Reclaiming control over complex IT environments

As the network perimeter disappears, agencies need comprehensive visibility into all their systems

Brandon Shopp
Group Vice President – Product, SolarWinds

THE PANDEMIC SENT MANY government employees home to work remotely, and we can expect to see a mixed workforce in the future as the public and private sectors adapt to allowing people to work from wherever they happen to be.

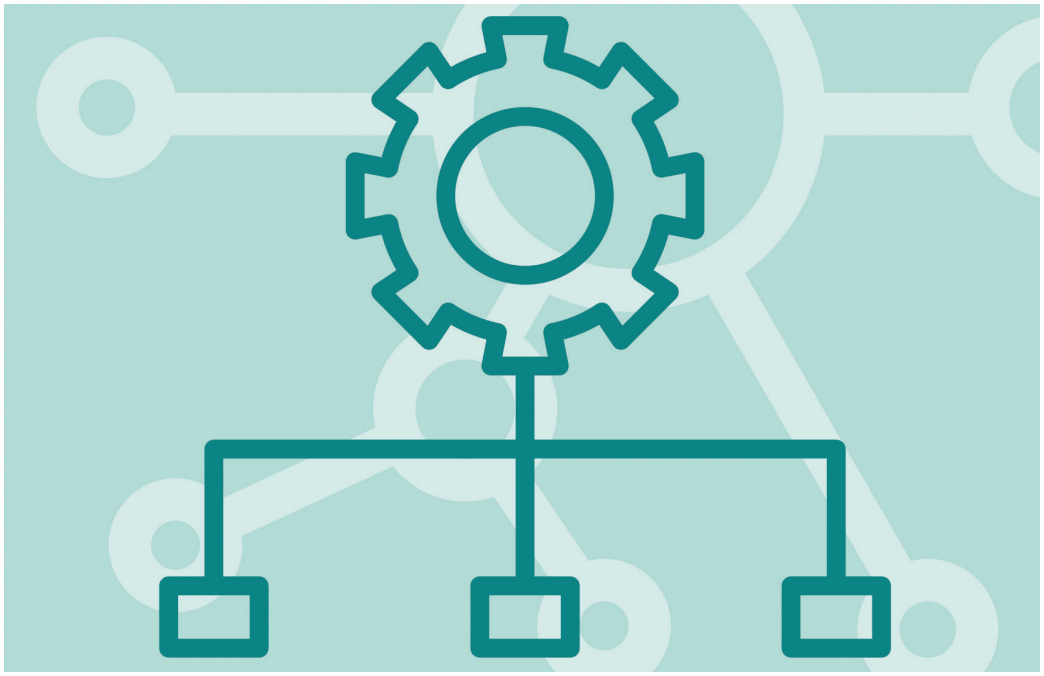
When employees were sitting in a government office behind a firewall, IT administrators had a clearly defined perimeter to protect. Now IT administrators are still focused on protecting the agency's mission and assets, but the responsibility has become more difficult because they've lost some visibility and control over the infrastructure.

In response, many organizations are moving toward strategies based on zero trust, which requires validating users and devices before they connect to government systems, or least privilege, which involves only giving employees access to the resources and applications they need to perform their jobs. Zero trust and least privilege require continuous monitoring and a risk-based approach to adding or removing authorizations.

Continuous monitoring of on-premises and cloud

Endpoint detection and response solutions are also increasing in popularity as agencies shift their focus from protecting an increasingly blurry perimeter to protecting the endpoints that access the network — whether they're laptops, desktop PCs, mobile phones or virtual machines. At SolarWinds, for example, employees and contractors cannot connect to our corporate network unless CrowdStrike Falcon endpoint protection is running on their devices.

As IT environments become more complex, agencies must have visibility and control over all their on-premises and cloud environments. Virtualization and cloud technology have helped agencies modernize their IT systems and quickly spin up new storage and compute resources in response to demand. However, someone must ensure those resources are configured properly from the beginning and then continue managing and monitoring them to prevent potential security vulnerabilities. The challenge is complicated by the fact that although there are some similarities, vendors often take a proprietary approach to their cloud environments.



Furthermore, many activities rely on multiple environments. A database, for example, might be hosted on-premises but is used by an application

Shutterstock/FCW Staff

> Instead of seeing just part of the puzzle, agencies must be able to see the full puzzle so **they can quickly identify and remediate a threat.**

in the cloud. This hybrid deployment model means IT administrators must have an appropriate level of visibility into both environments through a single pane of glass.

Seeing the full puzzle with a hybrid SIEM

To achieve visibility into a complex mix of IT environments, agencies should implement a hybrid security information and event management (SIEM) solution for a holistic view of their environments not just from a security perspective, but from a performance and health perspective as well.

Agencies must be able to understand the potential weaknesses and vulnerable entry points in their IT environments. They should make sure they have visibility into the security health of their systems so they can achieve insights that are as comprehensive, broad and deep as possible. This means deploying a hybrid SIEM tool capable of understanding and incorporating data from on premises and in the cloud into a single, comprehensive view.

Instead of seeing just part of the puzzle, agencies must be able to see the full puzzle so they can quickly identify and remediate a threat. If agencies have the appropriate controls and monitoring in place for their IT environments, they can quickly catch a potential vulnerability before it becomes an issue for the organization. ■

Brandon Shopp is group vice president - product at SolarWinds.