COMPANY

FEDERAL GOVERNMENT SYSTEMS PROVIDER

INTERVIEWED

DIRECTOR OF IT

CASE STUDY

IoT Secure™

“IoT Secure saved me weeks worth of time on not only on the initial device inventory and monitoring set up, but from doing periodic updates.

This gave me more time to focus on delivering IT value to the organization.”

Director of IT - Federal Government Systems Provider

IoT Secure Solution

IoT Secure's solution was instrumental in addressing these challenges:

The solution was deployed rapidly, in less than 1 hour, without network TAP/SPAN ports or agents. In addition the IoTSA easily handled all their locations with one single appliance.

Next, the IoT Secure solution profiled all the devices on the network to give the I.T. director full visibility into what was on the network, identifying devices by device type so he could make decision about what to remove from the network, as well as what stayed and to which VLAN segment it should be assigned.

After that, IoT Secure continuously and safely checked devices for vulnerabilities and automatically monitored devices for anomalous and malicious communications without any tuning required.

This gave him a near real-time view and alerting into devices at risk, as well as information on how to resolve the issues.

Finally, the IT director saved weeks’ worth of time on not only on the initial device inventory and monitoring set up, but also on the periodic updates that would be needed so he could spend more time delivering IT value to the business. In addition, the IT Director now had an easy evidentiary deliverable in support of his company’s roadmap to CMMC compliance.

IoT Secure™

sales@iotsecure.io | 1.404.260.7405 | www.iotsecure.io

Company Overview:

Company is a trusted computing innovator providing cybersecure, tactical edge computing solutions to the defense and aerospace industries.

Established in 1989 and headquartered in Atlanta, Georgia, the company is a pioneer of made-in-USA computing solutions and has endured firmly and unwaveringly at the forefront of the high-performance computing industry for more than 30 years, designing, manufacturing, assembling, testing, and supporting customer-driven rugged computers that accelerate and underpin the world's mission-critical programs, applications, and critical infrastructure processes.

Company manufactures and provides customized rugged servers, workstations blade servers and storage solutions.

The Director IT had these:

Compliance:

The IT Director receives a weekly report on asset inventory and any potential vulnerabilities so that the IT director would have a report ready to provide to any 3rd party auditing organizations as part of meeting the Cybersecurity Maturity Model Certification (CMMC) requirements mandated by the Department of Defense in order to become a DoD vendor.

Visibility:

He wanted to make sure that there was full visibility into exactly what devices were connected to the network and where they were physically located. This was especially important for identifying any shadow I.T. so it could be safely removed from the network. Additionally finding unmanageable devices so he could know what to secure and to assist in developing action plans to secure them. In particular, employees that are building rugged servers or testing other equipment would connect those servers and equipment to the production VLAN rather than to their internal testing VLAN. Our IoT Secure Security Appliances allows him visibility on whenever anyone had done so and also enabled him to enforce his policy that any new server being built should not be connecting into the production VLAN but instead connected to their test VLANs.

Security:

He also needed to know what devices caused security risks in the network as soon as possible. This included continuous vulnerability testing, device monitoring, and segmentation, as well as understanding the path to resolution to mitigate threats. Of particular interest for him was looking at the devices that were at-risk. That immediately alerted him to focus on those devices and take the steps necessary to resolve those vulnerabilities found on those at-risk devices.

IoT Secure™

sales@iotsecure.io | 1.404.260.7405 | www.iotsecure.io