Meet Cyber Essentials Requirements with Ordr

Overview

Cyber Essentials was created by the National Cyber Security Centre (NCSC) in 2014 to help commercial organisations establish a minimum standard for their cybersecurity operations. According to the NCSC, Cyber Essentials help **"protect your organisation, whatever its size, against a whole range of the most common cyber attacks."**

National Cyber Security Centre

CYBER ESSENTIALS

CYBER ESSENTIALS PILLARS:

1. Firewalls and Gateways

2. Secure Network Configuration

3. Access Control

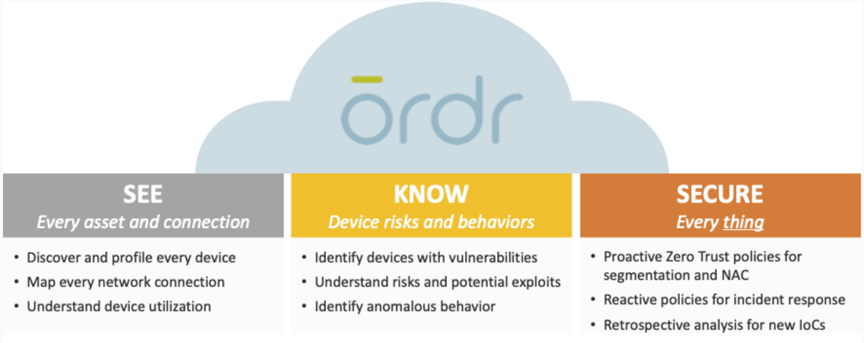
4. Malware Protection

5. Patch Management

The NCSC says that Cyber Essentials benefits those organisations that choose to follow its guidelines through the increased customer retention and new business development that comes from earning a reputation as a trusted steward of data. And while participation is voluntary, many organisations that collect and maintain certain types of sensitive consumer data, like personally identifiable information (PII), protected health information (PHI), and financial data **must comply with Cyber Essentials before doing business with government agencies.**

About Ordr

Ordr makes it easy to secure every connected device including traditional IT, IoT, IoMT, and OT devices. Ordr uses advanced machine learning to automatically discover and classify every device, identify risk, map all communications, baseline behavior, and provide protection with automated policies.



SEE
Every asset and connection

- Discover and profile every device
- Map every network connection
- Understand device utilization

KNOW
Device risks and behaviors

- Identify devices with vulnerabilities
- Understand risks and potential exploits
- Identify anomalous behavior

SECURE
Every thing

- Proactive Zero Trust policies for segmentation and NAC
- Reactive policies for incident response
- Retrospective analysis for new IoCs

How Ordr Helps with Cyber Essentials

Ordr's step-by-step guide, **How to Meet Cyber Essential Requirements for IT Infrastructure**, walks IT and security leaders through the NCSC's requirements and how to ensure compliance in accordance with the five pillars of Cyber Essentials.

Download your copy: https://ordr.net/cyberessentials

Guidence covered includes details on:

- Home working and BYOD
- Wireless devices
- Cloud services
- Firewalls
- Secure configuration
- Access control
- Password-based authentication
- Malware protection

Key Ordr Capabilities

Asset Visibility – Automatically discover, accurately classify, and collect high fidelity details of every device on the network including newly connected devices.

Asset Inventory – Integrate with CMMS and CMDB products to ensure device inventories are always up to date with accurate details.

Vulnerabilities and Risk – Identify devices with vulnerabilities and risk such as outdated operating systems, unpatched or unauthorized software, PHI, recalls, risky communications, and anomalous behaviour.

Device Risk Rating – Automatically calculate real-time risk ratings per device by combining vulnerabilities, risk, and customizable parameters to help prioritize remediation and mitigation efforts.

Vulnerabilitiy Management – Robust vulnerability management and mitigation capabilities including integration with existing IT tools, workflows, and network and security infrastructure to help teams efficiently manage risk.

Behavioural Profiling – Establish a baseline of normal communications for every device to identify active threats including zero-day attacks.

Threat Response – Improve threat response and with dynamically created policy enforced with existing security and network infrastructure.

Accelerate Zero Trust – Automate the creation of Zero Trust policy such as NAC or segmentation to reduce the attack surface and improve security.

Ecosystem Integrations – 80+ integrations with security, network, and IT products to enrich device insights, enable existing workflows, improve security efforts, and accelerate Zero Trust initiatives.

Compliance – Generate custom reports for evidence and a solution that is SOC 2 Type 2 certified, encrypts data at rest and in motion, does not collect PHI or PII data, and meets GDPR data privacy requirements by ensuring that all data collected remains in the United Kingdom.

Visit https://ordr.net/cyberessentials to download your copy of How to Meet Cyber Essential Requirements for IT Infrastructure or https://ordr.net/request-a-demo/ to request a demo to see how Ordr can help in your environment.