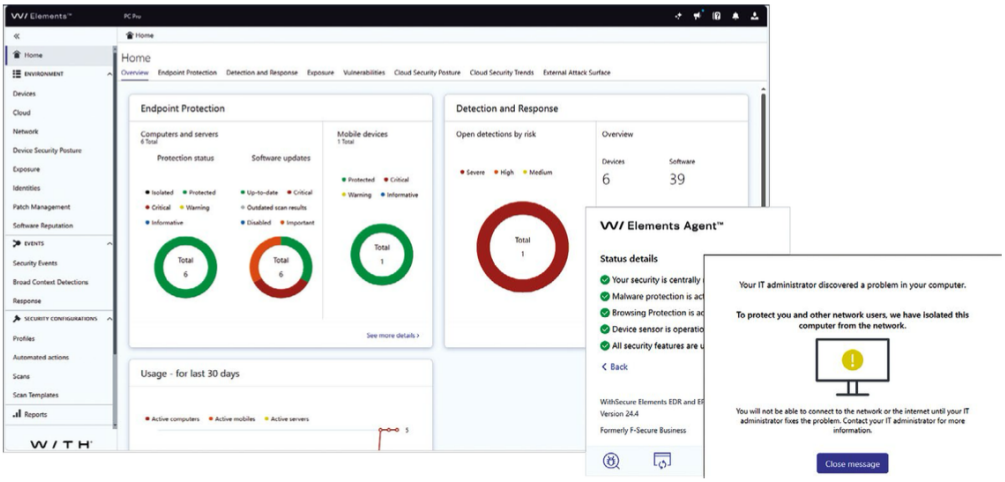
WithSecure Elements Endpoint Security

A top security choice for SMBs, with comprehensive endpoint protection, smart remediation and a good price

SCORE ★★★★★

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



WithSecure offers an impressive range of endpoint protection services, and it's been very busy integrating them all into a single unified cloud portal. Previously, there were separate EPP (endpoint protection) and EDR (endpoint detection and response) modules, but the Elements Endpoint Security (EPS) solution on review amalgamates them together under one extended detection and response banner.

The EPS portal is easy to navigate, and you'll find a lot more new features are in evidence. Accessed from the upper right menu, WithSecure's Luminen delivers AI-powered reporting services and, with one click, presents a detailed summary of security events.

You don't have to search for new features and updates either, as next to the Luminen icon is another one that drops down a list of all the things you need to know about. Platform support is another winner; EPS protects Windows and macOS workstations, Windows and Linux servers and Android and iOS mobiles, and includes patch management for Windows OSes.

For agent deployment, we could email links to users from the portal or download the relevant file and place it in a central location. Either way, it takes around four minutes to install and connect to your cloud account.

EPS provides preconfigured read-only security profiles that are assigned to devices on first contact, so protection starts immediately. We found it easy to create our own by cloning the predefined ones and tweaking them to our requirements.

Profiles manage real-time malware scanning, permit users to run manual scans, determine when automatic updates occur and schedule regular systems scans. Web protection services include reputation-based web page scanning, safe search enforcement, browser plug-ins and content controls with a list of 32 URL categories you can block or allow.

If you're worried about applying new updates to live systems, WithSecure has you covered with a feature that's always been in its profiles: early access to client software. Enable this option in a profile, assign some test systems to it and they'll get all updates at least a week in advance of general release.

ABOVE The BCD feature provides a breakdown of malware activity

"WithSecure's Luminen delivers AI-powered reporting services and, with one click, presents a detailed summary of security events"

Along with controlling access to endpoint removable devices, profiles enable the Rollback feature for instant ransomware protection for Windows systems. Unclassified apps are tracked by EPS and, if they show suspect behaviour, it will close them and automatically roll back any changes they've made to files and the Registry.

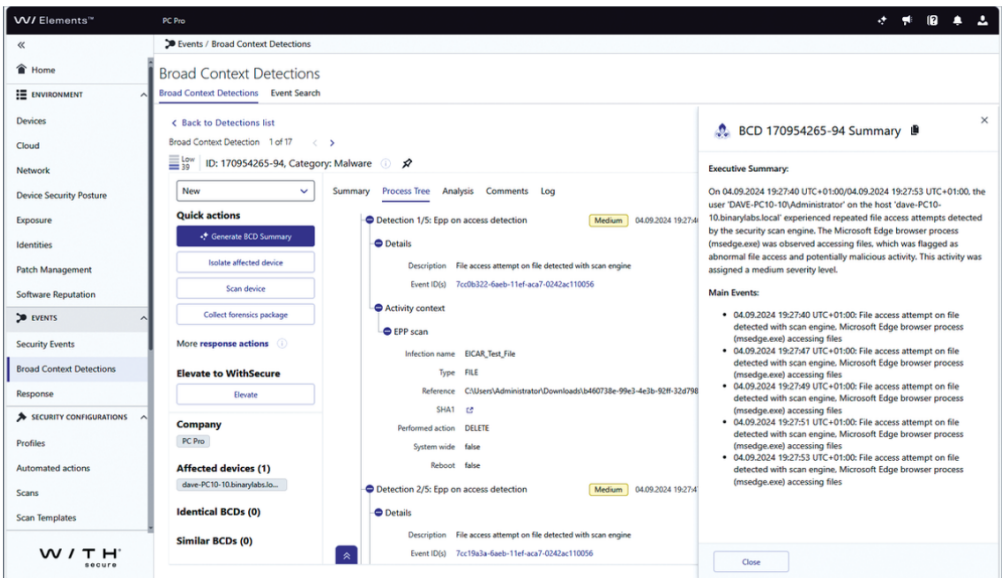
The portal's security events page provides all you need to know about malicious activity and lets you add multiple recipients for email alerts. We tested its response to threats and after introducing genuine malware to our Windows 11 test clients, we received email alerts in four minutes.

WithSecure's BCD (broad context detections) feature presents a filtered view of detected threats with a full analysis and process tree of suspicious events showing how the potential malware developed and what it interacted with. You can see affected systems, isolate them all with one click and, if you need more help, the event can be elevated to WithSecure's security teams.

You may not need to do this as Luminen also comes into play here, generating a summary of the main events and providing advice on remedial actions. Security teams that need a break may appreciate the optional co-monitoring service, where severe threats are automatically escalated to WithSecure's support teams. You can choose out-of-hours or full 24/7 cover.

WithSecure's Elements Endpoint Security delivers an impressive set of protection measures, all managed easily from its cloud portal. It supports a wide range of devices, Luminen provides valuable remediation assistance, and it's great value.

BELOW The web portal keeps you posted on all threats



REQUIREMENTS

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