Secureworks®

WHITE PAPER

How to Consolidate Your Cybersecurity Stack

Complexity is a fact of life for most people in cybersecurity. The last 10 years saw rapid innovation by threat actors with the industry running to catch up. As a result, most security environments now consist of a plethora of tools designed to tackle a variety of potential issues. There is now a staggering 47 layers in the average cybersecurity stack,[1] and often significantly more. Making matters worse is the fact many of these tools don't work well together.

While the future of security looks bright, as software and AI technologies combine to simplify security operations, it will take years before those technologies are widespread, and possibly longer before security teams get comfortable with the idea of removing tools from their environments. The simple fact is that today, most security environments are still too complex. This complexity often increases risk and commonly creates blind spots where threat actors seek opportunity. Many security leaders want to know what they can do to consolidate the security stack they are using today.

If you've determined that your stack is too complex, there are several approaches you can use to consolidate it. Start at the level of strategy, not tactics. This includes looking at the technology, as well as the people and processes within your organization. It requires cross-functional collaboration in your company and benefits from the use of industry-standard frameworks. Here's how to consolidate your security stack.

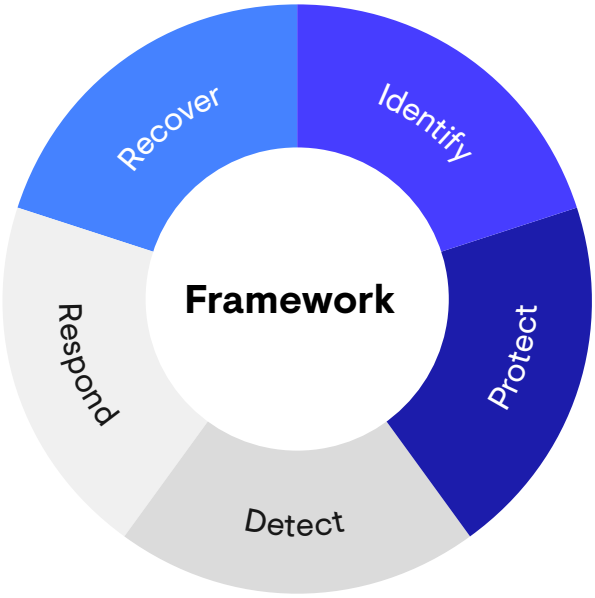
Today, most security environments are still too complex. This complexity often increases risk and commonly creates blind spots where threat actors seek opportunity.

Use a Framework

The discussion about which cybersecurity framework is best seems to never end. The important thing is that you identify a framework you can use to shape and assess your environment. A major benefit of frameworks is that they offer a way to bring order to the more chaotic parts of any security stack. Frameworks help your stack stay as lean as possible by giving a benchmark to measure against. Each framework is different, and it's up to you to find the one that best suits your organization. We often recommend the cybersecurity framework from the National Institute of Standards and Technology (NIST), but you may find another suits your operation better. Although the NIST framework came from the Department of Defense, it is widely applicable to most public and private organizations. The framework identifies 5 functions your environment needs to balance to reduce risk.

[1] Ponemon Institute via Business Wire, 53 Percent of IT Security Leaders Don't Know if Cybersecurity Tools are Working Despite an Average of $18.4 Million Annual Spend

Availability varies by region. ©2020 SecureWorks, Inc. All rights reserved.



While new tools often seem attractive, replacing a well-functioning tool that is already in your environment is a big investment of time and money.

This framework offers a useful barometer for your operation. After applying the framework, if you realize 80% of your tools are focused on the protect function, that's a sign your environment is imbalanced, and something should change. What cybersecurity frameworks don't offer, however, are hard and fast rules that can be applied with minimal effort. Each one requires significant work to apply as each environment is different, but the time is worth it.

Identify Which Tools Perform Critical Functions

There aren't any shortcuts to consolidating a stack. Most security teams will need to take inventory of the tools they have to fully understand what is working and what isn't. As part of this process, it's important to identify what each tool does and how well it does it. If a tool performs an important function well, it might be worth keeping it in place. While new tools often seem attractive, replacing a well-functioning tool that is already in your environment is a big investment of time and money.

That doesn't mean old tools can't also sometimes create problems. Many security teams are stuck with legacy tools that the organization still uses, which are sometimes decades old. In these situations, the legacy system often creates enormous risk. In an ideal world, most security departments would replace these tools for something better, but many organizations are reluctant to replace legacy tools for a variety of reasons. The best thing to do is to isolate and segment the tools to limit access to the rest of the organization.

Availability varies by region. ©2020 SecureWorks, Inc. All rights reserved.

Find Easy Candidates for Consolidation

Consolidation depends heavily on each individual environment, so there are no easy fixes. Despite this, there are common candidates for consolidation, which is where any security organization should start.

Asset Management

Understanding what assets you have and where they are is a critical part of a security program. It's a simple task that doesn't require anything complicated. One tool can do the job and do it well.

Firewalls

Are you running multiple firewalls? This is something we see regularly in customer environments. As with asset management, one good firewall is enough for most environments. If you feel like you need a backup, it could mean the firewall you're using isn't working well for you.

Endpoint Protection

Endpoints are another area where we sometimes see organizations running more than one tool. If you've done your research well, one endpoint tool can cover you. If you have doubts about any of the tools you're running to monitor endpoints, it might be worth considering sourcing a more robust endpoint protection tool that you feel confident with.

Consider Correlation Tools

Adding tools can sometimes simplify and consolidate your security stack, even if that seems counterintuitive at first. Many associate new tools with a learning curve and investment of time. While that's true, choosing the right tool can pay off when looking longer term. It all depends on the tools you choose and the function they fill.

Supplementing a stack is increasingly important. The sheer number of tools generating alerts and streams of data is often unmanageable. Correlating all that data is a crucial step in reducing blind spots and detecting threats. Threat intelligence is a great place to start. Rather than checking multiple feeds and cross-referencing against telemetry, we recommend finding a solution that can correlate your telemetry against threat intelligence automatically. That saves time, simplifies your operation, and helps you stay ahead of threats. Data loss prevention (DLP) software is another good candidate for correlation. DLP software is often exhaustive and requires significant time and energy to implement. However, DLP can miss threats that come from inside your organization, so a correlation tool can help you get the context you need to identify threats that DLP might miss.

Rather than checking multiple feeds and cross-referencing against telemetry, we recommend finding a solution that can correlate your telemetry against threat intelligence automatically.

Availability varies by region. ©2020 SecureWorks, Inc. All rights reserved.

Secureworks®

Don't Forget to Patch

A thorough patching program helps you stay ahead of threat actors and reduce complexity. Companies running a jumble of systems with a poorly organized patching program leave open multiple points of entry for threat actors. Not only that, but the complexity makes it harder to identify threats and triage important alerts. Create a plan to update each system at the earliest opportunity to prevent them from becoming attack vectors. And please, whatever you do, don't run anything on an outdated or unsupported operating system! If your organization has any systems running on Windows XP, prioritize updating those first. Windows XP makes life easy for threat actors.

Look at Software

Recent advances in technology are making correlation easier and more effective than ever. Key among those advances is the combination of software and artificial intelligence technologies informed by threat intelligence and security expertise. The right software product can analyze telemetry from a variety of sources, including network, endpoint, and cloud, using threat intelligence to identify potential threats almost in real-time. This can offer significant cohesiveness to environments composed of disparate tools with little cross-communication and speed up detection and response as a result. Some software products include features that also make event investigation easier.

When considering software, remember that no tool is plug and play. You'll need to spend time installing and understanding how to use any piece of software for your situation. The best software is informed by deep security and data science expertise, from teams who have been on the incident and threat research frontlines. While software can simplify things for your operation, it still pays to take inventory of your environment and consolidate where possible before purchasing any new tools. Reducing complexity and blind spots in your stack increases the effectiveness of any new investment.

Beware the Single Point of Failure

Consolidating a complex security stack can improve the efficacy of your operation, but the process is not without its own risks. It's crucial when you consolidate that you don't create a single point of failure anywhere in your environment. For example, if you consolidate down to one firewall, you need to ensure that your stack will still catch any potential threats that might come through if the remaining firewall fails. Any change in security introduces new risks, and consolidation is no exception. The process should begin with identifying those risks and assessing how to address them.

The benefits are huge. The consolidation process will help you identify and understand the risks of your current setup, including areas where threat actors could get in unnoticed. As a result, you'll find it easier to identify areas where spend is necessary and will have the knowledge needed to make a robust case for any additional spend. You'll develop a deep understanding of your environment that exceeds your knowledge before you started.

The consolidation process will help you identify and understand the risks of your current setup, including areas where threat actors could get in unnoticed.

Availability varies by region. ©2020 SecureWorks, Inc. All rights reserved.

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. ©2020 SecureWorks, Inc. All rights reserved.