Benefits Administrator Outmaneuvers Cyber Risks With Prevention-First Security Strategy

TRI-AD

"TRI-AD is held to a very high standard when it comes to protecting client information. We use the Palo Alto Networks platform to make sure data is not exfiltrated inappropriately or compromised by cyberthreats, so our clients can have full confidence that their private information is safe with us and compliant with the necessary regulations."

Doug Calapan | director of IT operations | *TRI-AD*

Industry

Professional Services

Challenge

Secure private, personal client employee data and business assets against the rising threat of cyberattacks and risk of exfiltration while ensuring compliance with government regulations.

Solution

Palo Alto Networks Next-Generation Security Platform, with application awareness and integrated cyberthreat prevention, extending from the network edge to remote users and endpoint devices.

Subscriptions

Threat Prevention, URL Filtering (PAN-DB), WildFire, GlobalProtect, Traps

Appliances

PA-3020 (2), PA-850 (1), PA-220 (2)

Results

- Enables preventive security posture from the network edge to endpoint devices.
- Elevates security of client portals with application-aware policies.
- Reduces complexity, eliminates interoperability issues and simplifies support.
- Improves reliability and performance for secure remote network access.
- Increases system uptime by preventing known and unknown threats.

Background

TRI-AD is a comprehensive employee benefits administration firm that serves the unique needs of both small and large employers. Founded in 1974, the hallmarks of this privately owned firm are its commitment to developing long-term, mutually beneficial client relationships and a superior service experience for plan participants. Over the years, TRI-AD has grown its service offerings to cover a full range of employee benefits administration services, from 401(k) and 403(b) plans to online benefits enrollment, claims reimbursement, health savings accounts, and COBRA administration, among many others.

Story Summary

As a leading provider of benefits administration services, TRI-AD understands the importance of protecting the private information of its clients' plan participants. Recognizing the rise of evermore sophisticated cyberthreats, the firm decided to simplify its network security infrastructure by replacing a mix of firewalls, VPN appliances and antivirus software with a single, integrated approach using Palo Alto Networks® Next-Generation Security Platform.

Since adopting the Palo Alto Networks platform, TRI-AD has reduced complexity, eliminated interoperability issues and simplified support while strengthening its overall security posture. The Next-Generation Security Platform ensures compliance with strict government regulations by preventing private personal, financial and health information from being compromised or exfiltrated by cyberattacks or vulnerability exploits. The platform has also improved performance and reliability for remote users requiring secure access to TRI-AD's data center, as well as increased overall system uptime and employee productivity by preventing both known and unknown cyberthreats from disabling workstations and servers across the enterprise.

Meeting High Standards for Securing Private Information

To the casual observer, benefits administration may seem like a service easily packaged for practically any company. How different could one plan be from another? In fact, they can be as different as one person from another – and no one knows this better than TRI-AD.

TRI-AD is anything but a cookie-cutter benefits administrator. For more than 40 years, the firm has staked its reputation on delivering white-glove service, tailoring its offerings to the unique needs of each client. Personalized, thoughtful attention to detail has earned TRI-AD high marks with its clients and proven a winning strategy that's driving the firm's continued growth. TRI-AD is now in its fifth decade of business.

> “With Palo Alto Networks, we have the No. 1-rated prevention algorithm that we can leverage from the edge of our network, extend to remote users and take all the way to our endpoints. That makes a powerful statement about how seriously we take security.”
>
> **Nick Viggianelli** | senior network engineer | *TRI-AD*

As a business that handles personal client information, such as Social Security numbers, investment account details and private health information, TRI-AD is extremely vigilant about protecting data in its care. The firm is also held to strict compliance with government regulations, such as the Health Insurance Portability and Accountability Act, or HIPAA, and the Employee Retirement Income Security Act, or ERISA. Before selecting TRI-AD, prospective clients often perform a risk assessment on TRI-AD’s security infrastructure, processes and ability to comply with these regulations. TRI-AD can respond with confidence largely because it has Palo Alto Networks Next-Generation Security Platform protecting its network infrastructure.

Doug Calapan, TRI-AD’s director of IT operations, remarks, “TRI-AD is held to a very high standard when it comes to protecting client information. We use the Palo Alto Networks platform to make sure data is not exfiltrated inappropriately or compromised by cyberthreats, so our clients can have full confidence that their private information is safe with us and compliant with the necessary regulations.”

Intelligent Threat Prevention From Edge to Endpoints

TRI-AD adopted the Next-Generation Security Platform to establish a prevention-first strategy against evermore sophisticated exploits as well as to consolidate multiple legacy security systems onto a single, integrated platform. In the past, the firm had a mix of SonicWall® firewalls, Barracuda Networks® SSL VPN appliances, and Sophos® antivirus software. The Palo Alto Networks platform does the work of all three, enabling TRI-AD to reduce complexity, eliminate interoperability issues and simplify support. Most importantly, the Next-Generation Security Platform strengthens the firm’s overall security posture by establishing a proactive, rather than reactive, approach to mitigating cyberthreats.

TRI-AD’s IT team deployed a high availability pair of PA-3020 next-generation firewalls in its production data center to secure the internet edge. A single PA-850 provides disaster recovery, while a PA-220 protects each of TRI-AD’s two business campuses. GlobalProtect™ network security for endpoints replaced the Barracuda SSL VPN appliances, and the firm now uses Traps™ advanced endpoint protection, eliminating the need for separate antivirus software. In addition to built-in Threat Protection and URL Filtering, the entire security infrastructure is further bolstered with WildFire® cloud-based threat analysis service.

“Everybody was on board with the move to Palo Alto Networks,” says Calapan. “Compared to our previous firewalls, the Palo Alto Networks platform meant a significant upgrade to our network security. For endpoint protection, in particular, we were trying to get ahead of the curve with all the new ransomware that’s been coming out. Traditional antivirus was just not the correct posture for us anymore.”

Nick Viggianelli, senior network engineer at TRI-AD, adds, “With Palo Alto Networks, we have the No. 1-rated prevention algorithm that we can leverage from the edge of our network, extend to remote users and take all the way to our endpoints. That makes a powerful statement about how seriously we take security.”

Mitigating Risk for Clients and Employees

One of the advantages TRI-AD gained with the Palo Alto Networks platform is application awareness through App-ID™ technology. Instead of traditional port-based traffic control, App-ID enables TRI-AD’s IT team to define security rules for specific applications. This is especially important to ensure only authorized applications interact with client portals.

“App-ID gives us an added layer of protection,” Viggianelli points out. “From a threat standpoint, if you block something only by port, hackers will eventually figure out how to sneak through using a different application. With App-ID, we can be more precise in how we define what’s blocked and what’s permitted through. It provides a higher level of security for our client portals than just locking down ports.”

Employee access is also secure. Using GlobalProtect, TRI-AD extends the full protection of the Palo Alto Networks platform to its remote users with the assurance of reliable, high-performance connectivity.

Viggianelli comments, “Connectivity with GlobalProtect has been great. We’ve had no issues, which is big in terms of productivity and efficiency. We wanted to avoid split tunneling, when users could be on our network and their home network at the same time. With GlobalProtect, we use an always-on full tunnel so that we know when they connect, everything is going through the Palo Alto Networks platform, and our security policies are being applied. So, the risk from outside threats is mitigated.”

> “Palo Alto Networks just seems to get it. They know what people are looking for and provide the products that meet those needs. That’s all you can ask for in a vendor.”
>
> **Nick Viggianelli** | senior network engineer | *TRI-AD*

Advanced Endpoint Protection Brings Peace of Mind

Traps further extends TRI-AD’s net of security with advanced, multi-method endpoint protection that prevents both known and unknown cyber exploits from sneaking in through its servers and end-user workstations. The IT team saw this firsthand in a demo that put Traps up against a simulated hacking attempt. With Traps turned off, the demo showed how easily a hacker could manipulate a machine’s vulnerabilities. With Traps enabled, however, the same hacking attempts were blocked.

“We saw how Traps prevents someone from going down a rabbit hole by just innocently clicking on a malicious link,” Viggianelli recalls. “That preventive approach to endpoint protection means more system uptime and user productivity because we don’t have to take down a production system to deal with an infection.”

He adds, “We also like that the footprint on machines is very lightweight. When traditional antivirus runs, it can slow down the machines. We haven’t seen anything like that with Traps. It just works.”

Calapan also notes the added value of having WildFire with Traps. “It’s peace of mind, more than anything else. We catch things like grayware or suspicious executables before they can do any damage. A lot of times, the end users don’t even know anything is going on in the background. That means we’re doing our job right – like the secret service, they’re safe, and nobody knows we’re there keeping them protected.”

Viggianelli concludes, “Palo Alto Networks just seems to get it. They know what people are looking for and provide the products that meet those needs. That’s all you can ask for in a vendor.”