Detecting Unseen Threats to Digital Infrastructure

How can public IT leaders ensure they have visibility into everything on their networks, including IoT sensors and other non-traditional devices? ***Mike Bimonte****, chief technology officer for the SLED public sector division at Armis, says the right software helps agencies detect threats other technologies miss.*

How do non-traditional devices contribute to the visibility gap in public sector IT?

Many agencies have visibility into traditionally protected IT devices. The visibility gap comes from the growing landscape of non-traditional devices, everything from cameras to speakers to thermostats to televisions. Endpoint monitoring software can tell agencies where they are with traditional devices. But they need to know where they *aren't* — that is, what are they missing if they can't see every device on their networks? A unified Asset Intelligence and Security platform can help provide full visibility and remediate vulnerabilities.

What's the difference between managed and unmanaged devices?

Managed devices are typical IT assets like desktop PCs and laptops — something you can load a software agent on to actively monitor. Unmanaged devices are things like cameras, TVs, smart speakers and Internet of Things (IoT) sensors. Unmanaged devices cannot use agents, so they must be passively monitored. Up to 90% of devices in enterprise environments are unmanageable with legacy IT security solutions.

Bad actors and nation-state attackers know managed IT devices are protected — so they're finding other ways in, via unmanaged devices.

Most of the nation's critical infrastructure is owned by the private sector. How can government and industry better work together to improve security of these assets?

President Biden's Executive Order 14028 mandates federal agencies to work more closely with service providers to secure cloud services, improve Zero-Trust security and establish baseline security standards. The objective is information sharing across public and private service providers to increase transparency around cyber threats. Public-private partnerships are the foundation for effective critical infrastructure security, and trusted information sharing among stakeholders is essential to the security of the nation's critical infrastructure.

How well are most states adhering to the standards in that executive order?

I've crisscrossed the country and spoken to a lot of state chief information security officers (CISOs) and CIOs. They've done a great job. The problem is the landscape has changed significantly as the number of unmanaged devices has exploded due to the convergence of IT, operational technology and IoT. They now need to close the visibility gap — gaining a holistic view of their entire environment and intelligence on every asset that touches their network.

The Infrastructure Investment and Jobs Act makes $1 billion available to improve cybersecurity. How can states access that funding?

The $1 billion commitment calls for each state to develop a comprehensive cybersecurity plan. States that put together this plan are eligible for monies to be distributed over three years. States must consult with localities to align their cybersecurity plan with the needs of local governments. States can then pass some of the funding in the form of grants to local governments within their jurisdictions.

Before joining Armis, you served as deputy IT commissioner for New York City. What were some of your biggest infrastructure security challenges?

Similar to today, I faced the same problem for the better part of two decades: I could not get complete visibility of what was running on my network. We tried a multitude of visibility tools, but we could never be 100% certain we knew what we had.

The foundation to any cybersecurity platform is knowing what's running on my network and in my airspace. If I can't see it, I can't secure it. Not having 100% visibility into network devices threatens the mission. A unified Asset Intelligence and Security platform like Armis eliminates gaps and visibility issues.

ARMIS.

Armis is the global leader in cyber asset security. Fortune 500 companies trust our real-time, comprehensive asset intelligence to deliver full visibility and automated enforcement across every connected asset and environment. Armis helps organizations across any industry continuously secure their entire cyber-asset attack surface.