Royal Air Forces Association

CASE STUDY

RAF Charity Securely Serves Members of the Royal Air Force and Their Families, Protected Against Cyberthreats by Palo Alto Networks Security Operating Platform

ROYAL AIR FORCES Association

The charity that supports the RAF family

"Like everything else from Palo Alto Networks, Traps just works .... Traps brings us significant cybersecurity awareness and protection at the endpoint, which is tied neatly together with the next-generation firewall and WildFire threat analysis service. Having all these capabilities on one integrated platform allows us to apply a consistent high level of security across our entire organization."

Darren J. Bisbey | Infrastructure and Security Manager | *Royal Air Forces Association*

INDUSTRY
Nonprofit

CHALLENGE
Enable unimpeded access to business applications and network services while securing personal information and protecting against cyberthreats.

ANSWER
Palo Alto Networks® Security Operating Platform to automatically prevent successful cyberattacks from the data center to endpoints and the cloud, while strengthening visibility and control to allow applications and user access based on business need.

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

APPLIANCES
PA-3020 (2), VM-300 (1), PA-220 (1), PA-200 (1)

RESULTS
- Prevents successful cyberattacks automatically
- Ensures consistent network security from the data center to endpoints and the cloud
- Improves employee productivity through selective content filtering
- Controls traffic and user access based on business need
- Simplifies network security through an integrated, platform approach

Customer Overview
The Royal Air Forces Association is a membership organization and registered charity which supports serving and former serving members of the Royal Air Force and their families – the RAF family. Formed in 1930 with just a handful of members, and honored with Royal patronage since 1936, the RAF Association today has more than 72,000 members and a network of over 400 branches, providing a wide range of charitable services that aid the comfort, comradery and welfare of members of the RAF family in need across the U.K. and around the world.

Summary
As a trusted charity the RAF Association requires strong security to protect the privacy of its members, some of whom belong to the royal family. However, after many years focused on building its services to address the special needs of the RAF families, the association's network security infrastructure had not been upgraded to defend against modern cyberthreats. Its legacy firewall lacked visibility and control, and sophisticated malware was slipping by its traditional antivirus software. To address this situation, the RAF Association replaced its previous security infrastructure with the Palo Alto Networks Security Operating Platform, with the Next-Generation Firewall deployed in its data center and Microsoft® Azure® public cloud. The association also extended next-generation security to its remote users with GlobalProtect™ network security for endpoints and locked down its endpoints with Traps™ advanced endpoint protection. This integrated, platform approach ensures consistent, strong security at all points in the organization, automatically preventing successful cyberattacks while enabling users to access the applications they need without being exposed to questionable content or distracted by inappropriate websites.

Protecting the Reputation of a Trusted Charity
Whether they are actively serving or long retired, members of the Royal Air Force and their families have sacrificed much in service to their country. When these honorable people find themselves in need – whether it be for personal advice, financial support, medical or mobility assistance, or simply to have a fellow veteran to talk with and share memories – the RAF Association is there to help.

Headquartered in Leicester, England, the RAF Association has more than 400 branches spread across the U.K. and around the world. Across the UK in 2017 the association carried out more than 115,000 welfare contacts, calls and visits, helped tell thousands of bedtime stories to children whose parents were away on operations, and gave tailored holidays to 2,500 RAF veterans, widows and family at its Wings Breaks hotels. Support ranges from simply providing conversation and friendship to preparing and submitting application forms for financial assistance.

Darren J. Bisbey, infrastructure and security manager for the RAF Association, has seen the good work of the organization up close, and it's an inspiration for him every day. "As I've been out traveling to the different areas we serve, I've met veterans who actually flew Spitfires in World War II. They did such

"From an IT perspective, you need to enable users to do what they need to with the least amount of resistance. But I need to make sure they can do that with the maximum amount of security. With the Palo Alto Networks Security Operating Platform, I get that balance with the comfort of knowing our network and our users are protected."

Darren J. Bisbey | Infrastructure and Security Manager | *Royal Air Forces Association*

amazing things, true acts of heroism, and yet remain so humble. You just want to do anything you can to support them."

Darren plays his part by ensuring the RAF Association has a reliable, secure information and communication infrastructure to serve members efficiently and effectively. This includes protecting the privacy of its members, and preventing cyberthreats from luring staff members onto malicious websites or victimizing them with ransomware.

"Our reputation as a trusted charity could be at risk if we were breached and private data got leaked," notes Darren. "Considering the possibility of threats from terrorist organizations trying to target high-value individuals amongst our members, we really have to have everything tied down."

Network Security Advances to the Next Generation

Prior to Darren coming on board in 2014, the RAF Association had a fairly flat network with minimal security controls. The organization had a WatchGuard firewall, which did some content inspection; but as Darren points out, it was clunky and lacked any degree of detailed visibility and control.

Having had previous experience with Palo Alto Networks, Darren wasted no time recommending to management that the RAF Association invest in the Palo Alto Networks Security Operating Platform. Initially deploying a PA-500 next-generation firewall, Darren upgraded after one year to a pair of PA-3020 next-generation firewalls in a high availability configuration located in the association's primary data center in Leicester.

"I love the approach Palo Alto Networks takes toward network security," says Darren. "I'm really sold on the whole ecosystem and the fact that it just works."

A true devotee, Darren even has a Palo Alto Networks next-generation firewall protecting his home network. "If you can have the best protection for your personal data, why wouldn't you?" he suggests.

Darren also had to look at the association's nine regional areas and three hotels, each with its own network domain and no central control. To address this situation, Darren first consolidated all the other sites under the association's central domain, and then brought them into a single point of security by deploying a virtualized next-generation firewall in Microsoft Azure. Today, the regional sites and hotels connect through the Azure cloud for secure access to business applications, communications and the internet with the same level of protection as if they were in the main headquarters.

Increased Visibility and Control

With the Palo Alto Networks Security Operating Platform, Darren and his team have granular control to allow or disallow traffic and limit user access to selected content. This adds a level of protection and flexible control well above the association's previous security infrastructure. Darren relies extensively on App-ID™ and User-ID™ technology for this.

"Being able to create specific rules for certain groups of users has been a lifesaver in a lot of ways," Darren remarks. "For example, the trading arm of our business is not permitted to use SharePoint. So instead of killing all their SharePoint accounts, I used App-ID and User-ID to block those users from accessing SharePoint. I can turn on or turn off access to apps in an instant."

Conversely, if users come to Darren about an application they want to use, but it's been blocked, ICT can evaluate the business case and potentially make an exception. "We assign a value of 1 to 5 to every application. If the App-ID is 1 to 3, it's considered sanctioned and allowed. A Level 4 application will be discussed with Senior Management, and if the users make a good case, we can allow it. But it's case by case. Anything at Level 5 is automatically blocked."

The ease of creating rule sets to handle complex user- or application-specific security requirements saves Darren a lot of time and hassle. "Having an easy-to-see list of rules is awesome, but then being able to instantly hop directly over to the monitor and see how a rule affects behavior is priceless. Finishing off the policies nicely with a 'Deny All' means I also capture everything not permitted by any previous rules."

Beyond these controls, Darren takes full advantage of Threat Prevention and URL Filtering to lock down the association's network to prevent successful cyberattacks. He uses URL categories to ensure the general members of the staff have access to the online resources they need to do their jobs but can't go on entertainment sites or social media that could detract from productivity. Where warranted, he extends additional permissions to select users who require access to otherwise questionable sites, such as gambling sites, which may be necessary in addressing RAF family problems.

Meanwhile, Threat Prevention simply runs in the background, stopping cyberthreats in their tracks. "What I really appreciate about Threat Prevention is that it does exactly what it says," Darren notes. "It finds all the nasties without me having to worry about it. It just sits there and does what it needs to do."

> "All of our laptop users have Palo Alto Networks GlobalProtect, so wherever they go, they have the same level of security as if they're connected directly to our network. If somebody uses the free Wi-Fi at a coffee shop, it's not hard for a hacker to spoof the connection, and all of a sudden you have a man-in-the-middle situation where all your data is seen ... GlobalProtect prevents this from happening by automatically connecting remote users to a next-generation firewall."
>
> **Darren J. Bisbey** | Infrastructure and Security Manager | *Royal Air Forces Association*

An especially important capability for Darren is SSL decryption, which unmasks encrypted traffic so Threat Prevention can be applied to it. SSL decryption ensures that even encrypted traffic is subjected to complete packet-level inspection, allowing integrated WildFire® malware prevention service to then identify and block any potential threats.

"Having decryption look inside emails before they hit our endpoints gives you that warm fuzzy feeling because you know they've been properly inspected." He adds, "We have a very small IT team, so having something that sits in the background and does all the work is a big win for us. I don't have time to babysit a firewall."

Darren acknowledges that, with any critical environment, device monitoring is a necessity. However, unlike many other approaches, the Palo Alto Networks platform provides a single pane of glass for monitoring and controlling the entire network security infrastructure without tediously examining one device at a time. "Compared to other platforms I have seen, the Palo Alto Networks platform really makes cyber life easier," he declares.

Extending Next-Generation Security to Remote Users

Darren's approach to securing the RAF Association reaches into every corner of the organization, including end user devices and data center servers. For example, he uses GlobalProtect to extend all the protections of the Palo Alto Networks Security Operating Platform to remote users and mobile devices, such as smartphones and tablets.

"All of our laptop users have Palo Alto Networks GlobalProtect, so wherever they go, they have the same level of security as if they're connected directly to our network," Darren explains. "If somebody uses the free Wi-Fi at a coffee shop, it's not hard for a hacker to spoof the connection, and all of a sudden you have a man-in-the-middle situation where all your data is seen, and the user is completely unaware. GlobalProtect prevents this from happening by automatically connecting remote users to a next-generation firewall."

Darren also says he is planning to make GlobalProtect a standard on all the association's mobile devices. He points out that any time someone uses their smartphone to access a website, their IP address may be different because it's assigned dynamically based on the nearest cell tower. What's worse, those user IP addresses are often sold by the service provider and can be correlated with an individual's personal and financial data. GlobalProtect eliminates this problem.

"Extending GlobalProtect to our mobile devices was a natural progression for me," says Darren. "It solved the problem of exposing IP addresses and brings all mobile traffic into a secure tunnel that's protected against spying eyes."

Advanced Protection From Core to Endpoints

Another vital aspect of securing the RAF Association is advanced endpoint protection provided by Traps. According to Darren, traditional Microsoft antivirus software was simply not effective, and other endpoint protection point products proved too clunky and required a lot of hands-on administration. But Traps was different.

"I researched Traps and saw how it used behavioral characteristics rather than just signatures to identify threats," Darren recalls. "That made a lot of sense. I also liked that Traps has a small footprint and requires very little management."

Today, the RAF Association has Traps cloud-delivered endpoint management service from Palo Alto Networks protecting its endpoints and servers. With the next-generation firewalls preventing successful cyberattacks at the perimeter, Traps is a last line of defense against other threats, such as phishing exploits or email attacks. Consequently, the legacy antivirus software has since been retired – and Darren is delighted with the results.

"Like everything else from Palo Alto Networks, Traps just works," Darren declares. "It sits there monitoring everything coming through the endpoints and alerts us of anything suspicious – usually an executable. Traps brings us significant cybersecurity awareness and protection at the endpoint, which is tied neatly together with the next-generation firewall and WildFire threat analysis service. Having all these capabilities on one integrated platform allows us to apply a consistent high level of security across our entire organization."

Darren continues to look for other ways to leverage next-generation security capabilities from Palo Alto Networks. He's considering Aperture™ SaaS security service to secure the association's Salesforce® and Microsoft Office 365® cloud applications. Darren has also successfully used MineMeld for aggregating and sharing threat intelligence, and he intends to deploy it in production in the near future. In addition, he is evaluating how Panorama™ network security management will further enhance visibility and control while simplifying administration.

Darren concludes, "For me, it's really about making sure people can do their jobs. From an IT perspective, you need to enable users to do what they need to with the least amount of resistance. But I need to make sure they can do that with the maximum amount of security. With the Palo Alto Networks Security Operating Platform, I get that balance with the comfort of knowing our network and our users are protected."