilha geral de segurança de dados.
>
> – Justin P. Byrd
> Vice-presidente, Plataforma de Dados e Integração, Novant Health

Akamai

A solução de gerenciamento de postura de APIs da plataforma revelou que algumas solicitações para as APIs no ambiente em nuvem da Novant estavam *contornando* e não atravessando a ferramenta WAF. Os invasores contornavam o WAF por meio de uma "porta aberta" que ele não conseguia proteger e atacavam repetidamente as APIs da Novant, deixando a empresa exposta e desprevenida.

Os insights fornecidos pela Akamai foram chocantes e imediatamente muito úteis. A capacidade da Novant Health de desenvolver e manter APIs de forma segura depende de ter um ambiente de trabalho em nuvem totalmente protegido. O vice-presidente da Novant, Justin P. Byrd, e sua equipe ficaram impressionados com a disposição da equipe da Akamai em arregaçar as mangas e aplicar sua solução de gerenciamento de postura de API para encontrar e reduzir as lacunas de segurança descobertas.

Com base nas descobertas iniciais, a equipe do COE agora pode usar as capacidades automatizadas da solução de gerenciamento de postura de APIs da Akamai, que verificam continuamente as APIs em busca de mau funcionamento e riscos ocultos, permitindo que a organização tome medidas para atenuá-los proativamente. Isso inclui a capacidade de identificar quais APIs e usuários internos podem acessar dados confidenciais.

Para uma organização como a Novant, que é responsável pelos dados de saúde que abrangem milhões de interações com pacientes, saber quais APIs lidam com informações confidenciais é essencial para construir e manter a confiança com pacientes, prestadores de serviços e reguladores.

Perceber a segurança e o valor comercial

Para o COE da Novant, que é composto por líderes de engenharia com experiência prática, outra prioridade foi incorporar a segurança nos testes de APIs da organização. A velocidade de desenvolvimento é essencial para cada API, e isso é especialmente verdade para uma organização como a Novant, cujas APIs desempenham um papel essencial no atendimento ao paciente. No entanto, a pressão para desenvolver rapidamente também faz com que vulnerabilidades ou falhas de design passem despercebidas enquanto os desenvolvedores correm para passar para a fase de produção.

O COE buscou recursos confiáveis de teste de APIs para avaliar as medidas de segurança implementadas em cada uma delas. Isso envolve a realização de testes abrangentes para identificar falhas em variáveis como mecanismos de autenticação, controles de autorização, integridade de dados e protocolos de criptografia.

É claro que, em qualquer implementação de uma nova ferramenta de segurança, o sucesso depende não apenas da funcionalidade, mas também do envolvimento dos principais interessados. Os desenvolvedores reconhecem a importância da segurança, mas, devido à necessidade de agilidade, geralmente ficam receosos com qualquer lentidão que uma ferramenta desconhecida possa causar.

No início, esse foi o caso na Novant Health.

À medida que a equipe da Novant se envolvia mais com a Akamai, ela identificou uma série de recursos que poderiam ajudar os desenvolvedores a realizar seu trabalho com segurança e criando eficiências. Por exemplo, o Active Testing do Akamai API Security poderia identificar proativamente erros que se tornariam problemas significativos e que consumiriam muito tempo mais adiante no processo.

Além disso, a solução também permitiu que o COE fornecesse notas rápidas aos desenvolvedores para aumentar a eficiência, o que foi uma surpresa agradável para os membros da equipe do COE que não sabiam que a solução também fazia verificações de controle de qualidade não relacionadas à segurança. Por exemplo, agora eles podem determinar se as especificações de uma API correspondem ao que as APIs criadas estavam realmente fornecendo. Não demorou muito para que os desenvolvedores, que estavam indiferentes no início, se juntassem à equipe do COE no reconhecimento dos benefícios da segurança e da eficiência e ficassem entusiasmados com o trabalho com o Akamai API Security.

"Desde o primeiro dia, a Akamai tem sido uma conselheira confiável sobre como descobrir, proteger e testar nossas APIs em todas as etapas, desde a codificação até a produção. Isso permite que nosso centro de excelência mostre a toda a organização como alcançar segurança e eficiência, tudo de uma só vez", explicou Byrd. "Esta parceria não abrange apenas produtos. As pessoas da equipe da Noname [atualmente uma empresa da Akamai] entendem o nosso mundo e os interesses comerciais por trás do desenvolvimento de APIs."

A liderança da Novant também concordou, citando a capacidade do Akamai API Security de "detectar as coisas antes que elas se tornem um problema" e ajudou a consolidar a segurança de APIs nos esforços de implementar a abordagem "shift-left" da organização.

Aproveitar os ganhos com a segurança de APIs

Atualmente, a Novant usa o Akamai API Security para fornecer "proteção automática" para suas APIs e para cada iniciativa digital que a empresa promove. Com base nos avanços da Novant em descobrir, inventariar, avaliar e testar APIs, a equipe do COE agora está aplicando a proteção abrangente da plataforma às novas APIs que a Novant desenvolve. A equipe acredita que, à medida que os desenvolvedores da Novant criam APIs com base em melhores práticas alinhadas, cada API será automaticamente protegida.

Olhando para o futuro, a equipe do COE prevê a expansão do uso do Akamai API Security para outras equipes dentro da empresa. Visando a um modelo colaborativo entre empresas para proteção de APIs, o COE prevê uma parceria entre eles, a equipe de segurança da Novant Health e a equipe de estrutura de fundação da organização para usar o Akamai API Security.

NOVANT HEALTH

A Novant Health é um sistema integrado sem fins lucrativos composto por 19 centros médicos e mais de 2.000 médicos em mais de 900 locais, além de diversos centros de cirurgia ambulatorial, clínicas, programas de reabilitação, centros de imagem diagnóstica e programas de alcance à saúde comunitária. Os quase 40.000 membros da equipe e parceiros médicos da Novant Health cuidam de pacientes e comunidades na Carolina do Norte e na Carolina do Sul.

Akamai