PAPER

Digital Transformation for Payers

Introduction

As your organization evaluates and adopts new applications, tools, and widgets to transform internal processes and enhance your members' experience, your cyberattack surface expands. Whether you are optimizing claims-processing workflows, reengineering member acquisition, enhancing the user experience for members, or complying with ever-evolving legislative mandates, cybersecurity investments must be built in to your planning and budgeting from day one.

And it's not just new technology. When software run by legacy systems is no longer supported, it may have vulnerabilities that new or more recently updated solutions have accounted for. This is an essential consideration for payers because claims adjudication systems, for example, can have a lifecycle of up to 50 years.

Cyberattacks relentlessly target healthcare organizations

As cybercriminals actively search for vulnerabilities to exploit, the valuable protected health information (PHI) contained in many healthcare systems makes payers a prime target. Stolen PHI is used for a range of nefarious deeds, including medical claims fraud and the illegal purchase of prescriptions. That's why cybercriminals are willing to pay so handsomely for it.

PHI is worth an average of $250 per record on the black market, with some estimates going as high as $1,000 per record. These are astronomical prices compared with other types of personal information. A social security number, for example, might be sold for a single dollar.

Each tool you use and application you deploy has its own impact on your organization's attack surface and requires a specific cybersecurity solution. A comprehensive approach is necessary to provide adequate protection for the vulnerabilities that criminals are looking for, and that's precisely what a secure access service edge (SASE) provides.

SASE is a cloud-based, enterprise security framework that offers a comprehensive cybersecurity approach focused on the challenges introduced during digital transformation efforts. Leveraging SASE framework can ensure a comprehensive cybersecurity strategy that includes a web application firewall, Zero Trust network architecture, and microsegmentation. Collectively, these solutions protect users while providing organizations with scale and efficiency gains for websites, applications, and APIs. Some of the most commonly needed solutions are described in the sections below, framed within the context of the various tools your payer organization may use.

Cyber risks for internal payer solutions

Cybercriminals often gain entry to a network through a social engineering vulnerability, like capturing an employee's login credentials in a phishing attack. That means your internal solutions are just as vulnerable as your member-facing applications. It's crucial to examine your team's varied and evolving tech stack to determine your vulnerabilities and the security solutions that will shore them up.

Claims adjudication systems and accumulators

Because claims processors and accumulators require member information from various sources (provider electronic health records, lab systems, pharmacies, clearinghouses, etc.), there are numerous opportunities for protected data to be compromised. Your network must allow certain connections for calculating total claim dollar values and verifying real-time eligibility, but these connections—both internal and external—increase the size of your attack surface and demand a robust set of security solutions.

For example, a distributed denial-of-service (DDoS) mitigation solution can limit network-layer DDoS attacks that threaten to overload your system. Using machine learning and crowdsourced intelligence, a DDoS mitigation solution helps identify and immediately drop malicious connections before they access your network. This is essential for maintaining strong relationships with members and provider networks. Members might leave if your network is deemed unreliable or untrustworthy, and contract negotiations with provider networks may become more challenging with a perceived lack of uptime reliability, causing significant lag in provider accounts receivable days.

In addition, Zero Trust Network Access (ZTNA) is a powerful security tool that treats each connection as a potential threat until it's proven trustworthy. In other words, ZTNA makes sure every internal access request comes from a known and trusted source before allowing the connection. Even when the same source makes a high volume of connections for sharing data, each request receives the same scrutiny. This type of identity verification is one of the most crucial steps you can take to secure the edge of your network.

Without ZTNA, bad actors might use an account takeover to access the active directory of all of your usernames and passwords. That information would provide unhindered access to your network, allowing the bad actors to do whatever they wanted, whenever they felt like doing it.

Criminals might lurk in your network for weeks or months before launching an attack. They study your system to learn all they can. In some cases, they might siphon off small volumes of data—completely unnoticed—for long periods. That can actually be more damaging for your organization over time, similar to how a long-running, leaky faucet releases more water than a burst pipe.

Pharmacy benefits manager connections

As the intermediaries of almost every aspect of the pharmacy benefits marketplace, pharmacy benefits managers (PBMs) require access to vast amounts of member data. They connect with employers, members, drug wholesalers, pharmacies, drug companies, and third-party vendors, all in an effort to facilitate the best health outcomes at the lowest possible costs.

PBMs are intermediaries, accessing payer systems frequently and posing a significant risk if compromised. For example, every time a provider sends in a prescription for one of your members, one of the primary tasks of a PBM is to confirm the patient's health plan and coverage with your system. In doing so, your network is potentially exposed to vulnerabilities presented by the PBM hundreds (if not thousands) of times per day.

If attackers are able to penetrate your system through a PBM (or other) connection, it's critical to limit the blast radius by reducing the lateral movements bad actors can make once inside. Lateral movements refer to the mobility a criminal has for accessing various parts of your network. In other words, entering through a low-value application might open a pathway to your most high-value data.

Previous incidents of this nature have led to the compromise of entire databases of protected information, including members' names, addresses, plan types, ID numbers, dependents' names, and primary care providers. Date of birth, premium invoice information, and Medicaid ID number were also exposed in some cases.

But with a microsegmentation solution, like Guardicore's, criminals' mobility is restricted by creating increasingly granular secure zones within your network, granting access to only the applications and data allowed according to a user's identity and role. This helps to mitigate attackers' network access and reduce the number of members affected by a breach.

Internal innovation team apps and solutions

The tools you develop for your team and partners, for tasks like automated claims intake and policy issuance, also contribute to your risk profile. Mitigating the increased exposure these solutions bring to your network requires a comprehensive view of your connections to create a clear map of where data is flowing to and from.

In addition to microsegmentation, Guardicore has a visibility tool that offers the comprehensive perspective you need. With easy insight into your network's core infrastructure configurations, potential attacks are recognized quickly and post-attack forensics are completed efficiently.

Think of the various and disparate systems that enable the sharing of information to and from your network—with provider groups, employer systems, pharmacies, etc. There are simply too many connections to keep track of and monitor effectively without help from the right solution. Guardicore offers that assistance by keeping a vigilant, watchful eye over every network connection and responding immediately to perceived threats.

Vulnerabilities associated with improving the member experience

Your organization already knows the importance of direct engagement with members and providers through the development and deployment of apps and other tools. But you may not realize that, while useful for boosting member acquisition and retention rates by improving the member experience, these tools unavoidably extend your network's attack surface and elevate the risk that your most valuable data will be breached.

As you replace existing tools and adopt new solutions, be mindful of your evolving and growing attack surface and the vulnerabilities that may be introduced. Incorporating the appropriate solutions is the best way to mitigate your risks and ensure adequate precautions.

Member engagement tools

Tools like member engagement platforms can elevate the level of engagement among your members. But each member runs the risk of initiating an account takeover by either mistakenly sharing their log-in credentials or having their information stolen or guessed through social media research. Even without accessing your database, account takeovers can have a damaging impact on your organization.

For instance, after a phishing attack successfully gains a member's log-in credentials, cybercriminals can then pose as the member to file false claims or acquire unprescribed medication. False claims can be a costly drain on your system, bogging down your processes. And a mistaken supply of drugs can damage the reputation your organization works so hard to maintain.

That's why it's crucial to protect your network's edge by verifying a user's device identity. In other words, you need to confirm that users are who they say they are at the point of entry to the internet rather than the point of entry to your system. Exploring new solutions as part of a broader SASE framework-based strategy can help identify the needs for these types of controls.

For example, your member-facing engagement tools, including web pages, applications, and APIs, can benefit from App & API Protector. This solution reduces your attack surface by automatically and continuously analyzing traffic, including known, unknown, and changing APIs. Potential threats are immediately flagged and mitigated. With additional bot visibility and mitigation capabilities built right in, simple workflows can also protect against DDoS, injection, and credential stuffing attacks.

Registration, enrollment, and billing tools

Under the umbrella of member engagement lies a slew of tools your organization depends on for communicating with employers and members. These tools facilitate activities such as new member registration and enrollment, managing services, and running your billing operations.

The mere existence of each additional employer or customer enlarges your attack surface and creates more vulnerabilities for your system. The same is true for your billing solutions and employee management tools. Various applications might reduce the resources required and lead to overall cost savings, but they can also increase the number of vulnerabilities to your system.

If your organization uses JavaScript to create a more engaging and personalized user experience, the scripts are potentially vulnerable to malicious code injection. This can lead to data loss or corruption, denial of access, or even a complete system takeover, and the resulting fallout can cause damaging ripple effects to your reputation and your bottom line. Existing members may leave for fear of another breach, and member acquisition may suffer for the same reason.

Page Integrity Manager will provide script protection to help thwart those threats before they materialize by monitoring scripts in real time, continuously analyzing first- and third-party URLs, and sending automated security event alerts.

Connected devices

Often categorized with the Internet of Things (IoT) or Internet of Medical Things (IoMT), connected devices that monitor members' biological data (like heart rate, sleep patterns, and so forth) are increasingly used by payers to encourage and track healthy behavior from members.

These types of devices can offer troves of insightful data that can assist with contract negotiations or help members avoid costly treatments. For example, a member who walks 12,000 steps a day is statistically less likely to need cardiac intervention. That information might help with premium adjustments, but it also presents an appealing target for criminals. Each connection to your network brings additional risk.

Beyond the impact a successful breach could have on your members, business operations, and revenue, there are also regulatory penalties and legal settlements to consider, which can both easily reach millions of dollars.

If your organization uses IoMT devices, it's recommended that you maintain adequate security infrastructure with ZTNA, web application and API protection as a service (WAAPaaS), and secure web gateway (SWG) services to protect users from threats like malware, ransomware, phishing, and data exfiltration. These solutions are all included within the SASE framework.

SWG, in particular, is designed to ensure that users and devices can securely connect to the internet wherever they happen to be. Using real-time threat intelligence, SWG checks every requested domain, URL, and payload for malicious intent and blocks untrustworthy requests before a connection is made.

Conclusion

It's time to stop thinking of cybersecurity as a competitive advantage. That may have been true in the past, but not anymore. Securing your network and protecting your data is a necessary cost of business in a rapidly changing industry.

You must protect your reputation and your bottom line by mitigating cybersecurity risks as much as possible. Members need to know that their data is safe with you. Otherwise, successful breaches could initiate a decline in your member retention rates and your new member acquisitions.

Beyond that, ransomware and DDoS attacks can create substantial network downtime, potentially costing your organization millions of dollars in lost revenue. That may cause members and partner organizations to question the reliability of your system and how much they can depend on your network in the future.

When combined with lost revenue and declining membership, monetary penalties and member suits can also contribute substantially to the overall cost of a successful breach.

With a comprehensive cybersecurity strategy delivered by an industry-leading vendor like Akamai, your organization can gain the necessary protections to stay competitive in an increasingly digital industry. Akamai is deeply invested in stopping cybercriminals. Our battle-tested solutions are backed by a team of experts who keep a watchful eye over your entire network at all times.

Attacks are bound to happen. And when they do, Akamai is ready to jump into action, mitigating costly damage to your network and getting your system up and operational as soon as possible.

Any person. Any device. Any time. Akamai can help.

Contact Akamai now to learn more.