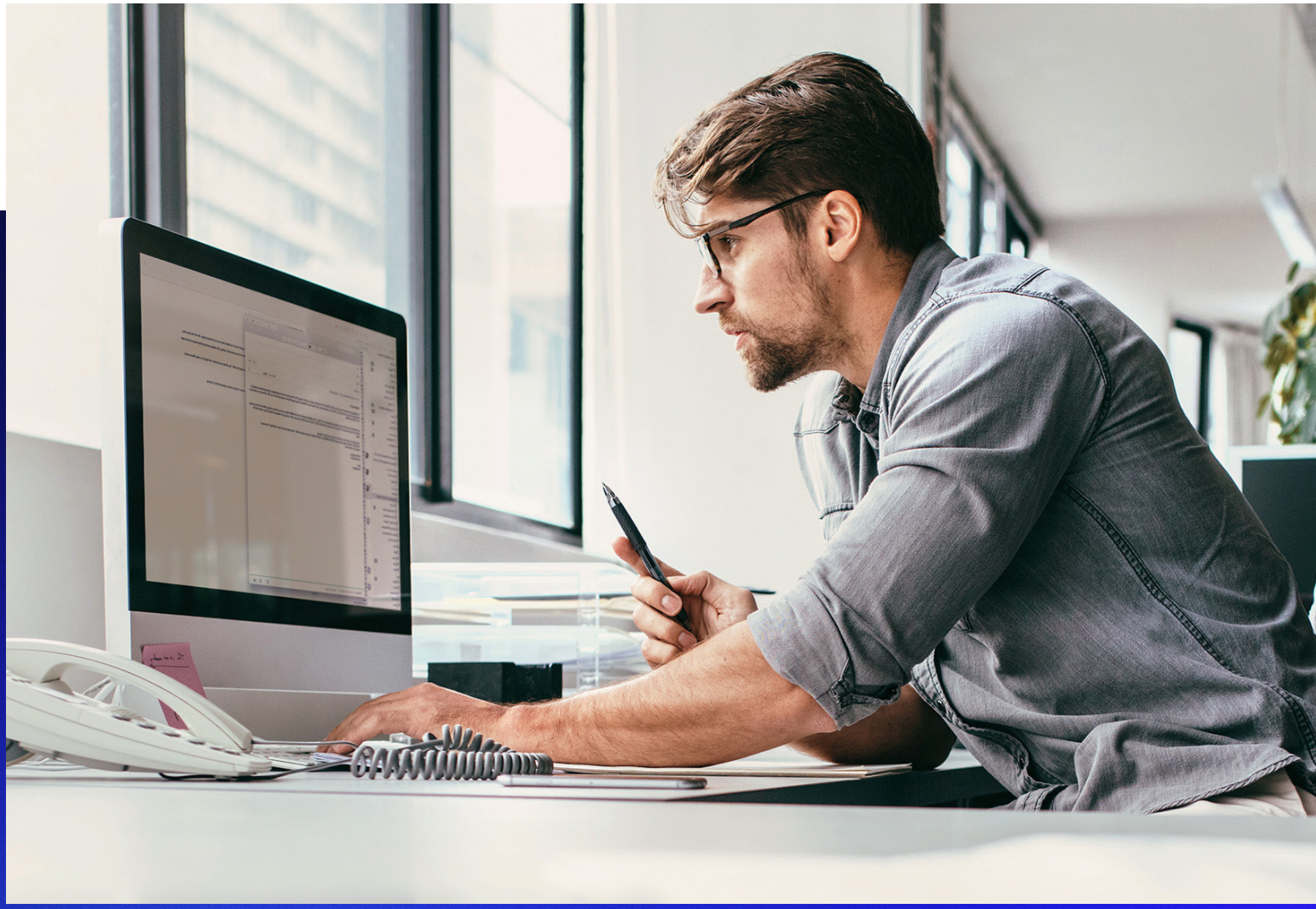
Secureworks®

WHITE PAPER

Evaluating Your Security Program to Meet Future Cybersecurity Needs

Keys to Refreshing Your Security Architecture



A widened attack surface on top of global, newsworthy events has created new opportunities for cybercriminals to attack organizations. Secureworks Counter Threat Unit™ (CTU) researchers have tracked instances of nefarious threat actors leveraging current events to entice victims to open malicious links and attachments.[1] As our world evolves, so do threat actors.

Complicating this constantly evolving threat landscape are the compliance directives that organizations must follow for their regions/countries and industries. For example, the California Consumer Privacy Act (CCPA), which went into effect this year, will be one of the most dramatic data privacy acts for companies and is estimated to impact 75% of California businesses.[2] In this complex environment, companies today are looking beyond simply checking boxes for compliance toward seeking to build adaptive security systems that can work within compliance frameworks and anticipate future needs.

With all this uncertainty, many organizations are looking at their security program and wondering if it is up to the challenge. Keeping up with the latest threats and addressing regulatory requirements – all while your business is changing – is a tall order without outside expertise. But searching for the right vendor to determine how to best address your organizational needs and obtaining buy-in from different stakeholder groups can be a tough process. If done in haste, security leaders may find themselves with an incomplete strategy that doesn't protect their organization from risk and is not backed by the confidence of senior leadership.

In this white paper, we'll review the steps to consider when undertaking a new vendor search to update your security program, as well as moving your program through from conception to implementation.

Maturity modeling is a pragmatic methodology for evaluating your cybersecurity program's strengths and identifying next steps in your security journey.

Defining Your Vendor Needs Through Maturity Modeling

Although every organization wants to fully address current security needs and proactively adjust its security architecture for future needs, many teams struggle to achieve this. Regardless of your organization's security maturity level, regularly reassessing your security architecture and keeping it relevant is the only way to ensure that the organization's security needs are being met. Even better is finding a vendor with the flexibility to evolve with changes in business and security circumstances.

[1] Secureworks Blog, How Cyber Adversaries are Adapting to Exploit the Global Pandemic

[2] National Law Review, Five Things to Do Now to Prepare for the CCPA Enforcement Deadline on July 1, 2020

Secureworks®

Maturity modeling is a pragmatic methodology for evaluating your cybersecurity program's strengths and identifying next steps in your security journey. The process measures your current state of maturity and finds areas that will progress your security posture, enabling organizations to confidently communicate to their leadership and stakeholders about your current state of security. The outcome helps clearly pinpoint where shortfalls exist, what is needed to overcome them, and the roadmap for getting there. Organizations can leverage the results to identify and prioritize the right initiatives so they can invest more wisely, identify a vendor that can meet their needs, and protect business value.

The process of maturity modeling will also help address the three main questions security leaders commonly ask:

- How can I locate resources and identify where to prioritize my investments while meeting regulatory and compliance needs?
- How can I align my risk management strategy with my organization's business goals?
- How can I further my organization's digital transformation without adding risk?

The maturity modeling process is often undertaken with a vendor who can bring context from a global customer base, help you fully understand your results, identify the top challenges, and offer solutions that meet your needs. The Secureworks Security Maturity Model takes a holistic, risk-based, business-driven approach to evaluating cybersecurity maturity based on an organization's business operations and risk profile. The model combines control requirements from well-known frameworks such as NIST and ISO27001 to create a consolidated set of benchmarks that address the most critical security domains and capabilities to meet today's risk-focused requirements. Together, we can work with your organization to reimagine your security architecture.

The outcome from this process should be a partial or full redesign of your organization's security architecture and how it will help deliver on the bottom line. The key to addressing future needs is to have a robust and flexible security architecture that will require relatively minor adjustments to meet evolving needs.

Seeking Buy-In Across the Business

Once you understand the changes needed to your security architecture, you'll need to get buy-in from your organization's leadership. Your approach should consider the priorities of different audiences, appealing to security and IT staff, as well as the C-suite, with each group having a different focus and set of priorities. At lower levels of an organization, the lack of buy-in to security policies and practices can negatively affect the use and implementation of security controls, while at higher levels, funding and resource allocations can suffer.

A good place to start when looking for buy-in is reporting. Robust reporting on the activity in your security environment can help make the case for the additional budget and time necessary to improve a security operation. If you can effectively demonstrate a huge number of alerts that need triaging, or events of interest that require significant investigation, this will strengthen your case. However, it's important to ensure that any reporting is tied to overall risk and business goals; if they're not, they become noise and irrelevant.

For security staff, the focus will be on the day-to-day tools they will be using, and how they impact their work. This group will be most interested in solutions that feature ease of use and provide simple ways to report events and incidents. Emerging technologies like AI and machine learning are helping to streamline alert triage, and threat detection and response processes and can lower the risks of human error. AI-based solutions like Secureworks' Red Cloak™ Threat Detection and Response can help identify issues at a much faster speed and with greater efficiency. While human intelligence is an important component of any security system, an organization's own data is an asset that should be leveraged with data analytics tools to build a truly cost-effective, scalable system. When building your security stack, you'll want to seek out vendors with solutions that can support those types of capabilities.

AI-based solutions like Secureworks' Red Cloak Threat Detection and Response can help identify issues at a much faster speed and with greater efficiency.

In contrast, members of the C-suite will be much more interested in understanding the organization's overall risk factor, the ROI of any security investment, and how any new technologies will integrate with the rest of the business or make processes more efficient. In helping to sell them on solutions, it may be helpful to remind them of the stakes – for example, becoming the poster child for the victim of a huge breach. Painting this picture may help secure the funding you need to mitigate risk or reduce it in a manageable way. Further, illustrating how the use of a vendor can reduce the time, complexity, and costs associated with deployment and management of in-house solutions can be beneficial to business leadership. Secureworks can help organizations reduce the total cost of ownership by consolidating all managed security services into a single provider with trained security expertise. Each organization will have its own amount of risk it's comfortable with, and as you seek buy-in, you should be prepared to outline how the use of a security vendor will address these potential risks.

Managing Expectations for Implementation

When leaders have signed off on your proposal, you'll need to set a clear timeline and KPIs to demonstrate your program is delivering upon the initial plan. For this exercise, it will be helpful to refer to the framework created in your maturity modeling to guide your reporting efforts. The framework is also a helpful foundation for any future changes as new risks arise.

Create a realistic timeline to set your security redesign in motion - it's not uncommon for these programs to take around 12-18 months to implement. Turnkey solutions are rare in cybersecurity, so six months or less might not be realistic. A new vendor and the tools they introduce will need time to adapt to your organization and the people who interact with them since your culture will always impact the reporting process.

Defining clear KPIs will help measure the success of your program and ensure organizational goals are being met. While this piece is easy to overlook, demonstrating financial justification will help strengthen the case to senior leadership for larger budgets and bigger infrastructure investments.

For organizations that are also pursuing digital transformation by expanding into new cloud and IoT technologies, a refreshed security architecture can complement these efforts by ensuring the security is baked into new technologies, rather than appearing as an afterthought.

Steps Toward Future Success

Committing to a security redesign is no small task and requires undergoing a full assessment and securing buy-in from different stakeholder groups in order to make it successful. While a large undertaking, through this process your organization can develop a robust and flexible security architecture built to withstand both short and long-term risks.

With our breadth of services, 20 years' experience, and security analytics software built for the future, Secureworks can help you better understand how to fix the issues with your security operation and plan where to develop next. We'll support you in securing the buy-in and investment you need from all levels of the organization to create the conditions necessary for future success.

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