Cyber Essentials technical controls, checked automatically every week.

A UK organisation with a cloud-first estate deployed Rebasoft, through its managed security partner, to test its Cyber Essentials technical controls continuously across Azure, Intune-managed devices, servers and the network, instead of once a year.

638
assets in scope: network, servers, user and mobile

3
Azure subscriptions discovered

348
unknown assets surfaced in the first report

Weekly
automated Cyber Essentials report

THE CHALLENGE

- Cyber Essentials is assessed once a year, but devices, cloud resources and vulnerabilities change every day.
- The estate spans Azure, Intune-managed laptops and phones, servers and a network in transition.
- A small IT team needed to know where it stood against each control without assembling evidence by hand.

OUR APPROACH

- Rebasoft delivered and supported by a managed security partner, with no agents to deploy.
- Cloud connectors into Azure and Intune, plus agentless discovery of the network and servers.
- Every asset checked against the five Cyber Essentials technical controls, with a scored report sent automatically each week.

WHAT THE REPORT COVERS

Asset inventory
Network equipment, servers, user devices and mobiles, with unknown assets called out.

Unsupported software
End-of-life operating systems and applications that would fail an assessment.

Coverage gaps
Devices that could not be assessed, so nothing is silently missed.

Patching
Critical and high vulnerabilities, highlighting those with known exploits and any past the 14-day deadline.

Secure configuration
Configuration findings per device, plus devices without a host firewall.

Trend over time
Each report shows the change since the last run, so progress can be tracked.

The outcome: Cyber Essentials becomes a weekly measurement, not an annual scramble, with every failing control traced to a named asset.

WHY IT MATTERS FOR CYBER ESSENTIALS

Continuous, not annual
Know your position every week, not just on assessment day.

Evidence ready
Asset lists and findings exported as CSV and PDF.

Partner-delivered
Run for you by your managed security partner.