Vulnerability Scanning

Managed Vulnerability Scanning & Remediation For Endpoints

urban.

DATA SHEET

OVERVIEW

Endpoint vulnerability scanning and application patching is the process of continuously identifying, prioritising, and remediating security weaknesses across your devices and the software they run.

It goes beyond simply updating operating systems, focusing heavily on third-party applications; such as browsers, and everyday business tools, aligning directly with the UK Government's Cyber Essentials framework

HOW IT WORKS?

Daily Vulnerability Scanning

Scans endpoints for missing security updates and vulnerable software versions, detecting weaknesses across operating systems and common business applications.

CVE-Matched Reporting

Each finding is linked to its relevant CVE and severity, providing clear context to understand the risk and prioritise fixes.

Autonomous Remediation

Applies vendor-approved fixes - such as patches, updates, configuration changes, or scripts - to resolve identified vulnerabilities. It also enables or maintains automatic updates wherever possible, in line with Cyber Essentials guidance.

Compliance Status & Evidence

Provides a clear compliance view for each device—showing what's up to date, what needs fixing, and any unsupported software—and keeps a full audit trail of scans, fixes, and exceptions.

Key Benefits

- Reduced Exposure To Common Attacks
- Less Manual Patching Effort
- Audit-Ready Evidence
- Clear Remediation Priorities

Alignment to Cyber Essentials

STRENGTHENING SECURITY THROUGH CYBER ESSENTIALS

Cyber Essentials is a UK Government-backed, industry supported certified scheme, delivered by UK GOV partner, IASME.

The scheme is designed to protect organisations of all sizes against common cyber threats. security.

1) Security Updates

Cyber Essentials demands fast patching and supported software. Endpoint Compliance handles this with daily checks, CVE tracking, and auto-approved updates.

2) Secure Setup

Keeping devices up to date cuts out risky, outdated software and helps lock down configs properly.

3) Malware Protection

Closing known gaps makes it harder for malware to get in, backing up your anti-virus tools.

Endpoint Compliance strengthens your Cyber Essentials position, but full certification still requires all control areas across your entire business.

FIVE TECHNICAL CONTROLS OF CYBER ESSENTIALS

Access Control
Strong passwords and approved access only, reducing the risk of data breaches and insider threats.

Firewalls & Routers
Secure network barriers that block unauthorised access and protect business-critical data.

Secure Configuration
Locked-down devices with up-to-date software, cutting out weaknesses attackers rely on.

Malware Protection
Protection against viruses and threats, keeping systems running and data safe.

Software Updates
Regular patching to close security gaps before they can be exploited.

Secure your IT systems, ensure compliancy within any supply chain requirements, provide detailed evidence and keep operations running with Urban Network today.

CYBER ESSENTIALS

urban.
Managed IT, Cloud & Cyber

ABOUT URBAN NETWORK

Urban Network have been providing SMEs with robust cyber security solutions for over 24-years.

Working with clients operating in regulated industries or within stringent supply chains, our team of experts align your technology to empower growth.

CONTACT US

Coppergate House, 10 Whites Row, London, E1 7NF

0333 188 9155
hello@urbannetwork.co.uk
urbannetwork.co.uk