AXONIUS

EBOOK

# Discovering, Managing & Securing **Ephemeral Devices:**

## A PRIMER FOR CYBERSECURITY ASSET MANAGEMENT

Ephemeral device adoption is growing at a rapid rate in cloud and virtual computing environments.

This acceleration represents yet another challenge for the teams responsible for managing and securing these assets.

**Left unmanaged or forgotten, ephemeral devices can drastically increase an organization's attack surface and introduce risk.**

It's important to understand not only why we need proper oversight of ephemeral devices – including their implications for security, governance, and compliance – but how we can oversee the network performance and monitoring of these devices, too.

## Read on to learn:

**What ephemeral devices are, why it can be so difficult to secure them, and what risk they pose to your organization.**

**Why traditional asset management tools and methodologies make discovering ephemeral devices problematic.**

**How using tools and technology built specifically for cybersecurity asset management makes it easier to discover and secure ephemeral devices.**

# What Are Ephemeral Devices?

By definition, an ephemeral device is a device that lasts for a short period of time.

Examples of devices that are often ephemeral include virtual machines, containers, and certain unmanaged devices. (We'll cover all these in more detail throughout this guide.)

Many of these devices are authorized and a normal part of operational workflows. **But that doesn't mean they're easy to manage**. For instance, it's usually tough for security, networking, and governance, risk, and compliance (GRC) teams to identify their presence in real time.

Assessing the state of a past ephemeral asset poses another challenge. For example, how can you look at the state of an asset that was present two weeks ago, running for a period of 24 hours?

An ephemeral device is a device that **lasts for a short period of time.**

Ephemeral devices bring along a host of issues that companies need to address:

- **How can we attest to various compliance metrics across an organization if we can't identify each device in the environment from a week ago, a day ago – even an hour ago?**
- **How can we determine the security posture of devices via a vulnerability scan, when the devices are created, live, and become deprecated between scan cycles?**
- **How do we deploy the security patches and agents needed when we're not notified that these short-lived devices are created?**
- **How can we triage an alert for a device that no longer exists? Or reconcile devices that appear to have the same IP address?**

This is just a short list of the problems and headaches that go hand-in-hand with ephemeral devices.

Now, let's take a look at a few examples of ephemeral devices to identify **why they cause so many challenges in the first place.**

# Virtual Machines

Virtual machines became ubiquitous in the last decade because they're a better use of computing resources. They offer a lower total cost of ownership versus stand-alone physical servers and just-in-time resource provisioning.

Once companies realized they could provision and deploy a new server in minutes – parceling out bare minimum processor, memory, and disk resources for mission-critical applications – the adoption rate ratcheted up.

For all their benefits, though, **virtual machines do have their downfalls.** While the average life expectancy of a physical server ranges from three to five years, the lifespan of a virtual machine is typically between two weeks and 12 months.

With virtual machines being spun up and shut down so quickly, it's extremely difficult to detect them — let alone secure them — using **traditional asset management methods.**


AVERAGE LIFE EXPECTANCY
OF A PHYSICAL SERVER


TYPICAL LIFESPAN OF A
VIRTUAL MACHINE

# Containers

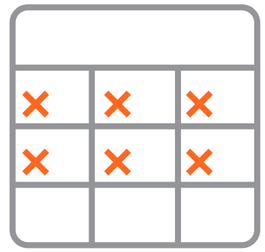
The rapid transition from the data center to the cloud was accelerated by the launch of container technology. **It is precisely the ephemeral nature of containers that drives the cost advantage of the cloud**, because customers pay only for what they use.

That cost advantage has been the key growth element for cloud platform providers like Amazon Web Services, Microsoft Azure, and Google Cloud Platform.

Thanks to containers, usage doesn't have to be bound in terms of months and years, or in simplistic terms like the number of servers, as we see with data center virtual machines.

Instead, customers now pay for container resources by the second and by the number of compute cores and memory. This offers up ultimate flexibility when it comes to controlling costs.

Because containers are such adaptable workloads, companies use them to perform specific tasks – and then deprecate the container. This usually happens quickly, with a short decay time from the inception of most containers.



WITHOUT ORCHESTRATION, THE AVERAGE CONTAINER LIVES FOR SIX DAYS

IN ORGANIZATIONS RUNNING AN ORCHESTRATOR, TYPICAL CONTAINER LIFETIME IS TWELVE HOURS

# Unmanaged Devices

Unmanaged devices make up anywhere between 10 and 30 percent of all devices communicating on a physical LAN network.

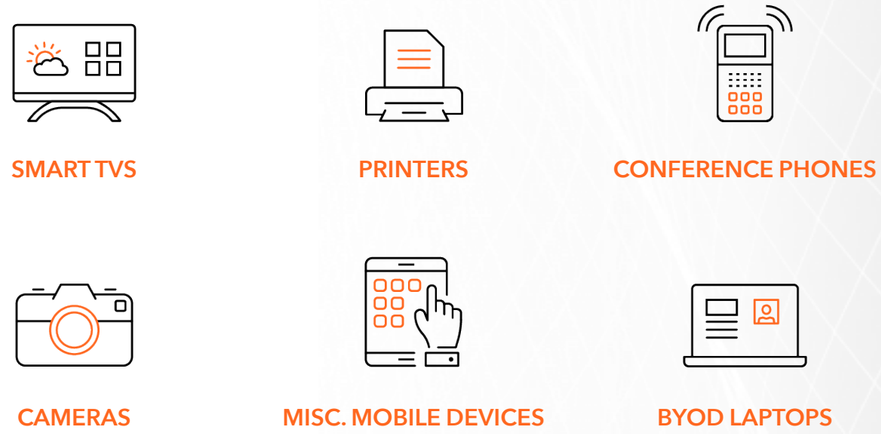
What exactly are these devices? Unmanaged devices are on the network, but not managed by any corporate-owned technology console. An unmanaged device won't have managed security agents deployed. They won't be joined to a directory services domain controller or endpoint management technology, either.

These devices **simply aren't known** to the vast management layers that exist across the enterprise.

Many of these devices are ephemeral in nature, in that they "appear on" and "disappear from" the network.

In the age of BYOD, devices like tablets, smartphones, and even IoT devices like cameras might connect to the network for very short periods of time, and then disconnect when the device's user leaves the building.

**Unmanaged devices usually include:**




The decay time is generally measured in minutes and hours, rather than days and weeks. And the device might only show up once and then never appear again – or it might appear periodically, especially in the case of employees BYOD.

**Unmanaged devices are often hard to discover.** They can evade real-time network sensors because of their location. They might appear between vulnerability or device scanning cycles. And they can be missed in log correlation engines, because they aren't always persistent.

# The Impact on IT, Security & Operations.

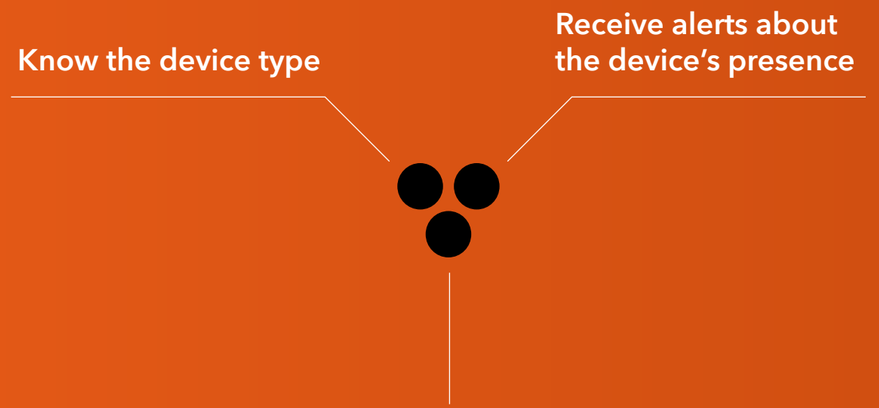
Ephemeral devices present a whole host of obvious security issues. For container and virtual machine deployments, new devices must pass a series of security checks and conform to painstakingly developed processes and policies.

- **Where a device will be deployed**
- **Whether there are appropriate network security controls**
- **Which personnel are authorized to use and access the devices**

The difference between a security **incident** and a security **breach** is often knowing when a device is present on a network it shouldn't have access to.

Security teams also need to ensure that the device has been patched and hardened, that critical data is encrypted, and that security agents have been deployed on the device, when possible.

**For unmanaged and unknown devices connected to the network, security teams should:**



# The Impact on IT, Security & Operations.

## GOVERNANCE RISK & COMPLIANCE RAMIFICATIONS

Large enterprise companies spend millions of dollars each year to prepare for external audits, meet various regulatory compliance requirements, and support remediation efforts.

They're also **spending on risk management** – including identification, measurement, mitigation strategies, tools, and monitoring.

The inability to identify and characterize ephemeral devices like virtual machines, containers, and unmanaged devices can render some of these efforts ineffective.

## NETWORK PERFORMANCE & TROUBLESHOOTING IMPLICATIONS

Understanding the devices living in and exerting demands on a network is a crucial step in planning network capacity and troubleshooting issues.

But when an ephemeral device is the root cause of a network performance issue, the **time and complexity** that go into solving and remediating the issue can be extensive.

For example, if a company had a network slowdown three days ago, how can it have a detailed understanding of what was present on the network at the time to identify the root cause of that slowdown?

# Identifying Ephemeral Devices: A Modern Challenge.

The challenge of ephemeral devices might be best illustrated by the “pets vs. cattle” analogy often cited in cybersecurity. Our servers and devices are the pets in this scenario. We care about them. We want them to live for a long time. If they get sick, we want to fix them.

**When they die, we’re upset.**

But ephemeral devices like virtual machines, containers, and other elastic workloads? They’re the cattle. They’re one of many. Expendable. We expect them to live for as long as we need them, and if something goes wrong… well, you know what happens when ol’ Bessie’s brought out back.

## A MASSIVE SURFACE TO MANAGE

**Because ephemeral devices are so easy to spin up, you can easily have hundreds of thousands of instances.**

That’s more than any team could handle. You’d never have the capacity to inspect all those instances for vulnerabilities. The attack surface is just too enormous and fluid for any team of humans to manage.

## THE FLEETING NATURE OF EPHEMERAL DEVICES

**Ephemeral devices are typically unaccounted for in an asset inventory built using traditional methods and tools.**

For example, a new container wouldn’t be accounted for in Configuration Management Database (CMDB) if it isn’t connected directly to sources that know about it. That means a container would need to be added manually. And once the container is deprecated, the CDMB would be outdated.

# Traditional Tools Can't Keep Track.

Many traditional tools used for asset inventorying can't effectively discover ephemeral devices.

Scanning tools won't find many ephemeral devices, since scans typically aren't continuous and instead are performed in cycles – sometimes on a monthly or even quarterly basis.

Such infrequent scanning means a **potentially massive ephemeral device visibility gap.**

Agent-based tools can be effective for identifying assets — but since ephemeral devices are short lived, they often never have an agent deployed on them in the first place.

Network-based tools will often lack many of the contextual data points needed to properly identify ephemeral devices.

For instance, tools like Network Access Controls (NACs) may see a virtual machine or container on a network.

But they'll often have limited visibility, collecting only MAC and IP addresses. (These challenges are compounded by the fact that tools such as NACs are difficult to deploy into cloud environments.)

## CAPTURING EPHEMERAL DEVICES WITH CYBERSECURITY ASSET MANAGEMENT

There are just too many pitfalls when it comes to using traditional asset management methodologies for identifying and managing ephemeral devices.

That's why it's critical organizations use tools **built specifically for cybersecurity asset management.**

This type of technology offers continuous asset discovery capabilities to identify and manage ephemeral devices.

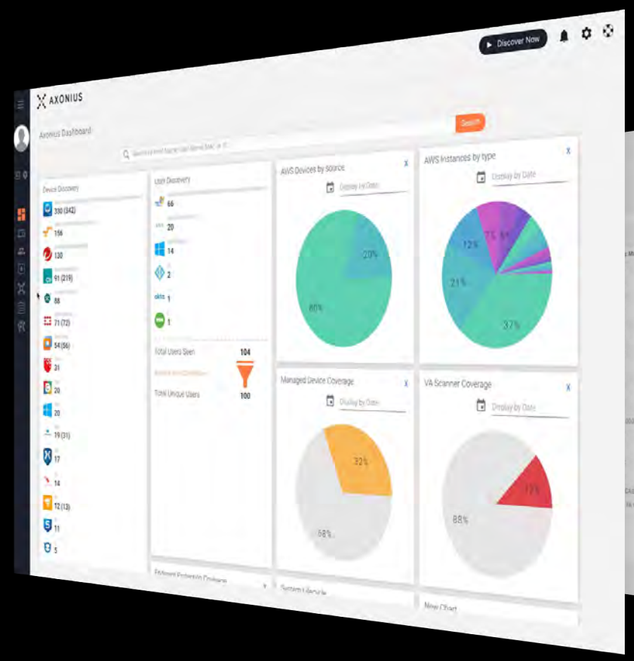
# Closing The Gap With Cybersecurity Asset Management.

Ephemeral devices pose a major challenge to organizations. They represent potentially millions of unsecured, vulnerable instances in an environment.

Even the largest cybersecurity team will tap out on attempting to find, manage, and secure them all – especially when the very nature of ephemeral devices means they often go undetected by traditional asset management methods.

**The good news? It doesn't have to be this way.**

Traditional methods may not cut it. But leveraging a cybersecurity asset management platform takes the question out of the equation by showing you all the assets in your environment – then helping you take steps to validate security compliance and automate remediation.




**Axonius can help you find, manage, and secure ephemeral devices – and everything else in your environment.**

LEARN HOW

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 250 security and management solutions, Axonius is deployed in minutes, improving cyber hygiene immediately.

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

**AXONIUS.COM** 