AXONIUS

AXONIUS
WHITE PAPER

THE FIRST STEP
TO ZERO TRUST

ASSET MANAGEMENT FOR CYBERSECURITY

THE HALLMARK OF ZERO TRUST IS SIMPLICITY. WHEN EVERY USER, PACKET, NETWORK INTERFACE, AND DEVICE IS UNTRUSTED, PROTECTING ASSETS BECOMES SIMPLE.[1]

JOHN KINDERVAG

SVP OF CYBERSECURITY STRATEGY AT ON2IT AND

FORMER FORRESTER ANALYST WHO COINED THE TERM ZERO TRUST

1 *"Tech Trends 2021." Zero trust: Never trust, always verify. Deloitte Insights. 2020.*

THE EVOLUTION OF ZERO TRUST

THE EVOLUTION OF ZERO TRUST

THE EVOLUTION OF ZERO TRUST

Zero Trust has come a long way from being just another buzzword to becoming a business imperative. So much so that questions around Zero Trust have evolved from, *"What's this new security model?"* to, *"How can we implement a Zero Trust strategy?"*.

As cybersecurity threats, business models, and workforce dynamics evolve, applying the principle of least privilege to data access has become an integral part of many organizations' cybersecurity strategies.

2003 Zero Trust's earliest work begins in the Jericho Forum, a security consortium where like-minded CISOs promote a new concept of security called "de-perimeterization".

2010 Forrester alum John Kindervag coins the term "Zero Trust", centering around the belief that security must be designed with the strategy, "never trust, always verify".

2014 Google internally launches BeyondCorp, its Zero Trust approach to user access and authentication, and the concept gains steam.

2021 President Joe Biden's **Executive Order on Improving the Nation's Cybersecurity** mandates federal agencies must advance toward Zero Trust security concepts. The NSA also releases guidance, **"Embracing a Zero Trust Security Model"**.

WHY ZERO TRUST IS MORE IMPORTANT THAN EVER

While the evolving threat landscape and high-profile breaches are compelling reasons alone for adopting Zero Trust, the biggest driver has been changes in the way we work – a shift driven primarily by the COVID-19 pandemic.

In fact, the number of remote workers has more than doubled since the start of the pandemic.

58% *organizations reporting a remote workforce*

23% *organizations reporting a remote workforce before the COVID-19 pandemic*

Remote work has relaxed BYOD policies and increased endpoints accessing an organization's data. Increase in device diversity has also led IT and security teams to put more focus on identity and access management solutions.

Plus, accelerated digital transformation, rapid adoption of a cloud-first approach, and a proliferation of IoT devices are constantly expanding and dissolving the network perimeter. All these factors quickly made the perimeter-based network defense approach obsolete.

A Zero Trust model, rooted in the principle of "never trust, always verify," minimizes risk by securing sensitive data, systems, and services.

2 *"Cybersecurity Asset Management Trends 2021: How the Rapid Shift to Remote Work Impacted IT Complexity and Post-pandemic Security Priorities." Axonius and Enterprise Strategy Group. 2021.*

Traditional network security approaches focus on defending a perimeter and assume anything on the inside is safe. The Zero Trust model makes no such assumption. It's centered on the belief that organizations shouldn't automatically trust anything inside or outside its perimeters.

A Zero Trust strategy — more risk-driven and context-aware — helps organizations strengthen their security posture and limit their attack surface.

Regulations like the General Data Protection Regulation and California Consumer Privacy Act have also raised the security bar for U.S. companies for protecting customer data.

A Zero Trust approach helps companies adopt a more rigorous security posture by:

- Requiring organizations to focus on having a real-time, updated inventory of all IT assets
- Limiting access on the principle of least privilege

These processes are crucial when maintaining compliance with latest regulations.

What's more, Zero Trust is now a mandate for federal agencies. President Biden's 2021 cybersecurity executive order outlined the actions federal agencies should take to move toward a more secure government.

Central among those actions? Implementing Zero Trust.

TECHNOLOGIES ASSOCIATED WITH ZERO TRUST

TECHNOLOGIES ASSOCIATED WITH ZERO TRUST

TECHNOLOGIES ASSOCIATED WITH ZERO TRUST

Let's take a look at some of the functional areas associated with Zero Trust and the technologies that can help:

01

WHAT IS THE DEVICE THAT'S TRYING TO ACCESS CORPORATE ASSETS? Is the device in question a laptop? Smart TV? IoT Device? Knowing the type of device is the first in a series of granular questions that determine whether granting access is appropriate. For example, a web-enabled baby monitor probably shouldn't be trying to request data from a file share.

02

IS THE CORE SOFTWARE UP-TO-DATE? Assuming a device clears the first hurdle, let's then check to see whether the OS is current. You may not want a laptop running XP to have access to… well, anything, really.

03

WHAT VULNERABILITIES EXIST ON THE DEVICE? Aside from the core software, what else is installed? What vulnerabilities come with the additional software residing on the device?

04

IS THE DEVICE MANAGED? Most organizations mandate that a specified endpoint protection solution is installed on each device, usually with an agent. If that agent isn't installed (or isn't running), you may want to only allow that device on the guest network. You may also want to force an installation of said agent before accessing anything that isn't publicly available.

05

WHICH USER IS LOGGED IN? Now that we know about the device, let's figure out the person using it. Is it a network admin? A member of the finance group? Someone who left the company six months ago?

06

DOES THE USER HAVE ACCESS? Finally, let's try to understand whether the user should be able to access what they're requesting.

Now, we'll explore some of the technologies that can answer these questions.

ACTIVE DIRECTORY

Active Directory (AD) helps us understand the device and user roles and how each fits in the organizational policy.

At the most basic level, AD can tell us whether a user and device are known and have permission to access any corporate asset. At the most granular, AD can tell us which assets are accessible by looking at group membership and policy adherence.

ENDPOINT PROTECTION

Most organizations mandate an Endpoint Detection and Response (EDR) or Endpoint Protection Platform (EPP) solution be installed and running on every endpoint. These solutions can detect, prevent, and remove malicious items like malware before they can move laterally and infect other network assets.

Additionally, in a BYOD and remote working environment, cloud-delivered endpoint protection products can be the only way to understand the security status of devices that never connect to a corporate network or VPN.

VULNERABILITY ASSESSMENT

To understand which vulnerabilities are present on any device, organizations use vulnerability assessment (VA) tools to compare lists of known vulnerabilities to the version of each application present. Based on the severity of any vulnerabilities found, actions can be taken to either prevent a device from accessing corporate data, or, if a patch is available, force an upgrade before granting access.

Although some VA tools have discovery capabilities, many will only scan devices that they know about in a given IP range. Because of this, we cannot rely on a result such as "no known vulnerability detected" as a condition to be met, as that requirement could come from a VA tool simply not knowing that a device exists.

IDENTITY AND ACCESS MANAGEMENT

Aside from AD, many organizations are looking to identity and access management (IAM) providers that offer multifactor authentication and single sign-on for added security and convenience. These products can also add application-level permissions for cloud-based services.

For example, a company may use AD to authenticate users to access files and corporate email, but may use an IAM provider to understand which users should have access to the CRM.

MOBILE DEVICE MANAGEMENT

In an increasingly mobile world, organizations can't just rely on endpoint protection, since employees use mobile devices constantly, switch devices often, and take their devices with them when they leave.

Mobile device management lets companies grant and revoke access at any time without needing physical access to an employee's personal devices.

SWITCHES AND ROUTERS

To understand which devices are unmanaged, we must:

- Look at the devices that have an agent installed
- Compare them to the list of devices known to the switches and routers to find the delta (those IP addresses known only to the network without agents installed)

This will give us a list of unmanaged devices that should be managed and those that are unnecessary.

CYBERSECURITY ASSET MANAGEMENT

Cybersecurity asset management platforms give a comprehensive view into all assets and users to understand the security posture of each.

By connecting to all security and IT products in an organization's environment, cybersecurity asset management tools provide a continuous view of the relationship between devices, users, and security product coverage – constantly validating each against the organization's security policy. A few examples:

Which devices are unmanaged, but should have an agent?	**What percentage of devices are running our endpoint protection platform?**
Which devices aren't being scanned by our VA tool?	**Which users have improper access rights or passwords that never expire?**

Cybersecurity asset management platforms automatically aggregate and correlate asset data into a single, actionable view.

IMPLEMENTING THE ZERO TRUST MODEL
IMPLEMENTING THE ZERO TRUST MODEL

IMPLEMENTING THE ZERO TRUST MODEL

Going from the traditional perimeter-based security approach to Zero Trust can seem daunting – but it's not an all-or-nothing process. Many organizations approach Zero Trust as an aspirational future state, making new security purchasing and implementation decisions with eventual Zero Trust in mind.

Let's look at a few steps organizations can follow to get started on the path to Zero Trust.

01

UNDERSTAND WHAT DEVICES YOU HAVE

You can only secure what you can see – and until you know which devices are in your environment, it's impossible to know whether those devices are satisfactorily secure.

Establishing an ongoing device discovery, classification, and inventory process should be the first step in your Zero Trust journey.

02

DISTINGUISH BETWEEN MANAGED AND UNMANAGED DEVICES

A smart TV in a conference room is different from the CEO's laptop, and they should be treated differently. While the smart TV doesn't need an endpoint agent or a patching schedule, the laptop does.

Creating a process to take action based on asset classification is critical.

03

ADDRESS THE GAPS IN SECURITY SOLUTION COVERAGE

It's safe to say nearly every organization has devices missing security solution coverage. Whether that means AWS instances not known to a VA scanner, R&D machines without an EDR solution, or iPhones without MDM, there are always gaps to be addressed.

Addressing these gaps on an ongoing basis is necessary for any organization implementing a Zero Trust model.

04

ESTABLISH ONGOING USER ACCESS AUDITING

Are there users in your environment with local admin access to all machines? Users with passwords not required or set to never expire? Service accounts with keys to the kingdom?

Even with strict access controls and granular policies, an ongoing auditing process is needed to ensure proper access rights.

05

IMPLEMENT SECURITY POLICY VALIDATION

Finally, any security policy on paper is only as good as it is enforced and validated in reality.

Implementing a security policy validation process is the only way to make sure nothing is missed and exceptions aren't exploited.

THE FIRST STEP TO ZERO TRUST
THE FIRST STEP TO ZERO TRUST
THE FIRST STEP TO ZERO TRUST

Visibility is key when it comes to defending assets. Cybersecurity asset management provides comprehensive visibility into all devices and users – and the security products that cover them – to validate security policies.

CONNECTING TO EXISTING SECURITY AND IT MANAGEMENT SOLUTIONS

Instead of installing an agent, scanning, or sniffing traffic, a cybersecurity asset management solution connects to the different security and management solutions already used. IT and security teams simply provide credentials (API keys, tokens, etc.) and the system immediately starts collecting and correlating information about assets. This way, there are no agents to install or maintain, no bottlenecks to route traffic through, no limit to scale, and no performance degradation.

CREATING A COMPREHENSIVE VIEW OF ALL DEVICES

After connecting all relevant adapters, a cybersecurity asset management platform creates a correlated list of all devices, which can be filtered and sorted by any property. The solution is constantly requesting up-to-date data from every connected solution, so the list of devices is always as close to real-time as the connected solutions allow.

IDENTIFYING UNMANAGED DEVICES

By connecting to the security and management solutions and comparing results to what's known only to switches and routers, the cybersecurity asset management solution produces a list of unmanaged devices. This lets teams distinguish between devices that shouldn't be managed (think of a smart TV in a conference room or an Amazon Alexa in the reception area), and an AWS instance that the security and IT teams don't know about.

UNDERSTANDING SECURITY SOLUTION COVERAGE

Even with a security policy dictating every device needs an endpoint agent and must be scanned by a VA tool, most organizations have gaps in coverage. With a cybersecurity asset management platform, IT and security teams can understand which devices aren't covered so they can act. It also helps automate remediation.

CREATING ALERTS

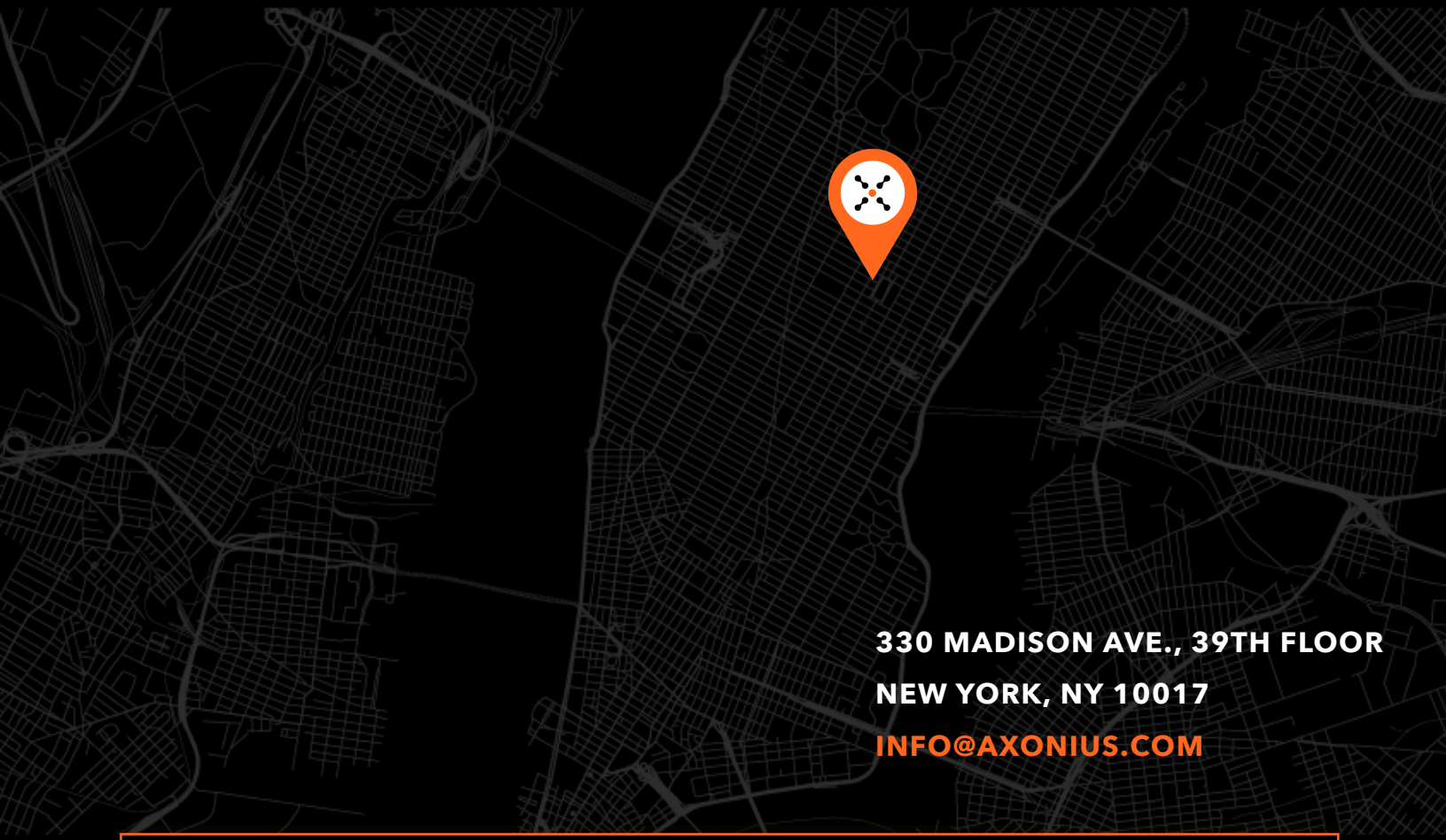
The core value of cybersecurity asset management tools lies in their ability to ask questions that validate a security policy on an ongoing basis. These tools also create alerts to notify staff or other solutions when something doesn't adhere to the policy. To do that, cybersecurity asset management solutions let teams save any query and create an alert from a query that can be sent via email, syslog, or through an integration with another system.

ENHANCING DEVICE AND USER DATA

In many cases, organizations already use many different security solutions and don't want yet another system to maintain and staff. Instead, they want to integrate cybersecurity asset management data with a system of record. Using the solution's API, teams can extract additional contextual information about users and devices, then push that data into their existing systems.

AXONIUS

Axonius is the cybersecurity asset management platform that correlates asset data from existing solutions to provide an always up-to-date inventory, uncover gaps, and automate action, giving security and IT teams the confidence to control complexity.



330 MADISON AVE., 39TH FLOOR
NEW YORK, NY 10017
INFO@AXONIUS.COM

See how the **Axonius Cybersecurity Asset Management Platform** drives your Zero Trust journey.

SEE IT FOR YOURSELF