CYLANCE™

Investa Takes on
Cybersecurity

INDUSTRY
Commercial Real Estate

ENVIRONMENT
- 250 endpoints and 150 Windows Servers

CHALLENGES
- Difficulty in maintaining anti-virus signature updates for a highly mobile workforce
- Lack of visibility into malicious activity on endpoints

SOLUTION
- Deploy CylancePROTECT® to protect employees' machines both on and off the network
- Gain visibility into attacks as they happen and their source

INVESTA★

The Company

Investa is one of Australia's largest and most recognized commercial real estate companies. With a focus on prime-grade office buildings in the major Australian CBD markets, Investa optimizes total returns by combining a low-risk investment approach and active financial, leasing, operational and environmental management. The company's integrated management platform allows them to lead the market, and to consistently deliver outperformance for their investors, while exceeding the expectations of tenants and staff.

The Situation

IT Manager Nathan Powell is responsible for ensuring the continued operations of Investa's systems. An eight-year veteran of the Investa IT organization, he oversees a relatively small security team that provides design and implementation enhancements to the company's environment. The team is also responsible for introducing any new systems to the environment.

"We were up and running with CylancePROTECT within a day. The competing product required a week of planning before we could get started with the installation" — **IT Manager, Nathan Powell**

The Process

Nathan's team set out to understand gaps in their environment, evaluate new defense mechanisms, and determine where additional layers of security were needed. As Investa has a significant number of mobile employees, better endpoint security for devices operating off the network was also an important consideration.

According to Nathan, "I found that traditional virus scanners depend on continuous definition file updates and require a device be connected to the network." This is problematic for a company with a high percentage of employees working in the field. In addition, Investa's existing security products provided very little visibility into endpoint threats.

He considered an endpoint security solution from a leading next-generation firewall vendor. The product was more expensive, and required a complex and time-consuming installation. Nathan said, "We were up and running with CylancePROTECT within a day. The competing product required a week of planning before we could get started with the installation."

The Results

According to Nathan, "We have had no incidents since deploying CylancePROTECT, including surviving both the WannaCry and Petra-like Ransomware outbreaks." He attributes this success to CylancePROTECT's algorithm based approach that protects employees' machines, both on and off the network, anywhere in the world. He added, "CylancePROTECT does not require downloading emergency DAT files."

CylancePROTECT also offers a better dashboard and alerting mechanism. "It articulates a far more detailed view than our previous AV," Nathan said. "CylancePROTECT provides an environment-based view where you can see activity about vulnerabilities versus at the device level. For example, the number of attempts by a particular malware as opposed to how many devices it has hit."

As for CylancePROTECT alerts, Nathan said they provide valuable information about malicious activity, including the timing of attack, and its source — such as a USB drive or a file sharing website.

Investa is running CylancePROTECT in auto quarantine mode with great success. Nathan said, "The simplest measure of a quarantine is whether or not you are getting false positives, and we have experienced no false positives."

The Investa security team also noticed a significant drop in CPU consumption required to support AV activities. Endpoint resources required to run CylancePROTECT are significantly less than with the previous AV solution. Nathan said, "Cylance is far more efficient."

Nathan summed up his experience by saying, "Every aspect of the Cylance transition was easy: the deployment was easy. Once deployed, we were able to successfully decommission the previous file scanning solution and get instant feedback on the improvements that were made."