

Background

Australian Aerospace is a subsidiary of the Eurocopter Group owned by the European Aeronautic, Defense and Space Company (EADS), one of the three largest aerospace groups in the world. Eurocopter has become Europe's leading fully-integrated aeronautical group, selling civil and military helicopters and maintenance services all around the world.

The Challenge

Systems Engineer Ben Crewe is responsible for providing support to all of Australian Aerospace's 500+ of IT systems, including servers and networking devices, as well as handling all security within the network. Crewe was dealing with a constant barrage of viruses across his network that his virus scanner could detect, but not stop from running or remove. While the majority of the viruses were non-lethal, they took up expansive bandwidth and significantly decreased user productivity and increased the amount of time Crewe and his team needed to spend dealing with the problem. Additionally, it was a challenge for Crewe to ensure that no company endpoint was running unauthorized software. Users consistently downloaded large programs, including iTunes, and common freeware applications, such as Google Toolbar and Yahoo! Toolbar, that came loaded with spyware and adware or links to the malicious code. Again, this caused major issues for the company's bandwidth and IT availability, as well as introducing additional malicious code to the network, making it vulnerable to attack and data theft.

Crewe needed to devote extra resources and time to manage IT systems, remove unauthorized software and fight rapidly transmitted malware. Crewe was looking for a solution that would not only prevent users from running unapproved applications, but also from using unauthorized USB devices to access corporate endpoints.

The Solution

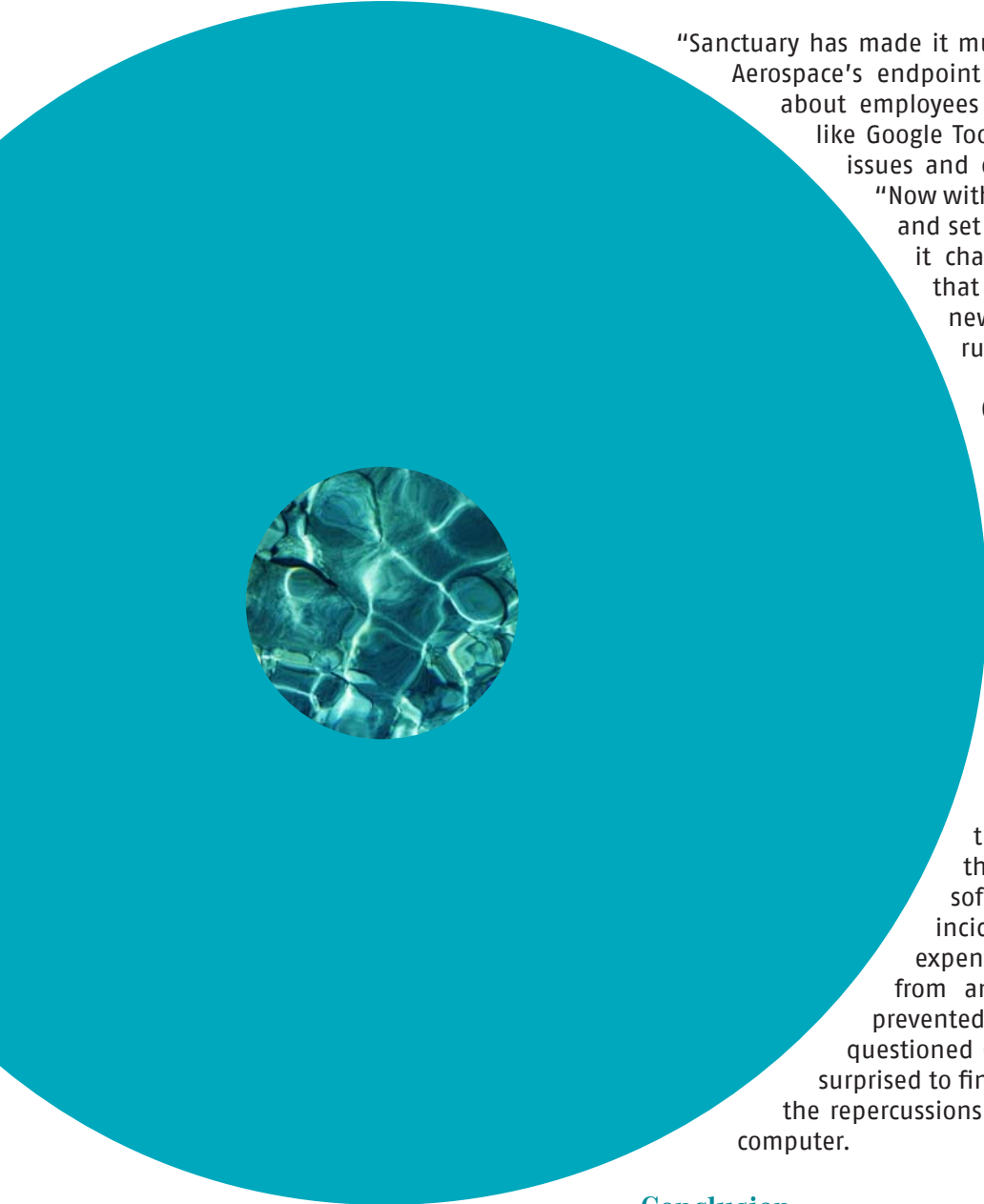
After determining the scope of the problem, Crewe chose the Sanctuary[®] product suite from SecureWave to stop the spread and execution of viruses and unauthorized software. He immediately chose Sanctuary for its high-level security and automatic whitelist feature and its ability to run at the kernel level. With Sanctuary, Crewe would have full control of all corporate endpoints and be able to prevent users' from freely installing applications, as well as ensure that no virus or other piece of malware would ever be able to execute.

SecureWave's Sanctuary utilizes a non-traditional automatic whitelisting approach to stop the threat of removable devices—such as iPods and USB memory sticks—and unauthorized executables—including spyware, worms and Trojans—from accessing desktops, servers and terminals. Administrators can easily manage a centralized list of allowed

devices and executables to deny access by default to anything else that tries to access corporate endpoints. Granular policy rules enable SecureWave customers to enforce flexible usage policies rather than simply prohibiting the use of all devices and applications. For example, administrators can easily set and enforce policies that govern what day or time period a user is allowed to access particular data and can set group policies defining what group of people can use a certain device. Additionally, Sanctuary keeps an intricate log of all user info, recording whenever a user tries to access data or plug in a device, regardless of whether it was accepted or denied.

The Benefits

Sanctuary immediately reduced the number of viruses and non-licensed applications on Australian Aerospace's network and desktops. Crewe finds the whitelist feature extremely easy-to-use and spends only an average one-hour per week on updating the list. Prior to Sanctuary, he often spent several days updating the blacklist and deploying patches.



"Sanctuary has made it much easier to manage all of Australian Aerospace's endpoint systems. I no longer have to worry about employees installing unauthorized applications, like Google Toolbar, which created major bandwidth issues and exposed us to malware," said Crewe. "Now with Sanctuary, once a computer is imaged and set up, we don't ever have to worry about it changing configuration unless we make that change. It ensures that the only way a new device or application is authorized to run is if we approve it. Period."

Crewe also cites quality control as one of the most important benefits he has experienced. "It is a huge relief to know that when we give an employee a PC that we've configured and know how it works that it is going to stay that way because Sanctuary ensures that the user can't install or run anything you don't want them to," says Crewe. "No other product I know has the same level of quality and security as Sanctuary."

Sanctuary not only prevents security threats, but also helps educate users on the dangers of malware and unauthorized software and applications. In one recent incident, a user attempted to install an expensive piece of software that he acquired from an unknown source. When Sanctuary prevented the software from installing, the user questioned Crewe and the IT department and was surprised to find out how much the software cost and the repercussions of having unlicensed software on his computer.

Conclusion

Crewe and his team are continuing to roll out SecureWave Sanctuary to a number of additional workstations and endpoints within its network as the business continues to grow and add new systems are added. Additionally, Crewe and his team are beginning to deploy Sanctuary Device Control across endpoints to prevent the threats posed by mobile devices. Crewe rests easy knowing that no matter how many users try to install the latest version of iTunes or run a corrupt executable, Sanctuary will continue to provide the most effective and proactive security measures available.



SecureWave
Safeguarding Tomorrow

www.securewave.com
info@securewave.com