The growing need for **asset management**

Eliminating blind spots is even more important now that IT resources no longer live in secure enclaves

Matt Kraning
CTO and Co-Founder, Expanse

DURING THE CORONAVIRUS pandemic, IT changes that might have happened over the course of years happened in a matter of weeks. In the past few months, the government experienced a surge in technology buying as agencies quickly adapted to support an increasingly remote workforce. Government leaders couldn't wait six months to procure new IT. They needed to move immediately.

As a result, a dramatic increase in the use of cloud-based technology is happening, but it is happening without a central governance solution. That lack of visibility is creating risks across government and in the private sector.

Avoiding new security gaps

More people are acting in decentralized ways right now, but that decentralization is part of a larger trend. Multi-month strategic plans are becoming a thing of the past, and fewer IT purchases go through the CIO's office. According to researchers, over half of IT spending is now done by line-of-business leaders, not by a central function such as a CIO.

Therefore, agencies must have a simple, comprehensive process for gaining insight into technologies as they're added to the network. Otherwise, more security gaps will invariably occur.

Those gaps are exacerbated by the pandemic because agencies cannot easily add secure data center capacity to support large-scale telework. It's much easier to use a government purchase card to address a pressing need for videoconferencing, for example. But even approved cloud products and services are not secure by default. They need to be continuously monitored.

Knowing what you need to defend

IT teams must be able to see and monitor new technologies so they can secure all the systems, tools and people involved. In other words, they can't protect something they don't know they need to defend. A complete asset inventory helps agencies understand the entirety of their attack surface so they can protect it. Those insights are also essential for efficient budgeting and planning.

Once they have that inventory, agencies should consider moving to zero trust architectures or similar approaches that assume a well-defined perimeter no longer exists.

The need for a rigorous approach to asset inventory and management has been important for some time, but the pandemic has added an even greater urgency. It can be difficult for agencies to know and understand their entire attack surface. That's where an industry partner like Expanse can help. We provide that central inventory view so that agencies can see and manage their entire attack surface no matter how quickly the IT environment evolves. ■

Matt Kraning is CTO and co-founder of Expanse.