Redjack

Government Agency Improves Network Visibility

Improves network performance and blocks illegitimate activity

INDUSTRY	PARTNER	ASSET COUNT	CUSTOMER SINCE
US Federal Government	**Telecommunications**	**> 8 million**	**2016**

CUSTOMER CHALLENGE

Network Visibility on a Massive Scale

This US Federal Government customer has a larger network than most nation-states, so they needed a solution that could handle a massive amount of data while providing valuable insights. Traditional network visibility solutions couldn't scale far enough to handle the demand, and they weren't able to provide the deep analysis into the causes and interdependencies of network traffic needed to create actionable recommendations.

Why Redjack

Redjack started in government services and continues to provide solutions to the community. Redjack's intimate knowledge of the customer's mission and operations—combined with our understanding of the desires and challenges of net defense operators—made us an optimal choice.

Redjack installed sensors that process the traffic flowing to and from the organization, then output network communications data that is fed into the organization's network forensics platform.

The records Redjack provides allow our partner and our customer to block traffic from sources without a legitimate need to communicate, unclogging the customer's gateway and enabling its network to function more efficiently. Redjack also aggregates the data in a way that no longer precludes it from analysis. This is important because having the ability to analyze network traffic in its entirety enables the organization to detect and block threats at the earliest possible stage of the cyber kill chain.

Business Results

Scalable, High-Capacity Performance

As most sensors are unable to handle the volume of communications passing through the organization, it was important to our partner that Redjack's sensors could capture everything. Redjack does this by summarizing the scan information, providing a single record that reflects many scans instead of an individual record of each scan. This creates scalability that enables us to successfully process the organization's high volume of traffic while simultaneously providing a complete record of it.

Beyond Network Visibility

Because of its size, the customer receives a large amount of internet traffic that is not relevant to the customer. By leveraging Redjack's filtering capabilities, our partner and the customer are better able to determine which traffic is important. Redjack's sensors detect illegitimate activity by looking for communications that don't transact information and then filter them out of the data set.

Among the illegitimate activity we detected were high-volume scans being executed once a day. Further analysis revealed that a nefarious company was behind this. Because they were periodically breaking the customer's network with their scanning, we recommended that the partner block all communications with them.

After eliminating high-volume scanners more than half of the incoming traffic that remained was in the form of illegitimate reconnaissance or distributed scanning—people using botnets to spam connections until they clog and stop working.

Side Note: Botnets are groups of internet-connected devices that a threat actor remotely controls without the owners' knowledge in order to perform malicious tasks.

After detecting illegitimate activity, Redjack's sensors aggregate it in a way that enables the data to still be analyzed, whereas previously communications that had been filtered out or blocked were excluded from analysis entirely.

Conclusion

Because of Redjack's history and reputation with government services, this customer decided to work with Redjack to help them understand the difficulties they were having with their network traffic. Gaining visibility into and an understanding of their network traffic enables the customer to be able to better analyze it and perform threat detection, ultimately improving their cybersecurity posture while avoiding unnecessary costs.

About Redjack

Redjack delivers total asset visibility and AI-powered business insights for cyber resilience. Our platform empowers enterprises to safeguard vital business functions, meet cyber regulatory standards, and digitally transform to align with business objectives.

Visit redjack.com

Redjack