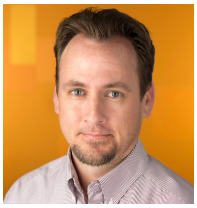
Navigating Security in a Fast-Changing Environment



Hybrid work, multi-cloud deployments and increasingly vulnerable software supply chains are just a few of the cybersecurity challenges that organizations face today. ***Brandon Shopp****, group vice president of product for SolarWinds, discusses cybersecurity trends, threats and solutions organizations should keep top of mind as they move into the future.*

The cybersecurity landscape has changed significantly in the last two years. Where should organizations focus as they assess their risk posture?

Folks are no longer working solely in offices sitting behind an enterprise firewall, so environments are increasingly perimeterless. In addition, workers are using their home wireless networks and cable providers to access the internet, which increases the number of risk points. In terms of threat actors, we're seeing an uptick in cyberattacks from foreign governments and the general hacking community — that is, civilians or organizations often motivated by money.

What challenges do organizations face when managing IT security across multicloud hybrid environments?

The cloud makes it easy to spin up new resources, but it also creates new risks. Many data leaks happen because somebody rolls out something quickly in the cloud but doesn't realize they have to configure it further to properly secure it. Additionally, organizations are using multiple clouds from multiple vendors on top of on-premises architecture. Securing multicloud hybrid environments requires a new level of skills and technology. Each cloud provider also tends to have its own tools and procedures, which the organization's IT team must learn.

What strategies can help protect data in today's complex environments?

We're seeing more organizations adopt Zero Trust and least privilege strategies instead of relying on legacy technologies like VPN. With Zero Trust, agencies can make data and applications accessible to the right people, no matter where they are without funneling those resources through a VPN. With the least privilege model, agencies can make sure people only have access to the resources they need. These strategies limit the potential damage to an organization if someone's credentials get compromised.

How can organizations — especially those with limited resources — simplify management of IT security?

Organizations with limited resources usually can't afford the high salaries cybersecurity professionals command, so many of them use managed security services providers (MSSPs). MSSPs can hire top security professionals and distribute their cost across multiple customers, which creates economies of scale. In addition, we see organizations leverage software-as-a-service (SaaS) and cloud service providers. Agencies still must configure the software properly for usage in their environment, and they must manage and maintain configuration settings. But they're not running the software and infrastructure on premises, so they don't have to secure it or patch software. It's a shared responsibility model to some degree.

How should organizations secure their supply chain from highly sophisticated cyberattacks?

Threat actors are constantly devising new attacks and methodologies, so organizations must stay on top of trends and constantly evolve how they build and secure their software supply chain. It isn't a "set it once and you're good" kind of thing. President Biden's executive order on improving the nation's cybersecurity and some bills going through Congress will help address some of the issues. Among many things, the executive order mandates service providers disclose security incidents or attacks. It's also important to establish a community where security professionals across the nation can exchange security and threat information. You don't want to solve these things in a vacuum. We're stronger as a community than as individual organizations.

Quantum computing is on the horizon. How will it impact cybersecurity, and what can organizations do to get ahead of the curve?

Quantum computing will enable the storage, processing and analysis of data at rates unfathomable today. A password that normally takes years to crack will be decrypted in a matter of minutes or hours with quantum computing, so the encryption technologies and techniques in place today will all be at risk. Using the full range of standard cybersecurity best practices — including credentials, least privilege and Zero-Trust strategies — can help organizations stay ahead of the threat. Even if they can't keep the bad actors out, these practices can help limit the scope of the damage.

Learn more at **Carah.io/GT-22-Cyber-SolarWinds**

solarwinds government

Discover tools to implement a zero-trust strategy

Visit solarwinds.com/government