Malwarebytes

University of Central Lancashire masters malware

The University protects its mobile workforce with Malwarebytes

INDUSTRY
Education

BUSINESS CHALLENGE
Stop malware-related issues on mobile devices

IT ENVIRONMENT
Data center with McAfee antivirus

SOLUTION
Malwarebytes Endpoint Security, which includes Anti-Malware, Anti-Exploit, and the Management Console

RESULTS
- Stopped malware and malware-related complaints
- Achieved insight into malware attacks for developing effective best practices
- Gained peace of mind today and confidence in Malwarebytes protection for the future

Business profile

The University of Central Lancashire (UCLan) is known for its proactive commitment to academic excellence. As a result, the 2015 Centre for World University Rankings placed UCLan in the top 3.8 percent of universities worldwide. When it came to fighting malware, UCLan took the same proactive approach using Malwarebytes.
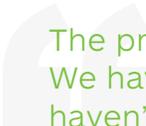
> " The problems—and complaints—just went away. We have far less after-the-fact remediation, we haven't had any ransomware incidents, and I haven't touched Malwarebytes since deployment.
>
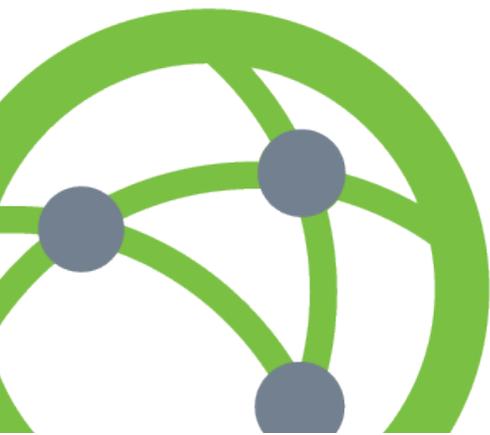> —Gareth Edwards, Technical Lead, Information Services, University of Central Lancashire

Business challenge

Defend mobile devices against malware

With academic partners around the world, UCLan's faculty and lecturers are on the go. That's why UCLan launched its Enterprise Mobility Project, which provides traveling faculty with Microsoft Surface tablets for teaching, meeting, and working abroad and keeps them fully connected to the university. The project launched with 20 tablets and now includes 600. By the end of 2016, UCLan will deploy 1,500 tablets.

However, the existing security scheme wasn't working well for the new mobile devices. Besides the tablets, UCLan has 7,000 Windows PCs for administrative and business users. The PCs run on centralized software, and all have McAfee antivirus running on them. When a desktop PC occasionally experienced malware, the IT team restored it from backup and updated the antivirus.

Malware became a much larger problem when the first tablets were issued. The users had administrative rights, so malware found its way in through downloads and other venues. Lecturers travel the world—to China, Oman, Mauritius, Spain, New York—which increases their vulnerability to malware coming from different sources. Mobile users began reporting poor performance and unexplained interruptions.

"The antivirus wasn't catching malware on the tablets," said Gareth Edwards, Technical Lead, Information Services, University of Central Lancashire. "We didn't want to wait for the problem to worsen, so we added a layer of protection with Malwarebytes. It delivered comprehensive capabilities and zero user intervention."

Malwarebytes Endpoint Security

Edwards and his team deployed Malwarebytes Endpoint Security on the tablets and began monitoring endpoints using the Malwarebytes Management Console. Endpoint Security provides a powerful multilayered defense engineered to defeat the latest, most dangerous malware, including ransomware. It includes Malwarebytes Anti-Malware, Anti-Exploit, and the Management Console in one comprehensive solution.

Malwarebytes Anti-Malware detects and eliminates zero-hour malware, Trojans, worms, rootkits, adware, and spyware in real time. It stops threats in their tracks, eliminating the need for the university to manually remove malware from endpoints. Malwarebytes Anti-Exploit adds four additional layers of protection to block exploits and prevent malicious payloads from being delivered.

Bye-bye malware

After installing Malwarebytes Endpoint Security, the malware stopped. With only three technicians, this was a huge relief. Re-imaging is almost nonexistent, and users don't have downtime.

"The problems—and complaints—just went away," said Edwards. "We have far less after-the-fact remediation, we haven't had any ransomware incidents, and I haven't touched Malwarebytes since deployment."

Hello insight and analysis

"Before we even turned on the Management Console for visibility, we were pretty sure Malwarebytes was working, just based on anecdotal evidence and the fact that users stopped complaining," said Edwards. "Now we can actually see what is happening and how Malwarebytes is working."

Reports and updates show UCLan exactly what is attacking its endpoints. Data analysis enables the team to see user behaviors and identify high-risk activities. They use that insight to develop best practices for user education, infection avoidance, and threat response. "At the risk of sounding utopian," Edwards muses, "we've been able to make the leap from reactive to proactive."

Superior responsiveness

Edwards also reports that when a vulnerability was found and they requested assistance from Malwarebytes, the Malwarebytes Support team took them seriously. "Their response was brilliant," he said. "From the CEO to the field teams, they worked through every step to resolve it with us. Malwarebytes support includes some of the best individuals I've come across."

Peace of mind

Edwards believes that security has become a full-time job for many IT teams, and the threat landscape is daunting. While he says his team's security efforts for the Enterprise Mobility Project are "certainly not voodoo," the team has done very good work and really moved the business forward. Malwarebytes is an integral part of their journey.

"The peace of mind I have is absolutely key to me," said Edwards. "Security on tablet devices is essential and Malwarebytes delivers that. As threats increase, we expect the value of Malwarebytes to continue to prove its worth as it protects us."