AXONIUS

A Primer on Unmanaged Device Discovery

White Paper • April 2020

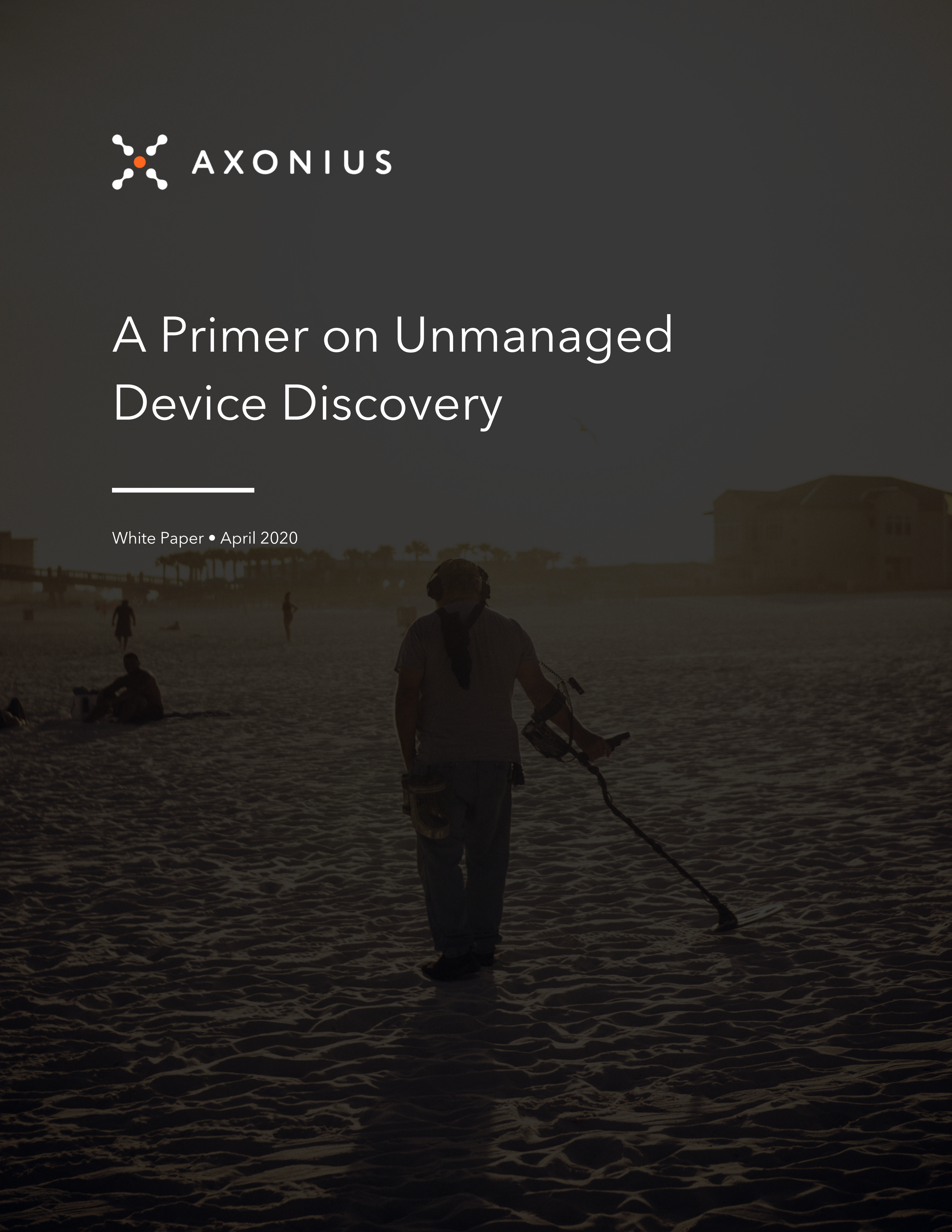

Table of Contents.

INTRODUCTION. 3

WHAT IS AN "UNMANAGED DEVICE"? 3

UNKNOWN DEVICES 3

UNMANAGED DEVICES 3

ROGUE DEVICES 3

DISCOVERING UNMANAGED DEVICES. 4

AUTHORIZED VS. UNAUTHORIZED DEVICES. 5

PASSIVELY GATHERING DEVICE DATA WITH AXONIUS. 5

CONCLUSION. 6

ABOUT AXONIUS. 6

Introduction.

Discovering unmanaged devices can be challenging both in definition and in practice. However, when done effectively, unmanaged device discovery leads to a more credible asset inventory, and a more effective cybersecurity asset management program overall. In this short paper, we'll look at what constitutes an "unmanaged" device, approaches to discovery, and how continuous data aggregation and correlation helps automate unmanaged device discovery.

What is an "Unmanaged Device"?

There are a few distinctions that need to be drawn when talking about devices that are unknown, unmanaged, or rogue. For the purpose of this paper, we'll use:

Unknown Devices

An unknown device is any device that is not part of an asset inventory. These are devices that access corporate resources, but are not owned or controlled by the IT or security function at an organization. An example would be a raspberry pi that an employee connected to the network.

Unmanaged Devices

An unmanaged device is not known by other data sources in a networked environment. All unknown devices are by definition unmanaged, but a device can be known and still be unmanaged. An example of an unmanaged device would be a laptop that has no security agent installed.

Rogue Devices

Rogue devices can be described as devices that have been placed on a network for malicious intent.

Discovering Unmanaged Devices.

The “discovery” of unmanaged, IOT and / or rogue devices is a bit of a misnomer. In reality, the evidence of the presence of these devices exists in specific data stores across any IT network. Indeed, whenever any network-connected device (managed, unmanaged, IOT, rogue) communicates across the network it leaves a trail of breadcrumbs in each of the network devices through which those communications traverse. This evidence exists in the form of logs, ARP cache, MAC address tables, DHCP and/or CDP/LLDP tables. Every device utilizing the IP protocol has an Address Resolution Protocol (ARP) table. Since IP is a layer 3 protocol and requires an underlying layer 2 protocol to communicate on local broadcast domains, there is a requirement for a network device to be able to translate an L3 IP address to its corresponding L2 address using ARP protocol. This L2 address information is stored as a 48-bit (6 bytes) MAC address with the corresponding switch VLAN or interface which received data from this address, often with an age in seconds, to expire out this address.

When an asset aggregation tool can passively connect to and collect this MAC and IP address information and then further correlate this data to other asset sources of data that also contain MAC and IP address information, then this yields the opportunity to identify whether a device is a “known” or “managed” device in the overall IT estate or if the device is in fact “unknown” and therefore “unmanaged”.

These are the only two possible outcomes for a device communicating on the network – either it is managed and therefore “known” to other siloed data sources in the organization or it is unmanaged and therefore “unknown” to other deployed systems.

If the device is ”managed”, i.e., known to other data sources in the networked environment, then we may combine pieces of data from the network layer and combine this with information from these other “managed” data sources. Some of these sources may include:

- Directory services like Microsoft Active Directory
- Endpoint management tools like Tanium or Microsoft SCCM
- Endpoint security agent-based tools like Symantec AV or CrowdStrike EDR.

If the device is ”unmanaged” or “unknown“, then the next step is to identify whether the device is “authorized” or “unauthorized” on a particular VLAN, network segment or in general, on the network itself.

Authorized vs. Unauthorized Devices.

The ability to identify whether an asset or device on the network is “authorized” or “unauthorized” requires an organization to have intimate knowledge of their environment. Further, the organization will also be required to correlate the MAC address to other pieces of information that help identify, in more detail, characteristics of the “unmanaged” device that can be used as context for comparison to this known, intimate knowledge. Characteristics that may provide this additional context can include the port and the protocol over which the device is communicating, and the network interface manufacturer of the device.

If a company can correlate the “unmanaged” device MAC address (as found in the network switch), along with the network segment (also found in the switch data) to the network interface manufacturer, then the company may now understand that an HP printer for example is communicating on a specific network segment through a particular switch. Combined with knowledge of what should and should not be communicating on a specific network segment, one may determine that the HP printer, while “unmanaged” is indeed “authorized” to be there, i.e., a valid and expected condition. The conclusion that a device is “unmanaged” and “unauthorized” is also a viable conclusion when the presence of an unmanaged device conflicts with the expectations tied to that intimate knowledge of a customer’s environment. The importance of this conclusion should not be understated.

Passively Gathering Device Data with Axonius.

Axonius provides companies with the ability to passively collect and aggregate device information from a wide range of technology types across an enterprise on a continuous basis. Data source types include:

- Infrastructure solutions like virtualization, DNS and DHCP solutions
- Network devices like routers, switches and firewalls
- Endpoint management tools like SCCM, Chef, Tanium and Lansweeper
- Cloud platforms like AWS, Oracle, Azure and Google Compute
- EPP and EDR solutions like FireEye HX, Carbon Black, SentinelOne & CrowdStrike
- AV solutions like Trend Micro, Symantec, McAfee and Sophos
- NAC solutions like Aruba ClearPass, ForeScout and Cisco ISE
- Vulnerability scanning tools like Tenable, Qualys and Rapid7

Conclusion.

Discovering unmanaged devices is a key component of a cybersecurity asset management. However, many traditional approaches make unmanaged device discovery a laborious, difficult exercise. Moreover, even when unmanaged devices are discovered, they are often identified at a specific point in time.

To effectively reduce risk in a dynamic threat environment, the ability to discover unmanaged devices on a *continuous basis* is crucial. Axonius can automate the discovery and enforcement of unmanaged devices, allowing Security and IT teams to efficiently reduce risk.

About Axonius.

Axonius is the cybersecurity asset management platform that gives organizations a comprehensive asset inventory, uncovers security solution coverage gaps, and automatically validates and enforces security policies. By seamlessly integrating with over 200 security and management solutions, Axonius is deployed in minutes, improving cyber hygiene immediately.

Covering millions of devices at customers like the New York Times, Schneider Electric, Landmark Health, AppsFlyer, and many more, Axonius was named the Most Innovative Startup of 2019 at the prestigious RSAC Innovation Sandbox and was named to the CNBC Upstart 100 list and Forbes 20 Rising Stars. For more, visit Axonius.com.

For more information, please visit Axonius.com.