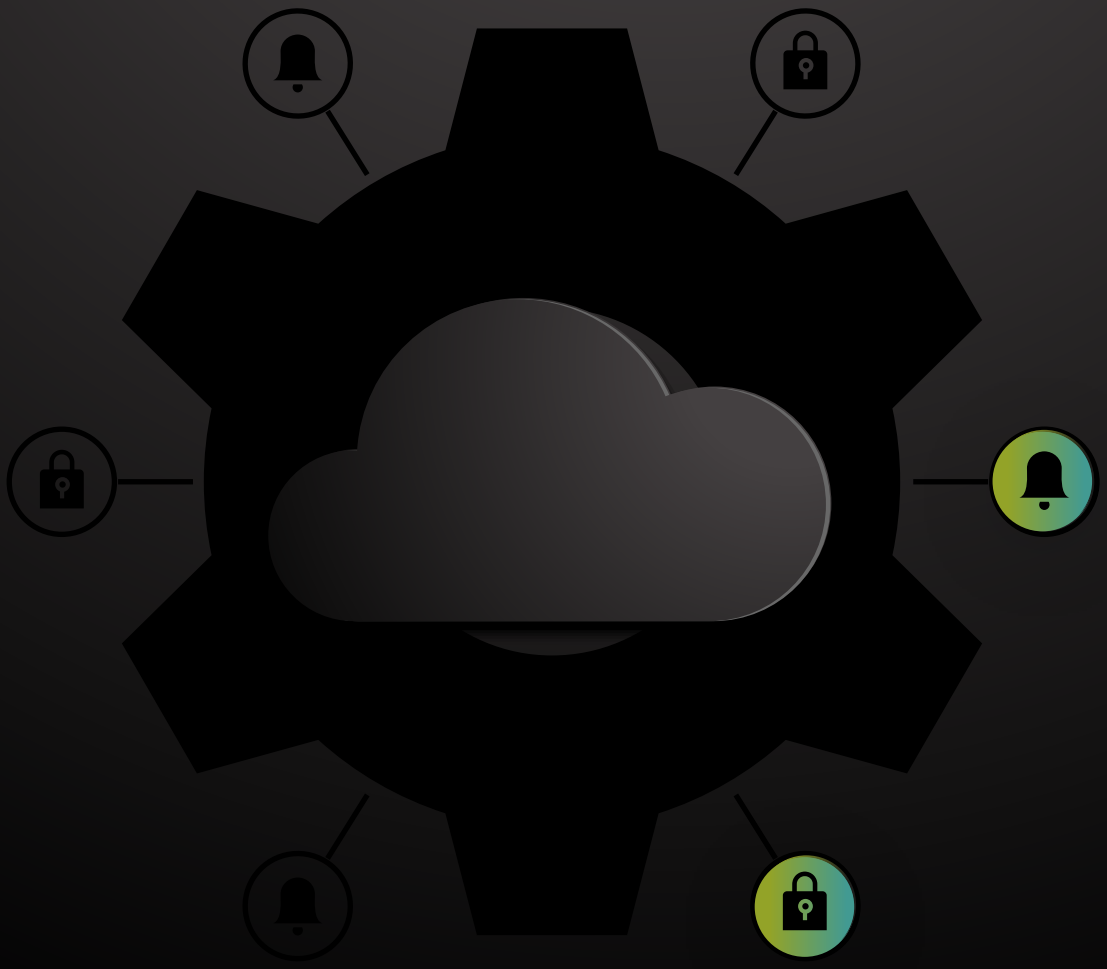

ordr

HOW TO MEET CYBER ESSENTIALS REQUIREMENTS

FOR IT INFRASTRUCTURE WITH ORDR CONNECTED DEVICE SECURITY

CYBER ESSENTIALS

OVERVIEW

Cyber Essentials scheme applicants must ensure their organisation meets all requirements outlined in the **Cyber Essentials: Requirements for IT infrastructure**. As part of the application process applicants may be required to provide evidence before certification is awarded.

Ordr provides a connected device security solution to help organizations improve security and meet Cyber Essentials requirements. With Ordr you will:

- ***SEE*** *all devices connected to your environment.*
- ***KNOW*** *the vulnerabilities and risks these devices introduce to your environment.*
- ***SECURE*** *devices and your environment to protect faculty, administrators, students, and data.*

This paper is based on Cyber Essentials: Requirements for IT infrastructure v3 and focuses on recommendations that pertain to connected devices such as Internet of Things (IoT), Internet of Medical Things (IoMT), and Operational Technology (OT) devices in addition to tablets, mobile phones, thin clients, laptops, and desktop computers. Each section provides an overview of a Cyber Essentials recommendation with details on how the Ordr solution can help organizations address requirements.

CYBER ESSENTIALS SCOPE

Cyber Essentials requirements apply to all devices and software contained within the boundary of the scope. Organisations should establish the boundary of scope and determine what is in scope within this boundary. ***Devices are "in scope" if they:***

- ***Accept incoming network connections from untrusted Internet-connected hosts***
- ***Establish user-initiated outbound connections to devices via the Internet***
- ***Control the flow of data between any of the above devices and the internet***

A sub-set can be used to define what is in scope or what is out of scope for Cyber Essentials, however, organisations that choose a scope that includes the whole IT infrastructure achieve the best protection and increase customer confidence. A scope that does not include end user devices is not acceptable.

CYBER ESSENTIALS RECOMMENDATION

Assessment and certification should cover the whole of the IT infrastructure used to perform the business of the applicant, or if necessary, a well-defined and separately managed sub-set. The boundary of the scope must be clearly defined in terms of the business unit managing it, the network boundary and physical location. The scope must be agreed between the applicant and the Certification Body before assessment begins.

- ***Organisations that choose a scope that includes the whole IT infrastructure achieve the best protection and increase customer confidence.***
- ***A scope that does not include end user devices is not acceptable.***

• User-owned devices (BYOD) which access organisational data or services are in scope.

• The default approach is that all corporate or BYOD home working devices used for applicant business purposes within the home location are in scope for Cyber Essentials.

HOW ORDR HELPS

Ordr helps organisations define a scope for assessment and certification that includes all network connected devices across the whole of your IT infrastructure. This includes IoT, IoMT, and OT devices in addition to tablets, mobile phones, thin clients, laptops, and desktop computers. ***With Ordr you will:***

• Automatically discover and accurately classify all network connected devices including end-user/BYOD devices and those accessing from home or other remote locations.

• Gain detailed device insights such as make, model, serial number, operating system, and installed software.

• Gain insight into device communications inside the firewall as well as communications to external Internet domains, cloud assets, etc.

Ordr analyses network traffic to automatically discover, classify, and gather granular details for every connected device across the whole IT infrastructure. Using this approach, Ordr does not require device agents and has no impact on device performance or availability. This means that all devices connected to the network can be discovered and classified, including end user devices not owned or controlled by the organization.

Within hours of deployment, Ordr provides accurate details on the make, model, operating system, serial number, application usage, port usage, and physical/network location for every device.

Ordr integrates with CMMS and CMDB tools to continuously enrich an existing inventory with missing devices and granular device details to create a real-time, single source of truth for all assets that is accurate and up to date.

With a complete view of every device across the whole IT infrastructure, Ordr identifies devices with vulnerabilities such as an outdated operating system, unauthorized software, weak ciphers, and weak certificates. Ordr integrates with 3rd party sources to enhance vulnerability identification to include known vulnerabilities, unpatched software, and devices with FDA or manufacturer recalls and other threats.

BYOD

CYBER ESSENTIALS RECOMMENDATION

BYOD devices are in scope if they access organisational data or services.

HOW ORDR HELPS

Ordr's agentless approach of analysing network traffic automatically discovers, classifies, and provides operating system and software inventory insights for all BYOD devices that connect to the network. Ordr also provides mapping of IP address to MAC (device) address to help with security and compliance use cases. Understanding these details for devices connecting over VPN or other scenarios where a device IP to MAC mapping changes frequently is especially challenging without a solution such as Ordr.

HOME WORKING

CYBER ESSENTIALS RECOMMENDATION

All devices used for applicant business purposes within the home location are recommended to be in scope as the default approach. This includes organisation owned devices, BYOD, and routers supplied by the organisation.

HOW ORDR HELPS

The Ordr Software Inventory Collector is a small script that can be deployed on devices that access the organisation from home locations or other remote environments. The Software Inventory Collector sends device details such as operating system, installed software, and anti-virus status to the Ordr solution.

Ordr also provides mapping of IP address to MAC (device) address to help with compliance and security use cases. This capability helps with use cases such as maintaining an accurate inventory that includes devices connecting over VPN or other scenarios where a device changes IP address frequently.

WIRELESS DEVICES

CYBER ESSENTIALS RECOMMENDATION

Wireless devices (including wireless access points) are in scope if they can communicate with other devices via the Internet.

HOW ORDR HELPS

Ordr automatically discovers, classifies, and gathers granular details for every wireless device connected to the network including wireless access points.

Ordr also provides mapping of IP address to MAC (device) address to help with compliance and security use cases. This capability helps with use cases such as maintaining an accurate inventory that includes wireless devices that move between access points and may change IP address frequently.

CLOUD SERVICES
(AKA EXTERNALLY MANAGED SERVICES)

CYBER ESSENTIALS RECOMMENDATION

Cloud services are in scope If the applicant's data or services are hosted on cloud services.

HOW ORDR HELPS

Ordr automatically discovers, classifies, and gathers granular details for assets running in cloud services such as VMware and AWS public, private, and hybrid cloud environments. Ordr also provides insights that include on premises devices communicate with workloads in cloud environments.

CYBER ESSENTIALS FIVE TECHNICAL CONTROL THEMES

Cyber Essentials defines five technical control themes and requires applicants to meet all the requirements. Applicants may also be required to supply evidence of meeting these requirements before being awarded certification.

FIREWALLS

CYBER ESSENTIALS RECOMMENDATION

Use firewalls to restrict access to services as a way to reduce exposure to attacks.

HOW ORDR HELPS

Ordr automates the creation of policy for enforcement on existing network and security equipment such as firewalls. Examples of Ordr policy include firewall rules for enforcement on boundary firewalls or ACLs for enforcement on network equipment. Ordr policy is dynamically created based on device baselines and device context gained from analysis of device communications. This helps to simplify and accelerate policy creation for connected devices.

Ordr created policy can be used to restrict (allow or block) inbound and outbound network traffic according to its source, destination, and type of communication protocol. Ordr policy can be used to restrict North/South communications between devices and the Internet, East/West communications between devices or groups of devices, or to isolate a device in the event of a security incident.

Ordr created policy can be shared with a certification body to supply evidence of meeting Cyber Essentials firewall requirements and aid in the certification process.

SECURE CONFIGURATION

CYBER ESSENTIALS RECOMMENDATION

Ensure computers and network devices are properly configured to reduce the level of inherent vulnerabilities and provide only the services required to fulfil their role.

HOW ORDR HELPS

Ordr can identify devices with potential vulnerabilities and misconfigurations such as:

- ***Outdated operating systems***
- ***Default or guessable (weak) account passwords***
- ***Weak certificates***

- ***Vulnerable applications, software, or services installed***
- ***Unauthorized or unnecessary applications, software, or services installed***
- ***Disabled security tools such as antivirus***
- ***Vulnerable and/or unnecessary network services enabled such as RDP, FTP, Telnet, and SMB***

Ordr can automate the creation of Zero Trust segmentation policies to restrict communications to and from vulnerable or misconfigured devices. Ordr policy is especially helpful to protect devices that are not able to be upgraded, patched, or easily replaced. For these devices, Ordr policy can be used to restrict communications to and from vulnerable devices to reduce risk while still allowing devices to remain operational.

USER ACCESS CONTROL

CYBER ESSENTIALS RECOMMENDATION

Enforce user access control to ensure user accounts are assigned to authorised individuals only and provide access to those applications, computers and networks actually required for the user to perform their role.

HOW ORDR HELPS

Ordr integrates with IT tools such as Microsoft Active Directory, DHCP, and DNS to provide a centralized view of user and privileged administrative account access to connected devices.

Ordr integration with Microsoft Active Directory provides a historical view of user access to connected devices to ensure that only authorised individuals have accessed connected devices and aid in auditing of device access to meet compliance requirements. This includes tracking of user accounts as well as privileged administrative accounts.

Ordr integration with Microsoft DHCP and DNS provides a historical view of IP to MAC address mapping for connected devices to aid in auditing of device access to meet compliance requirements.

PASSWORD-BASED AUTHENTICATION

CYBER ESSENTIALS RECOMMENDATION

Use technical controls to manage the quality of passwords.

HOW ORDR HELPS

Ordr can identify devices with default or weak passwords so teams can audit password risk, make appropriate updates, apply proper technical controls, and meet compliance requirements.

MALWARE PROTECTION

CYBER ESSENTIALS RECOMMENDATION

Restrict execution of known malware and untrusted software, to prevent harmful code from causing damage or accessing sensitive data.

HOW ORDR HELPS

Ordr creates a baseline of normal behaviour for all devices. From this baseline, Ordr identifies devices communicating outside of normal operations which may be an indicator of compromise. ***When abnormal communications are detected Ordr can send alerts to IT and security staff including tools such as SIEMs and aid in the response to active threats by:***

- ***Pinpointing the affected device, including the network and physical location***
- ***Providing an accurate device picture so teams can identify the physical device if needed***
- ***Automating the creation of policy to block traffic or quarantine and isolate an affected device to prevent the spread of a threat. Ordr created policy is enforced using an organization's existing security and network infrastructure.***

The operating system of many connected devices cannot be updated. These devices also do not support anti-malware software or other agents, and in some cases, scanning is not an option. Ordr can identify devices with outdated operating systems and software or unauthorized applications that may be susceptible to malware and other vulnerabilities. Ordr can also automate the creation of Zero Trust segmentation policy to ensure vulnerable devices can remain operational while restricting non-essential communications to reduce if not eliminate the risk of malware impact.

CYBER ESSENTIALS RECOMMENDATION

Prevent connections to malicious websites on the internet (by means of deny listing, for example) — unless there is a clear, documented business need and the applicant understands and accepts the associated risk.

HOW ORDR HELPS

Ordr provides insight into device communication with entities inside and outside of an organization. This helps to identify communication with websites such as command and control (C2) servers used for malware and ransomware operations in addition to other malicious websites. Ordr can also identify potentially risky communications such as devices communicating with domains in restricted geos such as Russia or North Korea.

In addition to providing these insights, Ordr automates the creation of policy for enforcement on boundary firewalls to restrict these risky or unauthorized communications.

SECURITY UPDATE MANAGEMENT

CYBER ESSENTIALS RECOMMENDATION

Ensure all in scope software is kept up to date and ensure devices and software are not vulnerable to known security issues for which fixes are available.

HOW ORDR HELPS

Ordr identifies devices with outdated and vulnerable operating systems and installed software that is vulnerable or unauthorized. Ordr also integrates with 3rd party sources such as threat feeds and manufacturer feeds to provide additional insights and aid in the identification of vulnerable devices and software.

Ordr provides a risk rating for each device to identify devices with 'critical' or 'high risk' and help in the prioritization of patching and other remediation efforts or mitigation activities. Ordr automates the creation of policy to aid mitigation efforts such as applying segmentation or other compensating controls to limit exposure for devices that cannot be upgraded or patched. Ordr can also create policy to quarantine "infected" or potentially vulnerable devices. Policy created by Ordr is enforced using existing security and network tools.

ABOUT ORDR

Ordr makes it easy to SEE every connected device, KNOW the risk, and SECURE every device, from traditional IT to newer and more vulnerable IoT, IoMT, and OT. Ordr uses deep packet inspection and advanced machine learning to discover every device, profile risk and behavior, map all communications, and improve protection with automated policies. Organizations worldwide trust Ordr to provide real-time asset inventory, address risk and compliance, and accelerate IT initiatives. Ordr is backed by top investors including Battery Ventures, Wing Venture Capital, Ten Eleven Ventures, Northgate Capital, Kaiser Permanente Ventures, and Unusual Ventures. For more information, visit ***www.ordr.net*** or contact us by sending an email to ***info@ordr.net.***