Case Study

FORESCOUT

Ardentec

Ardentec utilizes Forescout to gain real-time network visibility and protection from unauthorized and unsecured devices.

80%
increase in network security compliance

REAL-TIME
visibility of endpoints

100%
traceability of network devices

Ardentec
A testing partner you can trust

Industry
Manufacturing

Environment
4,000 endpoints used by over 1,000 employees across its four manufacturing sites

Challenge
- Ability to manage the growing number of endpoints
- Improve network visibility
- Reduce the risk of rogue and vulnerable devices gaining access to network resources

Security Solution
- Forescout platform

Overview

Chartered in 1999 in Hsinchu, Taiwan, Ardentec, a provider of semiconductor testing solutions in memory, logic and mixed-signal integrated circuits (ICs) to integrated device manufacturers (IDMs), pure play wafer foundry companies and fabless design companies, employs over 1,000 employees and operates four manufacturing sites across Taiwan, Singapore and Korea.

Business Challenge

As one of Taiwan's top wafer test service providers, the Ardentec IT team's goal was to fortify network security to all of its branch locations in order to gain thorough network visibility and reduce the risk of unauthorized and unsecured devices potentially gaining access to their company network. The approach would also demonstrate commitment to network security for their wide range of global customers. Other priorities included gaining 100 percent traceability of network devices, having accessibility to early warning and alerts of rogue devices and unsecured connection events, and having overall stronger operational insight.

Ardentec worked with InfoSource, a Forescout distributor, to assess its needs and to determine the requirements for a network control solution. The team quickly realized the need for an agentless approach to simplify and expedite the effort of managing more than 4,000 of their endpoints and preserving user experience. The firm also needed a solution that would be compatible with a broad array of switches and other existing infrastructure components from different manufacturers. After looking at competitive products, Ardentec settled on the Forescout platform because it met their requirements and offers the most flexible and extensible set of security policies.

Use Cases

- Device visibility
- Device compliance
- Network access control

Results

- Deployment ease due to agentless approach and integration with multivendor switch infrastructure
- A more transparent view of the network with real-time visibility of endpoints
- Increase in the network security compliance rate of ISO 27001 to 80 percent
- Lowered network asset management risk across the company
- Automated compliance enforcement and blocking of rogue devices
- Streamlined validation of IP and MAC address association

Why Forescout?

Ardentec chose Forescout because it provided the simplest, feature-rich and most cost-effective solution that was also easiest to deploy and maintain. The Forescout Platform's effectiveness to provide increased operational insight and its low impact to their existing environment helped in the decision.

The most important reason Ardentec chose the Forescout Platform was for its agentless approach while still allowing for strong policy control. Forescout distinguished itself further by preventing rogue and unmanaged devices from connecting to the network, especially since Ardentec discovered that its users unplug network cables from the factory machines and plug them, instead, into their own devices. Additionally, the Forescout platform offered the interoperability needed to query Ardentec's authorized device database. Leveraging the Forescout orchestration capabilities interface, the Forescout platform checks the IP and MAC addresses of devices attempting to connect to the network to make sure they match — a function only Forescout offered.

> By using the Forescout platform as extensively as possible, not only did we improve our overall network security and visibility, but also the effectiveness of our endpoint security investments.
>
> — Chris Chou, Director of Management Information Systems, Ardentec

Other factors in the choice of the Forescout platform included its use for identifying and controlling mobile devices, automating the process for controlling guest access to its network, range of endpoint compliance capabilities, and dashboard, query and audit reporting capabilities." With the Forescout platform, network control is much easier than we ever imagined," said Chris Chou, director of management information systems for Ardentec." We had the Forescout platform up and running across four sites in less than a month. The depth of visibility into devices connecting to the network is amazing, and its simple integrated approach let us easily manage the entire network from one dashboard."

Business Impact

Compliance

The implementation led to an increase in the network security compliance rate of ISO 27001 to 80 percent and lowered network asset management risk overall across the company.

Asset Classification

Ardentec found additional distinctive uses for the Forescout platform such as dynamic asset classification, an IP-MAC binding and MAC address validation used for factory devices and connections as well as wireless and mobile device security.

The Forescout platform monitors all devices connecting to Ardentec's network to ensure each endpoint has the correct settings, such as up-to-date antivirus and that the operating system patches are current, per the organization's standard security policies.

Real-time Visibility & Endpoint Compliance

The Forescout platform monitors all devices connecting to Ardentec's network to ensure each endpoint has the correct settings, such as up-to-date antivirus and that the operating system patches are current, per the organization's standard security policies.

Guest Networking

Prior to implementing the Forescout platform Ardentec used a manual process for guest access to its network. Today, when a device attempts to connect wired or wirelessly, the Forescout platform verifies it against a list of approved devices. Depending on the device provided, rogue devices may be taken off the network, devices may be automatically diverted to Ardentec's guest network or IT may be alerted to investigate the issue."

By using the Forescout platform as extensively as possible, not only did we improve our overall network security and visibility, but also the effectiveness of our endpoint security investments," said Chou.

Next Steps

Ardentec is seeking to tighten its management of mobile devices. The firm will use the Forescout platform to integrate with its MDM solution to enable stronger policy enforcement and more automated security control in support of its BYOD efforts.

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com