GOVERNMENT CASE STUDY

When no news is good news: avoiding security breaches

Mention "cybersecurity breach" and the companies that come to mind are Sony, Yahoo, Target, Marriott, Equifax and eBay. These are just the headline grabbers. According to a 2021 report from The Commission on the Theft of American Intellectual Property, "IP theft costs the US economy hundreds of billions of dollars annually and reduces US companies' R&D investment and innovation."[1] While the cost is often thought of in terms of the records compromised, an equal or larger cost is the risk or damage the breach causes for the organization, its insurers and account holders. When a state government's systems are attacked, impacts include citizens questioning the integrity and ability of its leaders to protect them and their information.

At a glance

Industry
State government
Customer
Southern state in the U.S.
70,000+ state employees
1,200+ locations, including: + Multiple cities and counties + State agencies and commissions + K–12 and charter schools + Higher education institutions
Challenges
DDoS attacks
Insufficient bandwidth
Budget constraints
Solutions
DDoS Mitigation Service
Dedicated Internet Services
Point-to-Point (P2P) and Ethernet
Results
Secure network
Geographic redundancy
Increased bandwidth
More cost-effective solutions

A difficult lesson

Knowing you have a problem is one thing. Identifying the source of that problem and deciding what to do about it is another. That was the situation when this southern state began experiencing network outages but was unable to trace their root cause. Responsibilities for resolving the issue fell to the information services agency—a team of 200+ individuals who provide management and oversight of the state's network infrastructure and the state data centers. Network departmental functions are divided between two groups with one responsible for the state network including voice and data services, while a separate group manages network security.

As a long-time customer of Windstream (dating back to the late 1990s when they procured Centrex service for the state's phone system, adding Internet services in 2014), the relationship has weathered many changes in networking, such as migrating from frame relay/ATM to Ethernet technology. Many changes drove prices for transport and Internet services down that, in turn, helped the state keep technology costs low.

However, when the Windstream Enterprise Network Operations Center (NOC) that monitors the state's circuits began noticing distributed denial of service (DDoS) attacks against their network, it didn't take long to realize that their agency budget—funded entirely by the agencies they serve—was no match for the potential losses they would incur if the problem wasn't solved immediately.

"In addition to educating the agency about how DDoS attacks impacted our network, the Windstream Enterprise team demonstrated how threats could be alleviated simply and easily by the addition of DDoS Mitigation Service."

"Improve our cybersecurity performance"

As one of the agency's publicly stated goals, the irony was lost on no one when the cybersecurity event became a reality for the agency. They had suspected network issues, but were unable to detect how many attacks they experienced. Fortunately, Windstream Enterprise immediately met with the agency to report what they detected and the severity of the situation. According to the Director, "In addition to educating our agency about how DDoS attacks impacted our network, the Windstream Enterprise team demonstrated how threats could be alleviated simply and easily by the addition of DDoS Mitigation Service." Because the department is dependent on the agencies they serve for every dollar of budget, (vs. state general funds) they are very cost-conscious. So, while they knew they needed a DDoS Mitigation Service to protect the network, they had to figure out how to get the budget to pay for it.

A safer and more cost-effective network

The decreasing cost for bandwidth played to the agency's advantage. In addition to mitigating DDoS, the agency knew they had to increase bandwidth to efficiently carry a growing amount of network traffic.

When they went out to bid for the K–12 network, their goal was to meet the FCC minimum goal of 100 Kbps per student. By the time they included staff in the K–12 user count, they were able to afford 200 Kbps/user, and they ended at 90 Gbps of Internet divided into 30 Gbps each at 3 different locations. Because costs had come down so much, when they went out to bid for the non-K–12 network they also asked potential vendors to bid an option for DDoS service.

Windstream Enterprise came through with a very attractive bid that helped the state realize that DDoS mitigation was within reach. "We were immediately interested and impressed by the proposal. Once the contract was awarded, we couldn't believe how quickly the solution was installed, how well the service works and the ease of using the DDoS service portal." Today, the state remains very pleased with their DDoS Mitigation Service. The service has helped them discover additional threats and has prevented others. Thanks to Windstream Enterprise DDoS Mitigation Service, "improve our cybersecurity performance" has become more than a goal. It has become a reality.

Cloud-enabled connectivity, communications and security—guaranteed.

"We were immediately interested and impressed by the proposal. Once the contract was awarded, we couldn't believe how quickly the solution was installed, how well the service works and the ease of using the DDoS service portal."

1. IP Commission 2021 Review. The IP Commission (March 2021).

To learn more, visit windstreamenterprise.com

WINDSTREAM ENTERPRISE