Case Study: Raymond James Financial

Global Financial Services Leader Bullish on Palo Alto Networks Next-Generation Firewalls

BACKGROUND

Raymond James Financial (NYSE-RJF) is a Florida-based diversified holding company providing financial services to individuals, corporations and municipalities through its subsidiary companies. Its four principal wholly owned broker/dealers, Raymond James & Associates, Inc., member New York Stock Exchange/SIPC; Raymond James Financial Services, Inc., member FINRA/SIPC; Morgan Keegan & Co., Inc., member FINRA/SIPC (branded as Raymond James | Morgan Keegan) and Raymond James Ltd., member Investment Industry Regulatory Organization of Canada/CIPF, have over 6,000 financial advisors serving 2 million accounts in over 2,500 locations throughout the United States, Canada and overseas. In addition, total client assets are approximately $375 billion, of which approximately $40 billion are managed by the firm's asset management subsidiaries.

Many Users and Offices, All with Sensitive Information to Protect

Not many companies spend nearly a year evaluating every major firewall on the market in a live production environment before choosing a solution, but Raymond James Financial isn't just any company. Moreover, network security isn't just another IT concern for the firm either – it is its top priority.

Raymond James Financial takes security seriously. It must. In the United States alone, 17,000 users access the company's network; many from remote branch offices. On top of this, thousands of its financial advisors do business online as well as from nearly 2,500 locations spread around the globe. With clients entrusting it to manage $375 billion in assets, it's imperative for Raymond James Financial to secure its data.

Vision = Security

Raymond James Financial needed a more modern, robust and scalable security infrastructure than its existing system could deliver to stay ahead of the ever-changing threat landscape, better protect its clients and corporate assets, and to simplify compliance. It also required a solution it could seamlessly roll out and scale to secure all of its remote locations worldwide.

The nature of Raymond James Financial's business, operations and IT infrastructure present specific security challenges and requirements. Compliance, inspecting Internet traffic and firewall manageability are all driving concerns. One primary and backup data center handles all Internet traffic for the firm. In addition, employees routinely access the company's network via personal devices, and remote and unmanned workstations are common. "We have to secure environments for both internal and remote employees, including those who bring their own devices to work," says Andy Zolper, Chief Information Security Officer, Raymond James Financial. "But our default stance is to say 'yes' first instead of 'no,' so we strive to enable access and activity securely."

Zolper and his team of engineers, policy, risk assessment and access management personnel are responsible for architecture, policy, engineering, and strategy regarding security and the privacy of client information. On the engineering side the team handles network security, access management security, content security and incident response.

Inspect to Protect

Compliance is a constant challenge for financial companies like Raymond James Financial. "It's very important for us to centralize data and have very strong network-based controls," explains Zolper. "When you have heavy virtualization, machines with remote management sessions and staff using their own devices, a key strategy to secure them is to inspect traffic going between machines and your data center."

Zolper and his IT staff also need granular visibility in order to inspect SSL encrypted traffic proficiently. **"**We have to inspect outbound and inbound traffic, for data loss prevention, for malicious command and control channels, for viruses, for inappropriate site usage, and for DNS activity that could indicate malware inside the network," he says. "We also need to screen and monitor internal and external applications and social media."

But safely enabling applications and gaining enough insight into encrypted traffic to feel secure isn't easy. It requires superior network visibility.

Making a List

Raymond James Financial developed numerous criteria for the security infrastructure that would help it achieve its objectives. It needed a firewall with granular visibility and extensive functionality that was easy to manage and deploy widely. It had reservations about finding what it desired. "Our engineering team identified our biggest challenge as finding a solution powerful enough for us to apply its higher level controls for data loss prevention, virus inspection, content and user activity monitoring, as well as for low level data packet inspection," Zolper says. "Our concern was that turning on all these advanced functions would cripple some of the boxes. We had to find a firewall with formidable hardware matched by an equally robust software platform to be able to do everything we wanted at the scale needed for our network."

The second major selection criterion for Raymond James Financial was manageability. "Ensuring the firewall could easily scale to manage numerous remote machines at our remote branches as our rollout further progressed was important," says Zolper.

A Full Year of Live Vendor Trials Begins

The Security Engineering team began their search for the ideal security solution on the Internet. "The team reviewed new technologies and infrastructure from vendors that met or claimed to meet our requirements," Zolper says.

But Raymond James Financial wasn't about to entrust the $375 billion in assets it manages for clients, and the company's sterling global reputation, on a sweet sounding sales pitch and a controlled vendor demonstration. "Lab evidence of a given firewall's higher level functionality and a trial run on demo applications would not suffice," explains Zolper. "The team wanted to actually see it perform in production on our network with our network traffic and applications, so it took a long time to find the right solution."

Indeed. Raymond James Financial devoted nearly a year to putting every major firewall vendor to the test. Its painstaking process and patience paid off when it tested the Palo Alto Networks PA-5000 Series next-generation firewall on its network.

Palo Alto Networks next-generation firewalls enable unprecedented visibility and granular policy control of applications and content – by user, not just IP address – at up to 20Gbps with no performance degradation. They isolate and protect data through security policies that are based on the user or group identity from within Active Directory. The user and group identity is then tied directly to a specific application, and the application can then be inspected for threats and unauthorized data transfer. Palo Alto Networks firewalls accurately identify and control applications – regardless of port, protocol, evasive tactic or SSL encryption – and scan content to stop threats and prevent data leakage. This level of granular control is unmatched by any firewall solution on the market.

"Actually seeing how well the firewall performed in our production environment, and the ease with which we were able to set up and run our policies on our network in just one day, really sold Raymond James on Palo Alto Networks," says Zolper.

The PA-5000 Series gives enterprises complete visibility and control, while significantly reducing total cost of ownership through device consolidation. The firewalls enable enterprises to extend protection over all types of traffic, applications, and threats to remote users. Palo Alto Networks safely enables applications, instead of the block-or-nothing approach offered by traditional port-blocking firewalls.

A Sound Investment

Impressed by the performance of Palo Alto Networks, Raymond James Financial purchased and installed 41 of the firewalls at its data centers: six PA-5060s, 21 PA-5050s, eight PA-5020s and six PA-200s. It also installed Panorama, Palo Alto Networks' centralized security management system. Panorama provides global, centralized control over a network of Palo Alto Networks firewalls including logging, reporting, policy management and all aspects of devices and/or virtual systems under management.

The Palo Alto Networks next-generation firewalls are providing everything Raymond James Financial sought, including the superior network visibility necessary to better manage compliance, efficiently inspect and monitor traffic and safely enable applications and access for personal devices.

"We have activated all the functionality built into the PA-5000 Series platform and are very pleased with its performance," says Zolper. "When it comes to Palo Alto Networks, the marketing information is in perfect agreement with what the product delivers on the network. From evaluation to implementation, it has scaled as planned. This is the most positive experience I've seen when implementing a platform of this nature."

The PA-5000 series will also deliver savings to Raymond James Financial. "Consolidating multiple tools on the network into one single product and one vendor will drive down operational costs as our staff only has to learn one platform and management interface," explains Zolper.

The support from Palo Alto Networks also stands out. "Support is available when needed, and anything escalated to engineering has been turned around very quickly to meet our unique needs, of which we have a few due to the legacy applications we run," says Zolper.

Zolper is confident Raymond James made the right decision. "The fact we chose Palo Alto Networks after conducting such an extensive live trial of vendors speaks volumes about the advanced nature and performance of their firewalls," states Zolper. The firm plans to add even more Palo Alto Networks boxes in the near future to accommodate anticipated growth.

Raymond James Financial got all the functionality and performance it wanted in one Palo Alto Networks firewall. "We're very happy with our purchase of Palo Alto Networks solutions," says Zolper. "I am very impressed. For us and for companies with similar data security, performance, and supportability requirements it is absolutely the right solution. "