AAA Washington

At a Glance

- Turned to Darktrace for protection against novel cyber-attacks
- Built trust in AI decision-making and moved to fully autonomous model
- Benefitted from continued protection throughout shift to remote working

American Automobile Association (AAA) Washington is a privately held member association and service organization that has provided road, travel, and insurance services for over 100 years.

Protecting the Environment with 24/7 Response

AAA Washington is continually examining its capabilities to address risk in the organization. A few years ago, the organization looked to reduce a risk had in their security monitoring. In essence, AAA Washington only actively monitored for malicious activity during typical working hours and had minimal capabilities to respond to a cyber security event during off-hours.

"We looked at what we could do to fill that gap," said Ron Nichols, Senior Information Security Analyst at AAA Washington. "Although we were advised to engage a managed service SOC, we saw many drawbacks. We knew that we would be competing for priority with other clients of the SOC provider, but we were skeptical of the extent to which the provider's technicians would ever completely understand our environment."

"Once we saw Darktrace, it was a no brainer to go that route. It was simple to deploy, effective in our needs for monitoring and resonse, and it provided us with a single pain of glass where I could see all the information I needed and investigate activity."

> "Darktrace was simple to deploy, effective in our needs for monitoring and response, and provided us all the information we needed."
>
> Senior Information Security Analyst, AAA Washington

AAA Washington

Building Trust in Autonomous Response

AAA Washington implemented Darktrace, with Autonomous Response initially set in Human Confirmation mode, where its actions must be first approved by the security team. In the first week of deployment, Darktrace provided the information security team with insight into activity they were not aware of. For instance, it revealed that every other night their back-up solution was shipping significant amounts of data to the vendor's datacenters.

"We thought we knew our environment, but Darktrace provided insight into aspects of our network that we weren't aware of, and added to our knowledge base about what was going on."

As the AI built a more comprehensive picture of AAA Washington's digital estate and the accuracy of its recommendations improved, the security team entrusted the technology to take autonomous actions in certain areas of the digital environment. For over two years, Darktrace has not taken an autonomous action that was undesirable, which has continually increased the organization's trust in autonomous action.

Darktrace's Threat Visualizer

Adapting to the Business with SaaS and Endpoint Coverage

As AAA Washington moved into a hybrid cloud environment, the security team feared losing the level of protection and visibility their on-premises Darktrace solution had given them. In response, the security team utilized the SaaS Modules for Microsoft 365 and other cloud platforms. With deploying this capability, AAA Washington has realized the same visibility and protections in its cloud environment as it enjoyed and relied upon for its on-premises systems. The security team is able to effectively monitor and respond to suspicious and malicious activities on a 24/7 basis, even as the business computing environment shifted.

One of the outcomes of the pandemic was the move to remote work for all of AAA Washington's workforce. This also meant that the monitoring capabilities that the security team had were diminished as many workstations were not coming into the VPN for on-premises resources. AAA Washington needed to strengthen its endpoint protection in this environment and the security team turned to Darktrace for Endpoint. This capability extended the coverage of Darktrace's Self-Learning AI to cover these remote devices, protecting remote workers from threats like data loss and ransomware with an additional layer of visibility and targeted action.

> "Darktrace has filled the need we had in 24/7 monitoring and response and adapted in its capabilities to provide us protection."
>
> Senior Information Security Analyst, AAA Washington