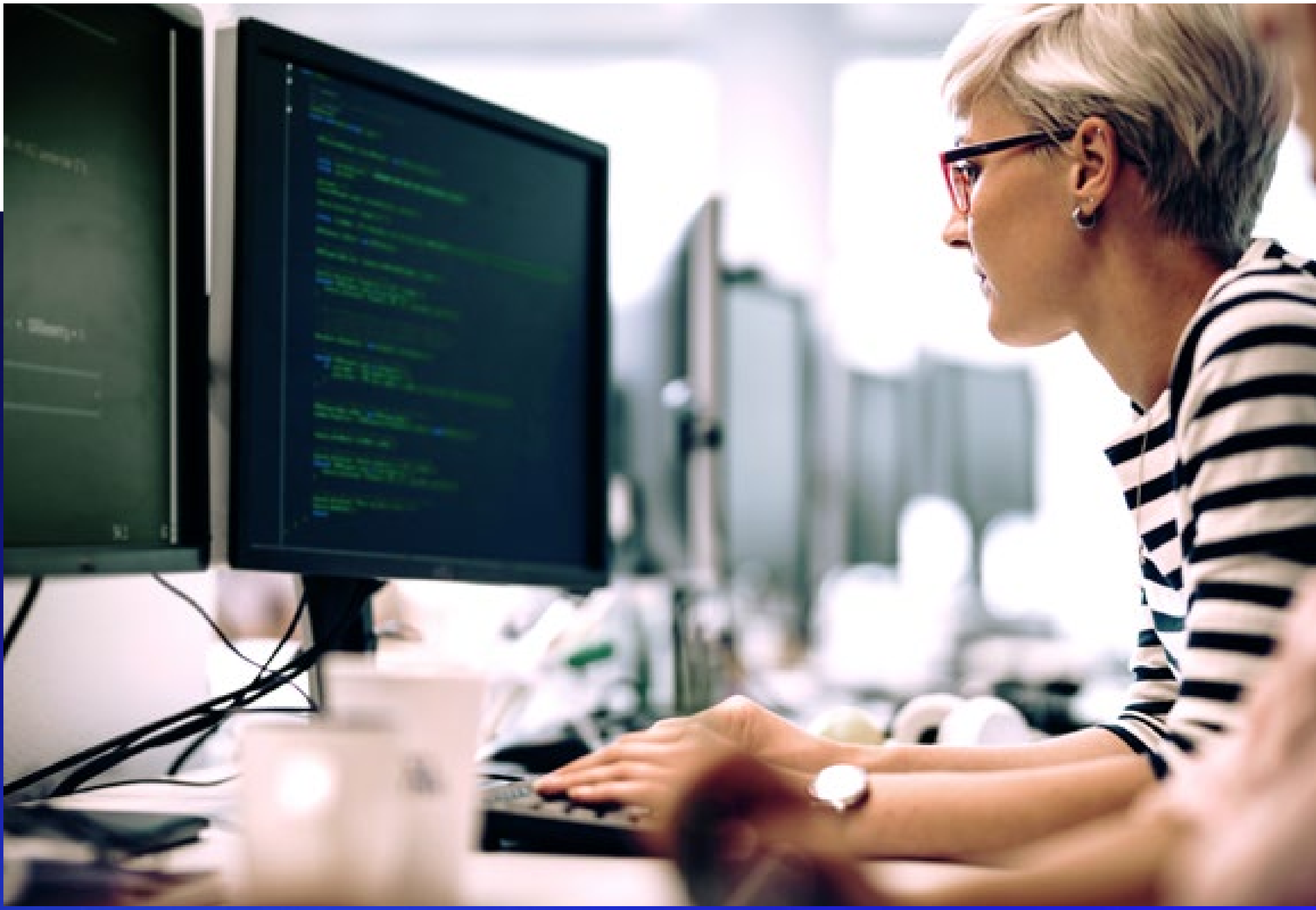
Secureworks®

WHITE PAPER

7 Ways to Identify Whether Your Security Stack is Too Complex



Complexity is a part of life for security teams. New tools are released to combat new threats, adding layers of complexity to security environments. Most security organizations are aware that this complexity may be causing problems, but struggle to assess how and where.

The bad news is there's no objective measure of complexity. Whether an environment is too complex depends on a variety of factors, including the size and industry of the company, its risk profile, and more. The good news is, there are several warning signs that indicate excessive complexity in an environment. The following list is designed to help you assess whether your environment is too complex.

While newer CISOs often inherit confusing configurations and contracts from predecessors, CISOs who've been with a company a long time sometimes forget about older tools that may have fallen out of favor.

Sign 1:
You're Reactive, Not Proactive

Complexity leads to reactivity. If you are constantly wrong-footed by events and incidents, it's a significant sign you should look to simplify your stack. A key indicator of this is a volume of alerts that your team struggles to process. In this situation, analysts often can't identify real threats until long after they happen. Things are frequently made worse for analysts by an overabundance of platform management and administration tasks, as well as the need to learn an often dizzying array of tools.

Sign 2:
You Can't Identify Where All the Budget is Going

If you're struggling to track where all your budget is spent, that can be a bad sign. In this circumstance, CISOs need to find where the extra budget is assigned. If a CISO is struggling to identify the spend, and the organization is spending much more than previous companies the CISO has worked for, it's likely there is a complexity issue. While newer CISOs often inherit confusing configurations and contracts from predecessors, CISOs who've been with a company a long time sometimes forget about older tools that may have fallen out of favor. Security has changed at a rapid pace over the last 10 years. As the industry has released new tools to tackle new threats, older tools are forgotten or ignored. It pays to take regular inventory of your environment. Remember that you should be able to justify return on investment (ROI) for every tool in your stack.

Sign 3:
Multiple Tools are Doing the Same Thing

Running multiple tools in parallel that do the same thing is another common sign of complexity. Some security teams have four or five programs running vulnerability scans at the same time, for no good reason. One should be enough. In these situations, the programs can generate a lot of noise that negatively impact KPIs for the security team and leave the CISO thinking they are receiving bad information from the team.

Sign 4:
Staff Struggles to Master the Tools

Every CISO should have confidence in their analysts, and the tools available to them should enable – not hinder – their success. If your security staff is struggling to master the tools in your stack, this is a strong signal that there may be too many. The team's time is divided between learning five tools that do similar things, rather than mastering one or two. The goal should be to arm your analysts with a couple of tools they can truly master. As before, the reason there are often too many tools in an environment goes back to solutions proliferating as the threat landscape evolved over the last five to ten years.

If your security staff is struggling to master the tools in your stack, this is a strong signal that there may be too many.

Sign 5:
You're Protecting Things That are Already Protected

People worry about the implications of moving to the cloud for security. Is it wise to hand over sensitive data to a third party? The answer is often 'yes.' A good indication of this is that cloud providers have been largely unaffected by the major ransomware attacks of the last five years.[1] While no solution is immune from attack, it's wise to think about your environment and identify areas where you might be duplicating security controls. Removing those controls will both save you money and reduce complexity.

Sign 6:
You're Spending a Lot of Time Documenting Tools

It's good practice to document tools so that common operations are repeatable and the security team can learn from their experiences. The goal is to pass on knowledge and save time. But there are warning signs to look out for during the documentation process that could indicate an excess of complexity in your stack. For example, if the team feels like they are documenting every operation for a tool, that's a sign something is wrong. It could be that the tool itself is not the right one for you. Or, it could mean something is wrong with the tool configuration. You can apply the same measure to your whole stack. If the team spends a lot of time documenting across all the tools in your stack, it's probably too complex and the tools may not be user-friendly enough.

Sign 7:
You've Forgotten About Some Legacy Tools

Here's a common scenario: A new CISO is hired, brings their favored vendors and maybe even some staff. In the process, older systems sometimes are forgotten. It's natural for CISOs to operate in this way and often makes more sense for them to play to their strengths. However, it also pays to guard against overlooking legacy systems that are still switched on. If a legacy system is still creating alerts, these can be missed. Worse, if a legacy tool catches an incident but nobody is reporting on the tool, that incident could go unnoticed. Even if an organization doesn't have a new CISO, this situation can be a result of rapid adoption of new technologies.

[1] Dark Reading, Cloud Backup: How It Can Protect Against Ransomware

Thinking About How to Reduce Complexity

Complexity is an expected part of cybersecurity today, but that doesn't mean it has to impact the efficacy of what you do. If after reading this list, you think complexity is causing some of the issues you see in your environment, it's time to start thinking about what to do next. Any solution should involve a holistic look at how security and other IT functions are cooperating. Functions like cloud computing and access control are critical to security, but these sit under IT in many organizations. You should also begin by identifying which assets are most critical to your organization and find ways to protect them with as few tools as possible. Cybersecurity frameworks like NIST offer a great way to help you build an efficient program. Of course, no framework offers a one-size-fits-all solution. You'll need to study any framework so that you can apply it to your own unique circumstances. It will also take time to educate other areas of the business about how a framework relates to their roles and responsibilities. The responsibility for security shouldn't lie solely with your team.

Begin by identifying which assets are most critical to your organization and find ways to protect them with as few tools as possible. Cybersecurity frameworks like NIST offer a great way to help you build an efficient program.

Secureworks®

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world.

We combine visibility from thousands of customers, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our customers a cyber-defense that is Collectively Smarter. Exponentially Safer.™

Corporate Headquarters

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp

Availability varies by region.