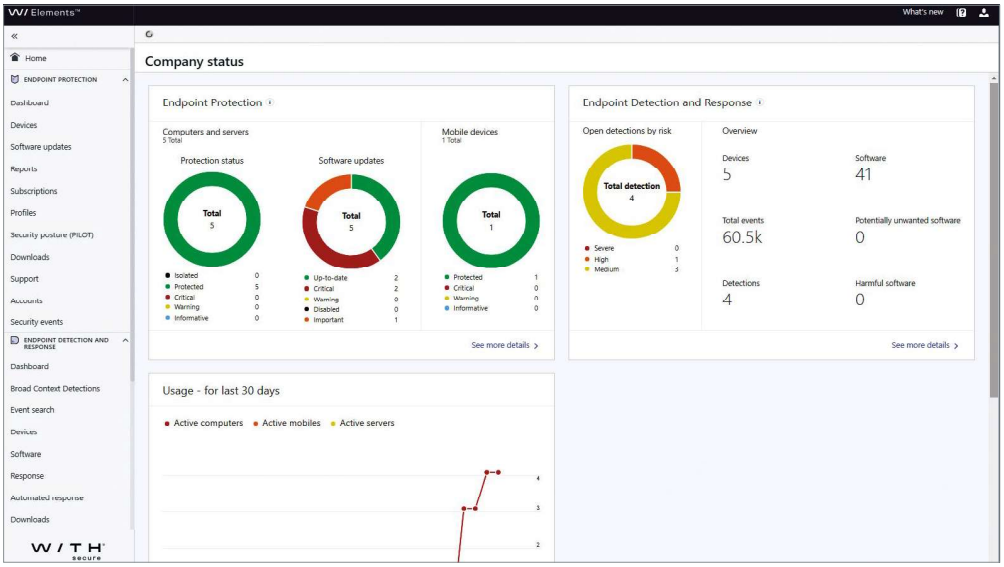
WithSecure Elements EPP and EDR

An affordable cloud-managed solution with smart automated remediation services

SCORE ★★★★★

PRICE 100-499 devices, £37 each per year exc VAT from withsecure.com



Finnish company WithSecure offers a complete suite of security solutions all easily managed from its Elements Security Center cloud portal. Its Endpoint Protection (EPP) module provides a firm foundation and a modular approach allows you to enhance it with other WithSecure components as required.

In this review, we test EPP and take a closer look at the Endpoint Detection and Response (EDR) module. EDR takes a proactive stance on cyberattacks, providing advanced threat detection capabilities, full attack analysis and automated responses for isolating compromised systems.

EPP offers great platform support, too: it protects Windows and macOS workstations, Android and iOS mobiles and Windows and Linux servers, and includes patch management for Windows OSes as standard. Workstation deployment is swift; we used our portal's EPP dashboard to email a download link to users, with the agent taking three to four minutes to install and link up with the portal account.

Protection starts immediately. The agent grabs a predefined profile that enables essential security functions such as real-time malware scanning, a firewall and browsing protection. Customising profiles is simple: you clone the read-only ones provided, tweak their settings as desired and use the devices page to assign them to multiple endpoints.

There's a lot to play with: profiles enforce web protection with a list of 32 URL categories, can stop users interacting with the agent and control access to all kinds of local hardware such as USB sticks, optical drives, and wireless and Bluetooth devices. An EPP Premium subscription enables application controls and WithSecure's DataGuard, which uses behavioural rules to detect potential ransomware activity.

Rollback is a smart new feature that provides instant ransomware protection for Windows systems. It tracks apps classed as unknown and, if they exhibit any dubious behaviour, it closes them down and automatically rolls back all the file and Registry changes they made.

Don't worry if the app turns out to be legit, as all changes are stored in local protected quarantine areas and can be restored by users. It can also initially run in safe mode, where it only reports on unauthorised changes.

ABOVE Automated features include rollback after a ransomware attack

PC PRO RECOMMENDED

"Profiles control access to all kinds of local hardware such as USB sticks, optical drives, and wireless and Bluetooth devices"

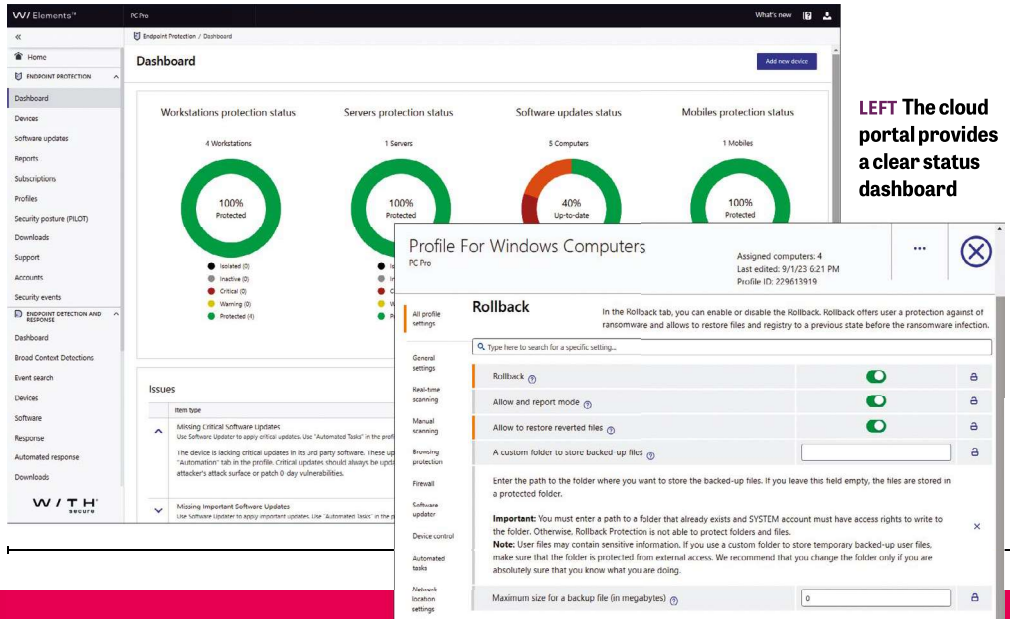
You can keep a close eye on the action using the security events view and set up email alerting for multiple recipients. EPP has fast reaction times: when we introduced malware to our test clients events were posted in the portal almost immediately, with alert messages winging in three or four minutes later.

EDR provides deep analysis of detected threats and uses the same agent as EPP, so adding this module later on automatically activates it for all endpoints. It features WithSecure's broad context detection (BCD), which cuts through alert avalanches by highlighting suspicious events so you can see clearly if an attack is taking place.

BCD shows a filtered view of all detected threats. Selecting one takes you to a threat analysis page, with a process tree showing how the potential malware developed and what it interacted with. If you don't like what you see, you can isolate all affected devices with one click.

An EPP/EDR subscription also enables the new outbreak control feature. The modules team up to track device changes, and if anything occurs to critical areas such as IP addresses and reverse DNS or new malware is detected, a stricter rule is applied automatically to affected devices.

Its high levels of automation make WithSecure a great choice for SMBs that want endpoint protection on a plate. It's simple to deploy, offers a wealth of security features, and all modules are easily managed from the Elements cloud portal.



LEFT The cloud portal provides a clear status dashboard

REQUIREMENTS

Windows 7/Server 2012, macOS 10.15, iOS 14.1, Android 8 upwards, Linux