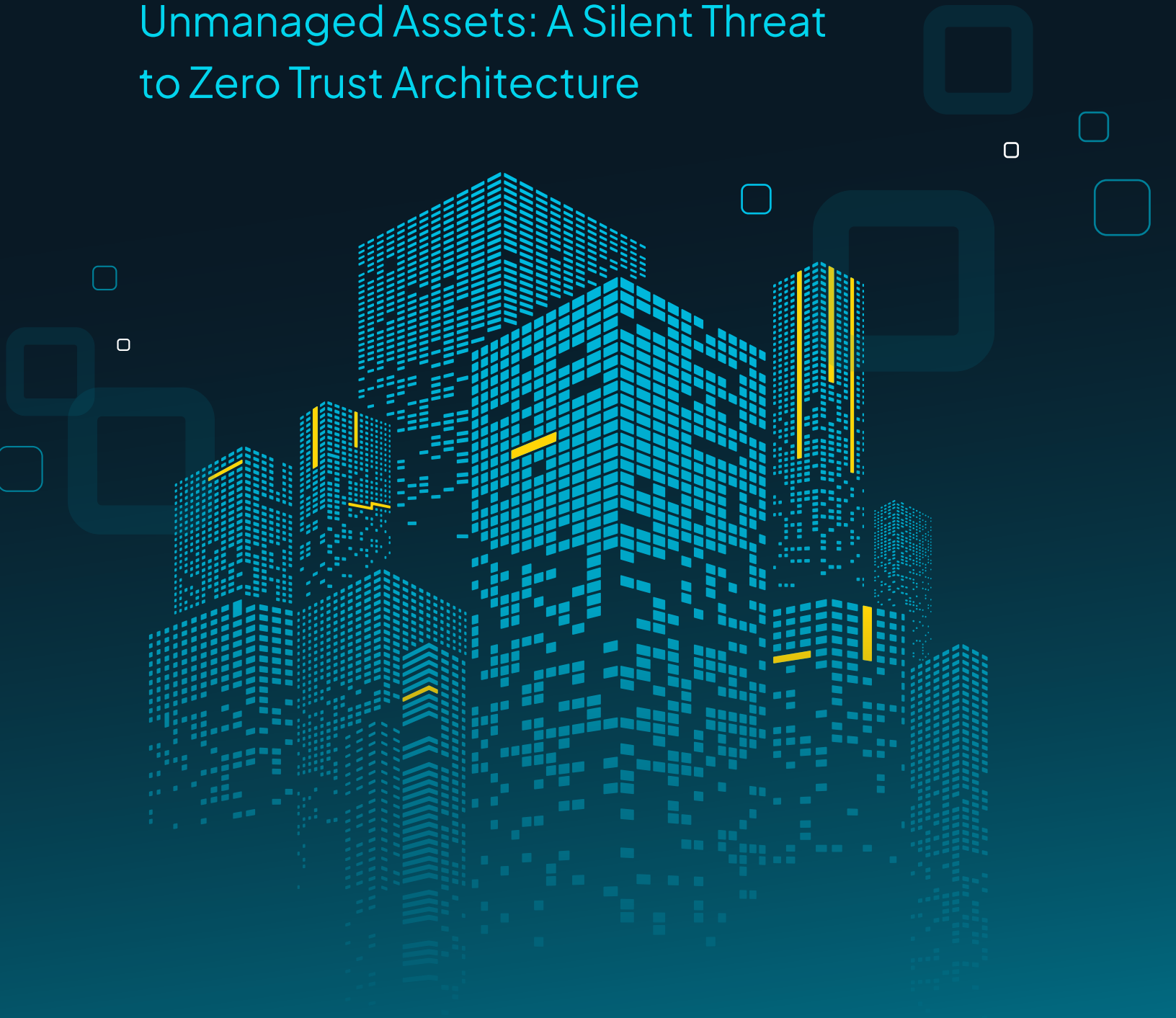
runZero

SOLUTION BRIEF

Unmanaged Assets: A Silent Threat to Zero Trust Architecture



This solution brief explores the obstacles hindering effective zero trust architecture (ZTA) implementation in federal agencies and proposes strategies to address them, emphasizing the importance of closing visibility gaps to enhance mission-critical security.

Unmanaged assets undermine zero trust architecture.

Escalating nation-state cyber threats targeting critical infrastructure in the United States have resulted in an urgent need for more robust cybersecurity measures, particularly within government sectors. In response, the president has issued several executive orders that focus on bolstering IT infrastructure security, notably advocating for the adoption of a zero trust architecture (ZTA) in **M-22-09**.

In the simplest of terms, zero trust means "never trust, always verify." In other words, never let an unverified device onto your network; it could be malicious. Despite its potential benefits, implementing zero trust in federal departments and agencies presents significant hurdles, including the proliferation of diverse and unmanaged devices.

Additionally, the evolving threat landscape, characterized by more frequent and perilous nation-state cyber attacks, like **Volt Typhoon**, has necessitated a critical shift in how government agencies approach cybersecurity. Traditional perimeter-based defenses are no longer sufficient to safeguard critical systems and data in the face of emerging challenges, such as cloud migration, BYOD policies, and the convergence of IT, OT, and IoT.

Devices that offer limited or low visibility can significantly outnumber devices that are highly visible to defenders. In a recent study of 4 million sampled assets, 45.46% of physical devices offered low visibility, with an additional 19.09% considered true dark matter. Read the **runZero Research Report, Volume 1** to learn more. ↓

Monitored Devices	Devices w/ Limited Visibility	Dark Matter
Laptops, servers, routers, switches	Smart TVs and projectors, wireless access points, printers	Thermostats, smart plugs, physical access control systems, aquarium pumps
		
High Visibility	Moderate Visibility	Low Visibility
Frequent human interaction with visibility via EDR and EPM, SNMP and other management protocols.	Some human interaction when people notice when they stop working. Particularly vigilant teams may monitor these devices more closely.	Often ignored by IT and invisible to security teams. Nearly zero visibility.
Updates are often automatic and en-masse, with rapid response to known threats.	Updates occur much less often, and sometimes never. Devices often require manual intervention to apply security patches and updates.	Updates are rare and may not even be upgradeable. Often run firmware that is many years out of date.

The proliferation of unmanaged assets.

The rise of unmanaged assets in network environments poses a significant challenge for organizations implementing zero trust architectures. These unmanaged devices, ranging from IP phones and cameras to printers and smart TVs, are proliferating rapidly, creating blind spots in security and management efforts. As the old adage goes, you can't protect what you can't see.

Traditional security and management tools start from a place of trust or management. These tools look for credentials or agent-based access within a managed asset to understand the risk profile. As a result, traditional solutions struggle to detect and secure unmanaged assets, leaving organizations vulnerable to potential security breaches.

Bad actors increasingly target unmanaged devices due to their susceptibility to exploitation. To address this issue, organizations need to develop strategies specifically tailored to discovering and securing unmanaged assets within their network environments.

Additionally, organizations should prioritize ongoing monitoring and risk assessment of unmanaged assets to prevent them from becoming weak points in their overall security posture. Unlike managed devices, which are consistently monitored by EDR and other solutions, unmanaged devices are often forgotten.

To protect unmanaged assets, organizations should implement a comprehensive strategy that includes the use of specialized technologies, ongoing monitoring, and thorough risk management practices. It's crucial to deploy tools that can identify all unmanaged devices within the network. These devices should then be subject to continuous monitoring to detect any unusual activity; regular risk assessments are necessary to ensure these assets do not become security vulnerabilities.

By effectively managing and securing unmanaged assets, organizations can strengthen their overall security posture and reduce the risk of potential security breaches.







Limitations and challenges securing today's complex threat landscape.

Unique Challenges in OT Environments:
OT environment components, such as SCADA networks and Programmable Logic Controllers, pose unique challenges because of their cybersecurity maturity, which differs from traditional IT environments. These systems are often overlooked or inadequately protected because reliability was traditionally more of a focus than security and they typically resided on their own network. With the proliferation of IT/OT convergence, this is no longer the case.

Criticality of Cybersecurity in OT Environments:
Given the increasing frequency and severity of cyber attacks by nation-state actors, strengthening cybersecurity in OT environments is crucial. Attacks on SCADA networks and PLCs can have severe and disruptive consequences, making it imperative to address vulnerabilities and enhance protective measures.

Need for Comprehensive Device Visibility:
A successful implementation of zero trust requires an understanding of all devices on the network, including those on various network segments, such as corporate, guest, wireless, administrative, and building networks. Additionally, connections to external networks and cloud services should be monitored.

Traditional security tools and methodologies fall short when it comes to securing OT and IoT assets.

Network Access Control (NAC) Limitations:
While NAC solutions aim to provide visibility into connected devices, they often fail to identify the information needed to determine if OT and IoT assets are risky. These solutions may only collect basic information, such as IP or MAC addresses, leaving critical details, such as device type, manufacturer, operating system, and vulnerabilities, unknown.

Endpoint Detection & Response (EDR) Doesn't Cover OT and IoT Devices:
Because agents cannot be embedded in OT and IoT devices, EDR solutions do not offer enforcement or detection for these types of assets.

Even with managed assets, such as laptops and servers, EDR solutions may be incomplete or misconfigured, leaving these assets vulnerable to attacks. This security gap highlights the importance of also properly monitoring and securing known devices.

In summary, achieving a zero trust environment requires overcoming various challenges, especially in OT and IoT contexts, by enhancing visibility, improving endpoint security, and addressing the unique characteristics of these environments. Additionally, organizations must prioritize cybersecurity efforts in OT environments to mitigate risks and safeguard critical infrastructure.

Applying zero trust to managed and unmanaged assets.

The principles of zero trust are the same for both managed and unmanaged assets, requiring accurate, in-depth visibility into:

- What each asset is (asset inventory)
- What data and which applications and network resources each asset needs to access
- What software vulnerabilities and other risks each asset contains
- What risk each asset poses to your organization

runZero and zero trust.

Legacy security solutions focus on managed devices, but are not designed for unmanaged or IoT devices. runZero is purpose-built for unmanaged devices, while also providing an overlay protection for managed devices and helping uncover unknown networks/subnets and shadow IT.

The runZero Platform also provides the most comprehensive asset discovery capabilities available today. It enables your agency to quickly drill into the details of every asset, including make, model, OS and firmware versions, owner, physical location, known vulnerabilities, risk to the organization, and more.

The combined capabilities in the runZero Platform are foundational for zero trust architectures; your zero trust systems can rely on trusted, actionable data from runZero to make better decisions relating to risk. And this software-only approach starts delivering value within minutes as opposed to agent-based solutions which can take weeks/months to deploy — and still not see or protect unmanaged assets.

25%
of assets (on average) found by runZero are previously unknown to enterprise customers.

Conclusion.

The recent zero trust-related executive orders are an acknowledgment that the threats to public sector infrastructure have never been greater. But agencies can't fulfill the zero trust challenge without seeing and securing 100% of their connected assets.

Implementation of a strong zero trust security architecture now requires that you also apply zero trust principles to the multitudes of managed and unmanaged IT, OT, IoT, mobile, and cloud assets that pervade the modern enterprise. Additionally, subsets of these assets don't support security agents, don't produce logs, and aren't easily patched. To realize the full promise of zero trust, you need specialized capabilities that deliver comprehensive visibility into every asset. And those capabilities must integrate with your existing zero trust tools and processes.

runZero delivers the most complete security visibility possible, providing organizations the ultimate foundation for successfully managing exposures and compliance. With a world-class NPS score of 82, runZero has been trusted by more than 30,000 users to improve security visibility since the company was founded by industry veteran HD Moore. Learn more on our website.

Test drive the runZero Platform for 21 days, with an option to convert to our free Community Edition at the end of your trial.

Try runZero for Free