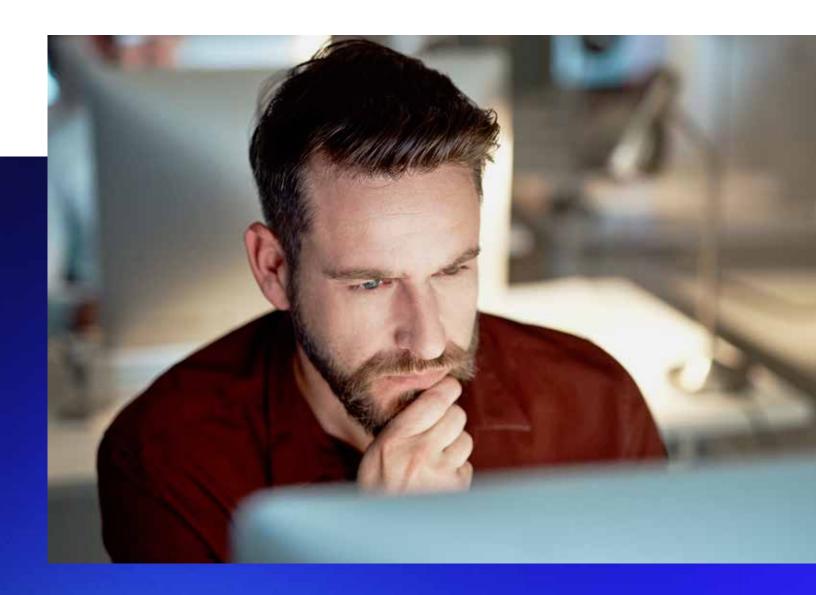# Secureworks®

5 Ways Secureworks Streamlines Your Security Operation

Secureworks®

We're living in an era of unparalleled risk for organizations. An explosion in threats over the last ten years has put companies on the back foot, struggling to keep up. As non-technical actors have benefited from commodity malware they can use without much prior knowledge, the industry has released tools that target these threats as they arise. This approach is no longer working and has created problems of its own.

This piecemeal approach to addressing threats created security environments composed of layer upon layer of tools and controls. Companies use 47 different cybersecurity solutions on average , sometimes significantly more. The situation is no better for smaller organizations, who often face a disproportional level of complexity compared with the size of their company. Security teams are commonly running multiple tools performing similar functions in parallel or have legacy and old tools in their stack they've forgotten about.

This complexity creates opportunities for threat actors. Wherever there is a forgotten asset, barrage of alerts, or unpatched system, there's a chance to enter unnoticed. Security teams have limited resources and time. The list of tasks needed for full coverage of an organization's environment is simply too long for most companies to handle in-house, and the security vendor landscape is confusing at best. How can you find the right partner who can help you streamline your operations?

Find a Partner Who Understands You

Finding a security partner you trust can bring order to the chaos of a security operation. It can simplify and consolidate your program to put you ahead of threats. Secureworks helps protect thousands of customers around the globe, and we have done so for over 20 years. With the expertise and depth of experience across all facets of security, we can help you simplify and streamline your security stack while also helping to build a holistic picture of your operation.

1. We're Solely Focused on Cybersecurity

Since 1999, Secureworks has only focused on security. Nothing distracts us from your mission to secure your organization in the most efficient and effective way possible. We don't try to sell non-security products to your company. Our recommendations originate from a holistic viewpoint, drawn from an in-depth study of your environment.

Our threat research and incident response teams have a deep understanding of how threat actors behave informs everything we do. We have a long history in running services to simplify security operations, including the critical aspect of correlation, and we're committed to significantly simplifying security operations using our proprietary security analytics software.

Companies use 47 different cybersecurity solutions on average, sometimes significantly more.

Secureworks®

2. Our Software Prepares You for the Future

Have you ever felt frustrated with the disjointed and layered approach to security that most organizations take? Our in-house team also lives and breathes those frustrations, so we built a solution. We combined advanced data science, premier threat intelligence, and incident response expertise to build our security analytics software, Red Cloak™ Threat Detection & Response. Red Cloak TDR automatically correlates your telemetry against threat intelligence to find potential threats with a high degree of accuracy. Our team has trained machine learning algorithms to automatically detect a wide range of attack methods and tactics, including the behavioral hallmarks of a threat. It's able to separate events that matter from those that don't so that your team is not wasting time on triage or investigation of benign alerts.

Red Cloak TDR breaks down operational divisions by bringing together data from cloud, network, and endpoints to build a full picture of the activity in your environment. Events are presented to analysts with context so they can make a quick decision about next steps. The software offers automated incident response actions to analysts who have the final say over the response. Red Cloak TDR also includes a chat box where your team can contact Secureworks with any questions. This way, analysts can learn with each new incident.

For organizations that have limited resources, Managed Detection and Response powered by Red Cloak TDR offers all the benefits of our software but operated by analysts in our SOC. Your security analysts can use the technology and chat with our experts to develop in the position, but our team is in control of operating the software to keep you protected.

3. We're Experts in Security AI

A word of caution: AI offers enormous potential to streamline security operations, but it must be applied carefully. AI and data science technologies, like machine learning and deep learning, provide an effective way to process and analyze huge amounts of data to identify threats and reduce the burden of alerts. However, there are use cases where an inexact application of AI can result in a disappointing number of alerts. Examples of this abound the crowded vendor landscape. Buyers should analyze vendor claims about AI carefully – if they can't engage a realistic discussion about the technology's limitations, they might be dealing in the hype. AI technology is not yet advanced enough to apply to all security functions without human input. This is why our team of data scientists and security experts supervise our machine learning algorithms to ensure accuracy. We believe AI should only be used when it brings maximum benefit to security teams.

A combination of machine intelligence and human expertise enables our AI to significantly reduce the time it takes to detect threats. Our experts have also trained it to detect advanced "living off the land" techniques that most existing security controls would miss. This futureproofs your operation as threat behaviors evolve much slower than malware does.

Red Cloak TDR breaks down operational divisions by bringing together data from cloud, network, and endpoints to build a full picture of the activity in your environment.

Secureworks®

4. The Network Effect Increases Your Visibility

When a new threat appears in one of our customer environments, we assess it, research it, then operationalize that knowledge across all our customer environments. That keeps all our customers safe and prepared against the threat. We call it "The Network Effect". We combine what we see and learn in one customer environment, for the benefit of all. This is made more powerful when you consider we have thousands of customers of all sizes and in all industries around the world.

The Network Effect means if we see the same threat in your environment, next actions are readily available from our previous experiences. It saves time and streamlines your operation by reducing the need for analysis and triage. Our security analytics software makes the process even faster than before. It's another example of how security analytics software prepares you for the future of security.

5. We Go Deep Into Your World

A common problem with running multiple tools or having a complex stack is that they don't communicate with or learn from one another. Secureworks' Advisory Services team works to understand your environment and uses that knowledge to facilitate a programmatic and holistic conversation and caution against purely tactical solutions. We study your organization's risk profile and appetite to find the best solution to the challenges you face.

Our Incident Response team frequently discovers more about a customer environment in one engagement than the in-house security team already knows, and they always share their findings so customers can mature their posture. Our IR and adversarial testing (Secureworks Adversary Group) teams are constantly learning new information about how threats could exploit security and environments, and we use that knowledge to help keep the rest of our customers safe. Our adversarial testing consultants have even discovered new vulnerabilities to share with the security community as part of their work.

Our Counter Threat Unit™ research team is comprised of talented individuals who could work at any organization they choose. They stay with Secureworks because we believe world-class threat research is critical to keeping our customers ahead of the threat, wherever they are in the world.

Secureworks has broad experience in multiple aspects of security over the last 20 years, which enables us to make recommendations founded in evidence and certainty. We take a holistic approach to confidently manage the tasks organizations might not feel confident about doing themselves. We've seen what works in thousands of

The Network Effect means if we see the same threat in your environment, next actions are readily available from our previous experiences. It saves time and streamlines your operation by reducing the need for analysis and triage.

Secureworks®

environments in different industries globally and use that knowledge to optimize our customers' security operation.

Your Trusted Security Partner

The security market is inundated with vendors trying to get the attention of security leaders. Sometimes it's hard to cut through the hype and identify companies that go beyond a typical customer-vendor relationship.

Secureworks views security as a partnership. We find the right solution for your unique needs based on 20 years' experience helping customers with a full range of security needs. Not much in security is new to us, but when an event is genuinely novel, our team of researchers and IR consultants are at the forefront of studying it to help keep customers safe. Our knowledge and expertise help you cut through the complexity of your environment and stay ahead of threats into the future.

Secureworks®

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