How-to

Alamy

SECURITY > VULNERABILITIES AND THREATS

How To Fight Security Tool Sprawl

Security tool sprawl is a challenge that organizations of all sizes contend with today. Explore the factors that contribute to tool sprawl and how to get your house in order.

Karen D. Schwartz | Jan 12, 2023

If you can't solve a cybersecurity issue with the tools you have, you can just buy another one, right?

This kind of thinking is guaranteed to lead to security tool sprawl, but many businesses find themselves doing just that. It's not uncommon, in fact, for small companies to have more than a dozen security tools, while larger businesses often have 50 or more. And the number of tools continues to grow: Security professionals add an average of six security tools every 12 months, according to security operations platform firm ReliaQuest.

What Is Security Tool Sprawl?

Related: 8 Proactive Cybersecurity Technologies to Watch in 2023 most organizations receive more than 500 cloud security alerts daily, and between 20% to 40% of those alerts

hi

on

Why Platform Engineering Is the Future of DevOps and SRE

5 Common IT Operations Security Mistakes

ıri

on

difficult to coordinate policy and controls across an overabundance of tools.

fu

on

an

and

Organizations Seek Platform Team Expertise as DevOps Matures

How Registered Apprenticeships Could Ease Tech Talent Shortage

How do companies get to the point where they are overloaded with often overlapping security tools? It's due to insecurity, said Mike Lloyd, CTO of cloud security firm RedSeal.

"It's an arms race and the bad guys keep innovating, which means we need new countermeasures," Lloyd explained. "Companies feel like they can't decommission older countermeasures, and threats keep evolving. So they keep adding tools and nothing falls off the backend."

Organizations also face an endless cycle of temptation. Security staff may attend conferences or talk to peers and learn about the best new product.

"If you go to RSA, you'll see two football fields full of vendors, and it's very tempting to keep buying [new tools]," said Joey Johnson, CISO of Premise Health, a 6,000 employee healthcare company. "They are chasing the curve by trying to address all issues. They end up with a huge number of security tools—often way too many for their companies to actually operationalize correctly."

But the strongest driver for security tool sprawl, Johnson said, is the "defense in depth" mantra.

"A lot of times, organizations will see a cool tool that will help them do incident response better than they do now, so they buy it. But that tooling may be built to address security at a greater maturity state than their underlying operations," Johnson said. "For example, the tool may assume that you already have an in-house SIEM platform and an orchestration platform, but if [you] don't have that, [you] could end up having to buy even more tools to plug the holes."

Whittling Down the Security Stack

Reducing the number of security tools to a manageable amount is critical to preventing overlap, identifying gaps, and improving an organization's security posture and effectiveness. The goal is to shrink the stack to the tools that are essential, eliminating unnecessary complexity so that limited teams can get maximum defensive benefit from a handful of technologies.

The first step for reducing the tool stack is to conduct an audit. Lloyd recommended using the OODA (Observe, Orient, Decide, Act) framework, which helps organizations make effective decisions by breaking the process into phases.

Johnson also advised doing what he calls the "least sexy thing": looking for free ways to reduce the threat surface. That means examining if you are getting all the appropriate logs from your systems, the logs are tuned correctly, and patch management is working properly.

"If you can't solve those fundamental security hygiene challenges, you'll still have the same basic problems, no matter how many tools you throw at it," Johnson said.

Turner added that adopting a zero-trust model may help. Zero trust aims to lock resources down before they can be attacked, which should mean that fewer tools, especially the incident response tools, are needed.

In addition, before adding new tools, make sure you really need them and have the bandwidth to use them. "When somebody on my team asks for something new, I ask them to justify the purchase by looking at our existing tech stack and telling me three ways we could solve the same problems with the tools we already have, or at least how far we could get with our existing tools," Johnson said. He noted that the team will sometimes discover a newly released module for an existing tool that will do the trick.

In other cases, the request for a new tool may be spurred by a critical risk. However, the IT infrastructure simply isn't ready for that tool. "If we haven't gotten the tools we bought last year running, adding a new one isn't going to help," Johnson said. "We still haven't solved the last big risk that justified us going out and spending money."

It's also helpful to simply look at your threat posture and how much risk you're willing to accept. Knowing the acceptable level of risk tolerance should guide IT security teams to the right toolset and ensure that security products contribute toward those risk goals.

Often, fighting security tool sprawl comes down to the simple things – that is, optimizing what you have; making sure you can't solve a problem with your existing tools; and ensuring that business, IT, and security teams work are on the same page.

About the author

Karen D. Schwartz is a technology and business writer with more than 20 years of experience. She has written on a broad range of technology topics for publications including CIO, InformationWeek, GCN, FCW, FedTech, BizTech, eWeek and Government Executive.