Automotive

ISSQUARED

Case Study

FortiNAC

ABOUT THE CUSTOMER

The company referenced in this case study is a leader in the automotive and industrial fields. It provides products to the Automotive, RV, Military, and Industrial markets with multiple locations across the US. Because a portion of the company's revenue comes from direct sales, third-party vendors and guests often visit their various locations.

CHALLENGES

The company had experienced challenges integrating new technology into their network. For example, when processing credit payments, the company's network would not maintain a consistent layout. This was needed to ensure devices were connected to the expected hardware and had the proper access and security. While the company had guests isolated on their network, it didn't have any way to track these guests. Therefore, it could not ensure that the guests were only connected to the Guest WI-FI and not on the wired network or a corporate WI-FI network.

OBJECTIVE

The company was looking for a mechanism to identify each device and user as they connected to the network while also providing relevant access for every device and user id. The company sought to deploy a solution that could identify each device as it joined either the wired or wireless network, which meant the solution needed to register each device based on its unique criteria and place it into a particular VLAN/network. Once a device joined a network, the solution would then selectively ping devices periodically for necessary compliance to ensure the select device/device group continues to meet the requirements. In the event the device did not match the compliance check either during the initial connection or during a periodic scan, the solution will then move that device to an isolation/remediation VLAN (Virtual LAN)/network and notify the user of the steps required to bring them back into compliance.

The company also wanted to ensure that privileged IT devices can connect as desired across the enterprise and as needed for routine IT-related activities. These devices needed to be identified with a unique policy.

TECHNICAL OVERVIEW

The FortiNAC has offered the company visibility and control of all the devices on its network. FortiNAC enables agentless and automated discovery of the devices by assimilating comprehensive data sources, such as RADIUS, DHCP, SNMP, LDAP.

- Leverages standard protocols such as Simple Network Management Protocol (SNMP) and SSH to organize information and secure devices.
- Integrates with Fortinet's Security Fabric for intelligent decisions within the Fortinet architecture.
- Utilizes Vendor OUI, TCP ports, HTTP, DHCP fingerprinting,and other methods to profile a device.

ISSQUARED

SOLUTION

Based on its needs and requirements, ISSQUARED® worked with the company to deploy FortiNAC into its network to overcome the challenges highlighted above. The FortiNAC solution was implemented in a phased approach, beginning with integrating the existing network infrastructure. FortiNAC leverages SNMP and SSH to integrate standard-based protocols that allow FortiNAC to work with many manufacturers. This initial integration has provided visibility into the network infrastructure, allowing the company to understand what devices/users are connecting and all the way down to the switch port or wireless service set identifier (SSID).

Once ISSQUARED® had established this visibility, the team participated in a learning phase to profile devices through a series of tools. ISSQUARED® integrated corporate user machines with FortiNAC's Persistent Agent (PA) through GPO's that allowed FortiNAC to understand these devices based on the PA installed and an internal trusted certificate. The PA scanned these devices, providing regular compliance checking.

When profiling devices that didn't receive the PA, the devices were scanned and identified using methods that allowed the team to identify these types of devices (Printers, Scan guns, HVAC, etc). These methods included TCP ports, OUI, HTTP, and DHCP fingerprinting amongst other methods.

Once the profiles were established, ISSQUARED® defined policies to ensure devices had the required security and domain checks for domain attached devices in place to meet compliance checks. When devices failed the compliance checks (scan), they were moved into a remediation VLAN (Virtual LAN) with instructions to remediate.

The team from ISSQUARED® also assisted the company with leveraging a self-service portal for guests which allowed them to use the guest Wi-Fi/Wired network through a self-service sign-up. This allowed the company to use an AUP (Acceptable Use Policy) with a basic audit trail for compliance for the corporate and guest users.

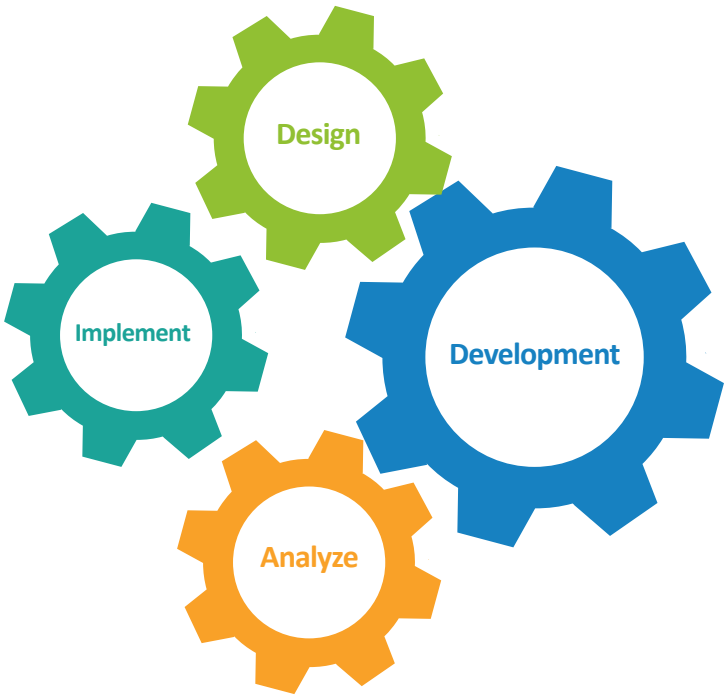
KEY BENEFITS

FortiNAC has provided the company with the ability to control network access and has enhanced visibility. The solution has ensured protection against cyber threats by reducing the threat landscape and providing visibility to administrators who can track connected devices on the network. FortiNAC controls third-party wired & wireless devices and automates responses to varied networking events. FortiNAC's policies are built on the following criteria Who (what user), What (what device), Where (what location, site building, wired or wireless) & When (time of day). Additional benefits are listed below:

Network monitoring & automated response: FortiNAC provides the company, ability to monitor the network continuously. The solution continuously evaluates users and devices as they attach to ensure they match the correct profile. FortiNAC can help identify endpoint risks and automatically organize a response by Fortinet as well as other 3rd party tools. This solution has enhanced the response to the events and helps prevent and mitigate threats before they spread. FortiNAC provides a broad and customizable set of policies for the automation that can instantly trigger configuration changes when the company observes a targeted behavior, leveraging Fortinet's Security Fabric.

Dynamic control of the network: FortiNAC has enabled the company to automate the provisioning and onboarding process for users, endpoints, and guests. Once the devices and users have been identified and profiled, FortiNAC places devices and/or users onto the appropriate access VLAN and the necessary resources. FortiNAC ensures the identity and integrity of endpoints by validating their configuration before they attempt to connect to the network. If the configuration is non-compliant, the device can now be isolated or provided with a limited access VLAN. This process mitigates security risk and prevents the spread of potential malware.

Device visibility across the network: FortiNAC has helped the company to identify and profile every single known and unidentified device. The solution has also enabled the company to detect and identify headless devices connected to the network accurately using multiple behaviors and information analytics. FortiNAC has also provided the company network visibility to discover every device and user using over 20 different techniques. Now that it has been implemented, the solution can profile each element based on observed characteristics and responses.



ISSQUARED®

ISSQUARED® is one of the leading providers of end-to-end IT technology solutions, delivering fine-tuned services across IT Security, Cloud, Infrastructure, Unified Communications, Industrial Operational Technologies and other solution areas. For many years, ISSQUARED® has been helping several Fortune 500 organizations and delivered several multi-million-dollar projects. Our proven expertise takes our clients through a seamless digital and security transformation, resulting in rapid business benefits and positions them for future success.

ISSQUARED® is headquartered in Westlake Village, California, US. It offers global delivery capabilities with its presence across the UK, Ireland, the Middle East, India, Singapore and other parts of the US too.

ISSQUARED

HQ: 2659 Townsgate Rd, Suite 227
Westlake Village CA 91361 USA

+1 805 371 0585
+1 800 779 0587

sales@issquaredinc.com
www.issquaredinc.com