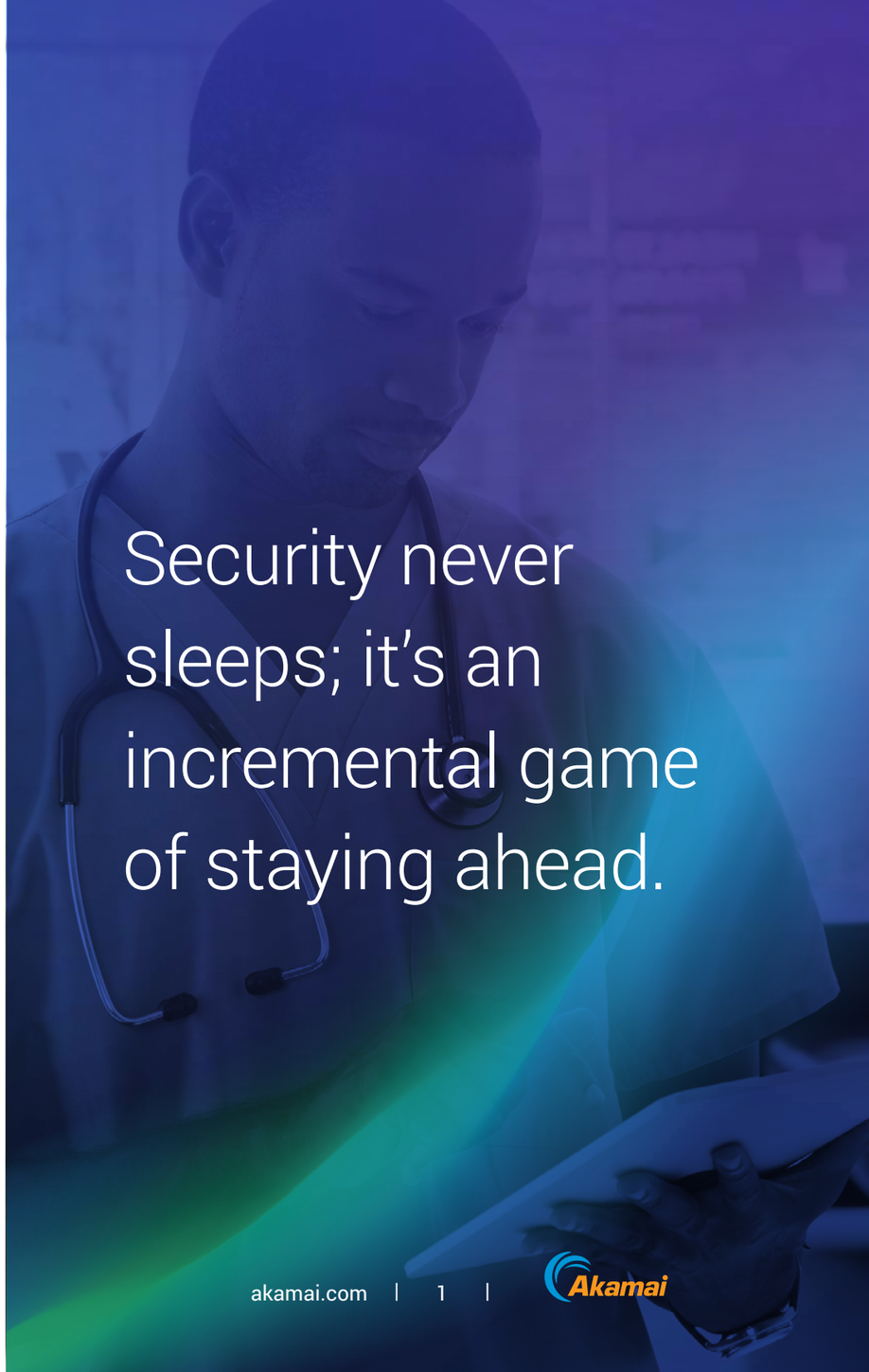
What's Next for Payers: Secure Your Infrastructure for Tomorrow with Akamai

At Akamai, we understand the payer landscape, working closely with 9 of the top 10 U.S. health insurance organizations. Our commitment to securing our payer partners requires deep organizational and industry knowledge to ensure we provide optimal support to the correct teams within these complex organizations, allowing risk mitigation and enabling our customers to develop resilient infrastructure. Securing critical infrastructure is not new for Akamai, as we secure infrastructure internationally and across industries. Akamai's footprint as a trusted partner spans from the U.S. military, to leading financial services and ecommerce organizations, to healthcare providers, payers, and pharma and life sciences companies.

The past year has demonstrated the vulnerabilities in some key aspects of our healthcare system. We work continuously with our partners to ensure they stop threat actors in their tracks. Below, we highlight some of our experiences to date, reviewing our customers' and partners' pain points and market trends. Security never sleeps and is an incremental game to stay ahead. As we outline each horizon, keep in mind that the challenges and solutions of one horizon set expectations for the subsequent horizon.



Past: Secure cloud infrastructure

- Our payer partners began migrating to cloud services, leaving their walled-off on-prem solutions that drove payer IT architecture and solutioning for decades.
- This migration, along with the expansion of web portals for patient enrollment and benefits viewing, led to initial cloud strategies and expanded websites.
- These first challenges aligned closely with Akamai's core strengths. With our experience in financial services (another highly regulated, distributed, complex industry), we assisted our clients with their content delivery, DNS, and WAF needs.
- Our 100% uptime services kept our customers safe as they began opening their systems to outside partners.
- In the past, payers still focused on compliance, but the targets of those policies and acts were different.
- Prompt pay, no surprise billing, and other claims processing requirements emphasized the need for system uptime — with downtime potentially leading to claims processing delays, which resulted in fines.
- The medical loss ratio, coming from the Affordable Care Act, also shifted how payers operate, resulting in more transparent financial reporting.

Akamai secures 9 of the top 10 U.S. health insurance organizations, leveraging deep industry knowledge to mitigate risks and build resilient infrastructure. Our solutions evolve with the payer landscape, addressing past challenges of cloud migration, present demands of interoperability and API security, and future needs for precise PHI/PII management.

With a track record of securing critical infrastructure across industries, Akamai offers payers a trusted partner to navigate complex security challenges, from DDoS protection and WAF implementation to Zero Trust architectures and API security, ensuring compliance and operational efficiency in an ever-changing threat landscape.

Some of the major persistent threat challenges are ransomware, which can have a material impact and affect patient safety; DDoS, which can impact access to critical capabilities; API attacks, outlined in the OWASP API Security Top 10; and credential or identity theft. While there are other attacks and technical debt issues the industry faces, these are generally the most pressing.

During this era, our typical payer partner worked with Akamai on:

- CDN for performance
- DNS security and performance
- WAF to stop attacks and prevent fraud
- DDoS mitigation to maintain resiliency

We helped our customers maintain uptime, securely, and feel comfortable with their cloud transitions and migrations.

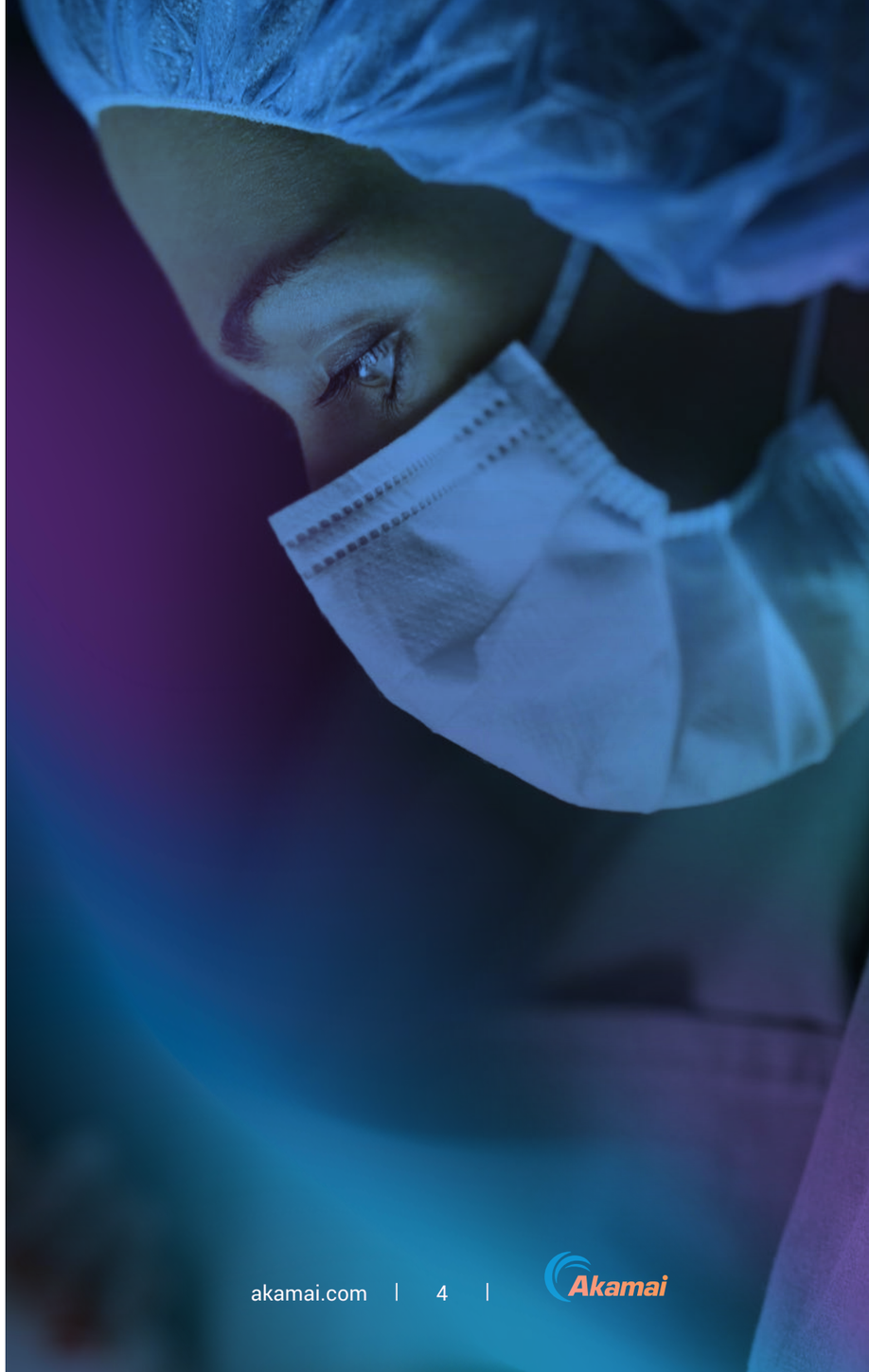
Akamai's healthcare security footprint

9 out of 10

Top U.S. health insurance organizations secured by Akamai

Present: Secure interoperability (built upon secure infrastructure)

- Interoperability and integration are table stakes for modern healthcare businesses — and compliance efforts, from the Cures Act to CMS-0057, and data centralization efforts such as TEFCA — are pulling payers toward API-centric FHIR exchange.
- Akamai has solved this before, as our partners in ecommerce and financial services experienced it previously. And we have been acquiring additional cybersecurity assets and capabilities that directly address the needs of today.
- One challenge our partners face is visibility of their current systems. Internal (east-west) API traffic often goes overlooked as organizations focus on external (north-south) traffic. Both types of API traffic are under-monitored. API gateways are important tools and can help with some aspects of Zero Trust, but they are not security systems. A more comprehensive approach is necessary in today's environment.
- Risk and attack mitigation are also top of mind, with the threat of parallel movement leading to redundancies along with additional physical and digital protections. Our payer partners appreciate our microsegmentation as another measure to increase resiliency and prevent threat actors from expanding their reach within compromised systems.
- As each new API integration (FHIR or otherwise) is promoted to a production system, our partners recognize the endpoint as another potential exposure point in their risk surface. Akamai's API security offerings expand API security capabilities by leading with discovery and posture management, and also providing runtime monitoring and identifying out-of-band calls.



Staffing troubles lead to outsourcing as organizations struggle with finding the right support, and our fully managed services meet our payer partners where they are, even in fluctuating labor markets.

The major cyber issues facing the industry today are:

- The proliferation of unsecure medical devices providing data
- Compliance issues for PCI DSS v4.0 (and for publicly traded companies, the requirement to report material events)
- Scrapers standing up fake sites to facilitate phishing campaigns
- Rogue APIs and API abuse not being discovered and addressed
- DDoS and ransomware attacks impacting healthcare organizations' operations

Today, our typical payer partner works with us on an expanded set of capabilities:

- From yesterday:
  - CDN for performance
  - DNS security and performance
  - WAF to stop attacks and prevent fraud
  - DDoS to maintain resiliency
- To today:
  - Bot management
  - Zero Trust to include microsegmentation and MFA
  - API security
  - Domain protection
  - Scraper protection
  - Full support offerings from managed service to on-demand engineering for optimization

Future: Precise PHI and PII strategies and retightening of controls

Nobody can predict the future, but we anticipate some of the following themes over the next few years:

- Looking ahead, as networks become more complex, visibility and situational awareness become vital, and the ability to push policy to enforce appropriate segmentation is a must.
  - Building from the strong foundation provided by Zero Trust, we anticipate stronger encryption protocols as the new standard for sharing health data.
- The open sharing of healthcare data today will cause a tightening of data sharing tomorrow to execute HIPAA's "minimum required data" imperative.
  - With providers seeking more financial and operational data and payers seeking more clinical data, efforts like TEFCA are opening up data sharing to more parties. While this is better than the cordoned-off private networks of yesterday (where monopolies and private networks dominated), this provides new challenges.
  - The market will look for a secure core database to house PHI. Something like a Fort Knox for healthcare data. Akamai's secure cloud compute services are a natural fit as a security-first, cloud database implementation method.

- Contracts/complex logic for permissions of granular data sharing.
  - Having experienced interoperability and open-industry trends, we anticipate a retightening of policy to control how and when PHI and PII are shared among parties.
  - The long tail of use cases included in TEFCA begin to complicate data sharing among entities, with organizations acting “on behalf of” other organizations and their patients/members having possibly too much data access.
  - We anticipate additional efforts to ensure patients actually consent to data record sharing among parties, with significant implications to aggregate datasets.
  - While this is a bit speculative, it could look something like an open blockchain with encrypted patient keys, and digital consents to filter shared data to only include consented data.
- The threat ecosystem will continue to grow while the industry faces financial and staffing challenges. Resiliency will become more important, and more care and services will become remote. Cyber risk issues will keep growing in scope and sophistication.
- Customers will continue to demand high levels of performance from both websites and applications, so distributed compute will become more common to meet these expectations.
- DDoS attacks across DNS, Level 7 web presence, and Level 3/4 infrastructure continue to set new records for speed, volume, and complexity, which will require continuous validation of capabilities.

- Fraud continues to explode, so positively identifying customers will continue to grow as a vital part of your business. This requires low-friction processes to evaluate customer identity fraud as a potential risk.
- Transformation is driving adoption of APIs, which have a unique set of vulnerabilities (as outlined in OWASP API Security Top 10), so payers need to field solutions that are designed to protect APIs.
- Scrapers are becoming a major issue, as attackers often scrape the content of corporate websites, then create their own spoofed site, registering a misleading domain to fool unsuspecting users into compromising their credentials or buying from counterfeit sites.
- Brand impersonation, which is often used to steal customer credentials, is driving the need for domain security.

> With Akamai, security and performance are not mutually exclusive.
>
> – Claire Broome
> Sales Manager, Healthcare & Life Sciences, Akamai

Learn more about our healthcare & life sciences solutions.