WHITE PAPER

ZERO TRUST

ordr

5 Steps to Zero Trust for Unmanaged and IoT Devices

Zero Trust has quickly emerged as a foundational concept of cybersecurity that guides the way many organizations approach securing their networks, devices, and users. The idea emerged as a response to the failures of the old "crunchy on the outside, soft and gooey on the inside" approach to perimeter security. In the old model, the boundary between the inside and outside of an organization was heavily secured, but on the inside, assets and traffic were presumed to be safe and trusted. This became a liability because once past the perimeter, attackers had free rein to spread throughout the victim network and cause virtually unlimited damage. This strategy has become standard practice for attackers and has been tied to some of the most destructive attacks and breaches in the past 5 years. The Target 2013 breach was probably the best example of this. Once attackers had access to the network via an HVAC contractor's login, they had free rein to do as they pleased.

Zero Trust offers a new approach that aims to stamp out the presumption of security, and instead, replace it with a mantra of "never trust, always verify". No devices or connections are to be implicitly trusted. Instead of one-time access decisions, security is to be addressed dynamically and continuously in a way that adapts to observed changes in the environment. And while organizations have made progress applying Zero Trust concepts to many of its traditional resources like laptops and servers, most have struggled to do the same for the rapidly increasing number of unmanaged, IoT, and OT devices in the enterprise.

The recently published second draft of NIST's **SP 800-207** Zero Trust Architecture lays out several core tenets of Zero Trust and how they can be applied to an enterprise. This includes the following important points that are particularly relevant to IoT and other unmanaged devices:

- **"All data sources and computing services are considered resources"**

  In a Zero Trust model all devices matter including IoT devices. No devices should be outside the scope of Zero Trust policies simply because they are harder to manage, perform a legacy function or fall under a different operating ownership (for example IoMT devices owned by clinical technicians).

- **"All communication is secured regardless of network location"**

  Devices and connections should not be trusted simply due to being inside the network or behind the corporate firewall. In fact, internal devices and connections should receive the same scrutiny that is applied to external connections from the Internet.

- **"Access to resources is determined by dynamic policy, including the observable state of client identity, application, and the requesting asset, and may include other behavioral attributes"**

  Security must be a continuous and ongoing process based on the evaluation of a wide variety of factors. It is not enough to simply whitelist a connection and assume it is safe. A device's behavior, compliance state, and risk posture can change throughout its lifecycle which has a direct impact on its trust level over time.

- **"The enterprise ensures that all owned and associated devices are in the most secure state possible…"**

  Organizations need to understand where their devices are unprotected, if they have vulnerabilities, and take steps to resolve and mitigate problems when they are discovered. It is important to identify which devices are currently managed versus unmanaged, as it determines what level of mitigation is possible for security and risk mitigation.

In this document, we analyze how these and other core concepts of Zero Trust apply to IoT and unmanaged devices. We provide 5 key steps organizations can take, and how the Ordr Systems Control Engine can put them into practice today.

Key Steps to Zero Trust For Unmanaged and IoT Devices

1

Gain Visibility Into the Device Attack Surface

Before Zero Trust policies can be applied to an asset, the organization must first know that the asset exists as well as its capabilities and purposes. This can be particularly challenging for the multitudes of devices that are unmanaged in the traditional sense. Security cameras, HVAC controllers, printers and industry-specific devices such as infusion pumps are all vastly different devices, with very different uses and risks. Yet, in many cases, an organization may only know each device as an IP address that belongs to a broadly defined subnet.

As a result, organizations need reliable methods to discover, classify, and inventory all devices in the enterprises-- both managed and unmanaged devices. This should include detailed insight into what type of device is detected as well as its make, capabilities, location, application/port and behaviors. It is critically important that the discovery and classification capabilities are automated as large numbers of unmanaged devices can be hard to track manually, and many devices may be physically moved from location to location as needs arise.

2

Identify At-Risk Devices

Once basic visibility is established, organizations should take into account the risk profile of the device. This could include devices operating with known vulnerabilities or lacking protection software, devices that have been recalled, or which are using weak passwords or certificates. Organizations will also naturally want to identify any devices that are exhibiting signs of a compromise as such behaving abnormally, contacting malicious domains, or other indicators of compromise.

Teams should naturally use this information in order to plan corrective actions to remediate any detected weaknesses. However, organizations can also use this information in order to drive risk-based policies in a Zero Trust architecture. Devices with higher levels of risk may be dynamically barred from communicating with certain high value devices or prevented from accessing risky domains.

3

Understand Device Communication Needs

Next, Zero Trust policies need to know how a device needs to communicate in order to perform its function. Unlike general use devices such as laptops, many IoT devices have very predictable behaviors. Many IoT and OT devices will use industry-specific protocols that may not be supported by traditional packet analyzers or security tools. Likewise, many of these devices will have very limited needs to interact with the Internet. Instead of managing the many Internet needs of a user’s laptop, an IoT device may need only to access the Internet to share data with a cloud backup or obtain patches and updates from a vendor support site.

Organizations should be able to automatically baseline the behavior of devices in the network as well as known behavior of similar devices. This should include baselining what other assets a device needs to communicate with and over which protocols as well as verifying the communications are safe and not destined to bad actors or part of threat activity. Security teams can then create very narrowly-defined policies that strictly limit devices to communicate to the few resources that are truly needed to operate without service disruption (see item 4 on segmentation).

4

Dynamically Segment Devices

Ultimately, Zero Trust requires that risk and security context is put into action. Policies need to be dynamically enforced based on the most current information available. Only required communications should be allowed and all others automatically denied.

One way that this can be done is with microsegmentation. Instead of traditional network segments where similar devices are grouped together either based on local topology or similar device function, microsegmentation policies define rules based on the needs of the device. So unlike a traditional segment where attackers are free to move laterally within a given segment, each device is only allowed to communicate with essential services while all other traffic is blocked, regardless of the device's location in the network.

Policies should also be enforced based on the observed risk context of a device. Mission critical devices may require more stringent policies. Organizations may want to limit the accessibility of devices that are at risk due to vulnerabilities or that have shown signs of compromise or anomalous behaviors.

5 Continuous Monitoring and Learning

Finally, teams must remember that Zero Trust is a dynamic and ongoing approach to security. Security contexts are always changing, and just because a device or session was trusted previously doesn't mean that it should be trusted on the next login.

IoT and unmanaged devices are often in constant state of changes with new devices being introduced to the environment, and other devices moving from location to location. Risk and threat contexts can change from day to day, and organizations need to be able to identify newly introduced devices, changes in behavior or signs that a device has been compromised. This means that all of the aforementioned requirements need to be performed automatically and continuously.

Using Ordr to Extend Zero Trust to All Devices

The Ordr Systems Control Engine (SCE) allows organizations to automatically discover, assess, and enforce policy on any device in the network including IoT, OT, and unmanaged devices. The platform uses agentless and passive methods, ensuring that the solution is easy to deploy and that all devices can be discovered without interfering with normal network operations.

Discover and Classify Every Device

Ordr quickly and dynamically discovers and inventories every "thing" in your domain, including IoT devices, OT, unmanaged devices, as well as traditional endpoints. The platform automatically collects a wide range of data on every connected device. This includes decoding more than 80 device and industry-specific protocols in order to analyze detailed application-level behavior of each device. This data is analyzed by a constantly evolving machine learning (ML) engine to classify each device based on its type and business function. For example, Ordr users could choose to see all physical security devices, or more specifically, all network cameras, or even specific cameras by model and version.

VALUE FOR ZERO TRUST

This allows organizations to bring all devices into the scope of Zero Trust. Additionally, the detailed classification of devices lays the groundwork for establishing policies based on the unique value of each device and the sensitivity of the information that it handles.

Automated Device Risk Assessment

Ordr next analyzes each device in terms of potential risk to the organization. This can include a wide range of traits including the identification of high-value devices, devices with vulnerabilities, devices that have been recalled, devices that are using weak or open passwords, weak TLS ciphers or expired certificates. For example, Ordr can identify devices that process sensitive information such as protected health information (PHI).

Next, Ordr discovers signs of compromise using both known and behavioral indicators of compromise. Known indicators can include interaction with known malicious IP addresses or domains. Alternatively, Ordr can recognize behavioral anomalies within devices based on observed baselines in the network or deviations from norms for a particular device profiled.

VALUE FOR ZERO TRUST

This capability allows organizations to find weaknesses in the environment as well as apply policies based on observed device risks. Devices with vulnerabilities, recalls, weak passwords, or signs of threats can be tagged for remediation, and optionally protected or isolated in order to limit exposure. Ordr's continuous analysis aligns with the Zero Trust requirement for security decisions to always be evaluated based on the most current information available.

Automated Microsegmentation and Isolation

Ordr automatically learns the unique communication patterns of each device; the Ordr Flow Genome reveals the specific communications flows that are required to perform its function. Ordr can then dynamically generate microsegmentation policies for existing infrastructure such as switches, wireless controllers, firewalls or NAC policy servers to ensure that devices can only interact with other necessary devices with the minimum required access.

Once generated, these policies can be added manually by staff or automatically by Ordr via integration with the target system (e.g. firewall API). Policies can likewise be created to isolate or quarantine devices that have high levels of risk or signs of compromise.

VALUE FOR ZERO TRUST

Zero Trust requires organizations policies to be put into action before a user or device is granted access to a resource. Visibility into IoT and managed devices is a great start, but that information needs to be enforceable in order to deliver on the goals of a Zero Trust architecture. Ordr provides the only solution that can deliver the full lifecycle of unmanaged and IoT device security from discovery, assessment, to enforcement in a completely automated fashion.

Zero Trust Architectures can involve a great deal of additional context and consideration, and implementation details naturally vary from organization to organization based on their unique needs and environments. This document provides a high-level introduction to Zero Trust and how it applies to the world of IoT and unmanaged devices. To learn more about Ordr and how the SCE platform can provide visibility and security for your organization, please contact the Ordr team at **www.ordr.net**.