WHITEPAPER

PERSONAL | PREDICTABLE | PROTECTION

The Path to Security Effectiveness

/// The cybersecurity industry has an effectiveness problem. Every year, new technologies, vendors, and products emerge. Yet despite this constant innovation, high-profile breaches keep making headlines. Clearly, the status quo is not working. Organizations seeking the path to truly effective security need to take a new approach.

Part 1: The Cybersecurity Industry Doesn't Have a Tools Problem

The 2020 edition of Momentum Cyber's CYBERscape outlines 18 distinct cybersecurity categories within the industry. Within each of those there are multiple sub-categories, with thousands of vendors in total.

For organizations of all sizes, the sheer volume of choices can make managing tools and developing a security strategy a difficult task. This fact is underscored by a recent survey conducted by Enterprise Strategy Group, which showed that 55% of enterprises currently use 25 or more cybersecurity technology products within their organization.

With organizations having no shortage of options when it comes to security products and vendors, this creates issues on its own. Gartner, the industry's leading analyst firm on enterprise security, recently stated that "many security teams have overinvested in a plethora of tools. As a result, they are also suffering from alert fatigue and multiple console complexity and facing the challenges in recruiting and retaining security operations analysts with the right set of skills and expertise to effectively use all those tools."

Another challenge with the number of tools on the market is that many security tools are tightly clustered in terms of efficacy. Using endpoint protection tools as an example, numerous independent researchers show that most top solutions stop the vast majority of common malware seen in the wild. For an IT or security decision maker, this means they can select almost any leading solution in the market and be protected from the vast majority of malware threats.

> “
>
> Many security teams have overinvested in a plethora of tools. As a result, they are also suffering from alert fatigue and multiple console complexity and facing the challenges in recruiting and retaining security operations analysts with the right set of skills and expertise to effectively use all those tools.
>
> **— Gartner,**
> https://www.gartner.com/document/3834578

Company	Malware Protection Rate
Avast. SparkCognition, Trend Micro	100%
Microsoft, Panda, Seqrite	99.9%
Bitdefender, Endgame, K7, McAfee, Sophos	99.8%
Symantec, VIPRE	99.7%
Cisco	99.5%
Fortinet, Kaspersky	99.4%
ESET	99.3%

The table above comes from AV Comparatives' Business Security Test for the second half of 2019. The chart shows that 17 endpoint protection solutions scored over a 99% protection rate against real-world threats.

So, if real-world testing shows the majority of endpoint solutions are stopping threats, why do breaches still occur? Before IT and security leaders spend another penny on cybersecurity, they need to strongly consider if swapping vendors or adding a new tool is actually going to move the needle in terms of overall security effectiveness.

Silver Bullets Ultimately Fail to Deliver

Over time, the cybersecurity industry almost always met new challenges with new tools. Vendors pivoted from focusing signatures to heuristics to reputation to whitelisting to IOC sharing to sandboxing to machine learning to behavioral analytics, and now, to threat hunting. These moves responded to an ever-evolving adversary and only recently has the industry started to realize that the latest "silver bullet" will not stop all threats.

One reason it's so hard for organizations to be effective at cybersecurity is because the attackers themselves are smart, capable humans. With advanced persistent threats, once the attacker gains a foothold in the environment they leverage "living off the land" strategies and tactics to masquerade as a legitimate user. Human analysts and human intuition are often the most effective way to detect and remove these types of threats. As a result, a winning security strategy for organizations must include a significant emphasis on the human element. However, businesses must find the right way to add this human element to their security strategies, which becomes a major challenge in itself.

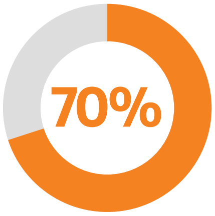
According to research from the 2019 SANS SOC Survey , only 1 in 1,000 companies have a security operations center (SOC). Even in large enterprises this figure is only about 50 percent. To counter skilled and persistent human adversaries, organizations need to ensure their strategy includes skilled and persistent human defenders. But because building a SOC and staffing it with talent is the harder path, they rarely do so.

Part 2: The Cybersecurity Industry Has an Effectiveness Problem

Year after year, cyberattacks grow more sophisticated, more damaging, and more prevalent. And as advanced tools find their way into the hands of cybercriminals, organizations of every size risk falling victim to data breaches despite having an army of tools at their disposal. Research from Risk Based Security's Mid-Year QuickView Data Breach Report shows that data breaches in the first half of 2019 saw a 54% increase over those observed in 2018.

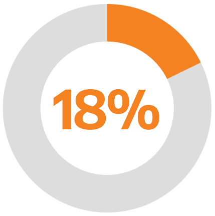
The ineffectiveness of tools is further highlighted when looking at data from recently onboarded Arctic Wolf® customers. As part of this onboarding process, the Concierge Security® Team (CST) works with customers to configure their environments so that, using the Arctic Wolf® Platform, the CST can detect and respond to threats on their behalf. As new customers, they serve as an ideal environment to examine what types of threats can go undiscovered by a company's existing processes.

Here's what Arctic Wolf has discovered:



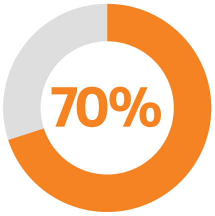
Advanced Threats

Advanced threats such as malware are found in 70% of all new Arctic Wolf customers. These threats have already bypassed existing security tools and processes deployed by the customer and have been embedded within an organization's environment for an undetermined amount of time.



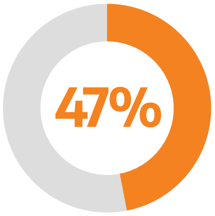
Phishing

Most companies have some sort of email protection platform in place, but phishing activity is discovered to have bypassed those tools in 18% of organizations.



Account Takeover

70% of new Arctic Wolf customers are found to have some form of personally identifiable information tied to their corporate credentials available on the dark web, and 5.5% of all new customers have an exposed plaintext password published online.



Cloud Monitoring

Protecting data in the cloud by identifying misconfigurations and other vulnerabilities is a growing challenge for many businesses. Nearly half (47%) of all security incidents detected across new Arctic Wolf customers include a cloud component. While businesses continue their rapid adoption of cloud applications and services, they still struggle with cloud security—and attackers are exploiting that gap.

The Perfect Storm: Complexity, Alert Fatigue, and Staffing Shortages

With the majority of companies deploying more than 25 security tools, how can such a large number of security incidents keep occurring? In 1999, Bruce Schneier, a well-known cryptographer and Fellow at the Berkman Center for Internet & Society at Harvard Law School, published a short essay called "A Plea for Simplicity. " In it, he predicts that "networks of the future will be necessarily more complex, and therefore less secure," and that even systems at that time "are far too complex to analyze, and that there are security flaws everywhere."

Over 20 years later, Schneier's predictions appear on the mark, with Cisco's 2019 CISO Benchmark Report documenting the extreme alert fatigue organizations now experience. Cisco's research shows that two-thirds of all organizations face more than 10,000 alerts per day. In that sea of 10,000 alerts, only half of those are investigated, and of those investigated, only a quarter are legitimate. Of those that are legitimate, only 43% of them get fixed.

> "Networks of the future will be necessarily more complex, and therefore less secure."
>
> — **Bruce Schneier,** Fellow at the Berkman Center for Internet & Society at Harvard Law School

Another demonstration of this complexity concerns the industry's reliance on endpoint solutions and agents to secure systems. For example, recent research from Absolute shows that a typical organization has ten endpoint security agents deployed on their devices.

The net effect of purchasing and deploying a plethora of security tools has left organizations awash in a sea of alerts with a portfolio of security tools that are misconfigured, out of date, or unable to be managed by in-house teams. This complexity of these implementations is, in effect, killing the effectiveness of these solutions while failing to make these organizations any more secure.

Unfortunately, there's no such thing as "set it and forget it" in cybersecurity. Sophisticated cybersecurity tools are effective only as long as they are operated effectively. A vendor may help configure a new tool to work on day one, but there is a myriad of factors that can impact it its effectiveness on day 100.

When a tool is installed it needs precise configuration to ensure an organization's entire environment is captured correctly. But modern businesses move quickly: servers (especially cloud-based servers) are commissioned and decommissioned on a daily basis, new employees start work each week, and a myriad of new IT and security tools are constantly rolled out. All of these factors can quickly cause a security tool's configuration to instantly become out of date.

For a tool to continue to operate effectively, a single individual on the IT or security team is typically relied upon to become an expert on the use of that tool. These individuals must be trained on how to operate the new tool, as well as how to maintain and update its settings as new features are added and configurations within the organizations change. This training costs time and money, and the more tools an individual has to manage, the higher the likelihood that something is missed.

Then comes the challenge of having the team member responsible for a tool leave the company. When this happens the institutional knowledge that person has about how the tools operate, particularly within an organization itself, can disappear overnight. This causes issues in the handoff of tool ownership, which often results in missed alerts, tools soon forgotten entirely, and—in a worst-case scenario—the occurrence of a data breach.

2/3

of all organizations
face more than

↓

10,000

alerts per day.
Of those alerts,

↓

HALF

are investigated.

↓

1/4

of those
are legit, and

↓

43%

of those that
are legit get fixed.

Part 3: The Cost of a Breach

In its 2019 Cost of a Data Breach Study, Ponemon cites $3.9 million as the average cost of a data breach, with the average cost of a single breached record at $150M. For organizations that store and manage sensitive data records numbering in the tens of thousands or more, that's a lot to lose. These records could include vendor, personal, or financial information, and map to a variety of industries such as healthcare, financial services, insurance, retail, legal, public administration, and more.

Some of the associated costs are immediately evident, such as the detection and escalation costs in terms of salaries and fees of the security teams required to perform investigations and forensics where tools may have failed. There are also the costs for public notification via public relations and press announcements, post-data breach response costs related to hiring an incident response team, and any necessary or required communications through phone calls and emails to those who need to know or might be affected. Depending on the circumstances, legal fees, regulatory fines, and compliance penalties may factor into the equation too.

These costs often add up to breathtaking figures—even before factoring in an organization's high potential for loss of future revenue as the result of customers no longer trusting it to secure their data. In fact, for a few unlucky and unprepared companies who invested millions of dollars each year in security tools, it was a lack of security effectiveness within their organization that ultimately led to losses topping $100 million.

Recent High-Profile Breaches

Equifax

In September 2017, Equifax, one of the three big consumer credit reporting agencies, announced it suffered a breach at the hands of hackers. The fallout compromised sensitive information belonging to as many as 143 million Americans, including names, birthdays, addresses, credit card numbers, Social Security numbers, and driver's license numbers.

Hackers infiltrated Equifax by exploiting a software vulnerability in Apache Struts, a framework for creating web applications written in Java. The vulnerability they exploited was previously disclosed and was detected by a vulnerability management tool, but patches were not deployed fast enough to stop the breach.

Capital One

In July 2019, Capital One, one of North America's largest credit card issuers, announced it had experienced a data breach that included the leaking of names, addresses, zip codes/postal codes, phone numbers, email addresses, dates of birth, and self-reported income from more than 100 million credit card applications.

The alleged perpetrator was a software engineer in Seattle, who managed to breach AWS S3 storage buckets through a multi-step, targeted attack. The root cause of the breach was a misconfigured firewall in the Capital One AWS infrastructure that the hacker used to gain access because Capital One was unable to identify and mitigate the risk in time.

Target

In December 2013, U.S. retailer Target reported that hackers stole data on as many as 70 million shoppers (including data from 40 million credit cards) who visited their stores during the 2013 holiday season.

According to Bloomberg , Target had a malware detection tool in place that detected the breach and sent an alarm, but the warning went unheeded by Target's security operations center.

The common thread among these breaches? They were not caused by tool failures; they were the result of operational problems. If organizations want to protect themselves from these kinds of breaches, they must move beyond their reliance on tools and, instead, take an operational approach to security.

Part 4: The Emergence of Security Operations

To finally solve the effectiveness problem in cybersecurity, organizations need to find a solution that combines technology with human expertise and delivers it in a way that addresses day-to-day security needs while also ensuring that their overall security posture becomes stronger over time.

This realization has led to the emergence of "security operations" as its own discipline in cybersecurity. By considering security operations as a discipline unto itself, organizations think beyond tools to a state of operations in which they have broad visibility into and across their technology, whatever it encompasses and wherever it resides. This insight enables their security teams, processes, and workflows to become highly effective, while also ensuring that targeted security outcomes are informed by experts and designed with the future in mind.

Security operations marks a significant departure from two more traditional security pathways typically used by most organizations.

DIY

The do-it-yourself model has proven ineffective for most organizations. Hiring in-house security experts and building a team for 24x7 coverage is cost-prohibitive for all but the largest organizations. The average salary of a security analyst is approximately $100,000, and according to Gartner, depending on the functions and capabilities provided, a fully functional SOC running 24x7 requires at least eight to 12 full-time employees regardless of company size . In total, the Ponemon Institute estimates that a typical organization spends $2.86 million annually on its in-house SOC.

By the numbers:

8 to 12

full-time employees needed for a fully functional SOC running 24x7, regardless of company size

$2.86M

annual amount that a typical organization spends on its in-house SOC

MSSPs

Frustrated by the challenges of finding and retaining in-house talent, many organizations turn to managed security services providers (MSSPs) to help monitor, maintain, and manage their security around the clock, 24x7. MSSPs are sometimes a popular option, particularly with small and medium-sized enterprises for a simple reason: They provide an affordable, subscription-based security model.

An MSSP can relieve the pressures of alert fatigue from tools and the struggle to find qualified security analysts, but it's critical to realize that hiring an MSSP is not a way to achieve security effectiveness. Some of their shortcomings include:

Limited Scope:

While an MSSP can take alert monitoring off the hands of an organization, it doesn't necessarily include analysis, triage, and response. In many cases, that's still up to the business to manage, so adequate in-house expertise is still needed.

Lack of Personalized Support: Support is often relegated to contact centers where representatives have limited contextual insight into the client's business or industry and don't necessarily understand how the client's internal systems work. As a result, problems may take significantly longer to resolve than one might expect. This lack of knowledge and insight may also impede an MSSP's ability to make strategic recommendations.

Poor Visibility: MSSPs won't help an organization holistically improve its security posture, and they very rarely aid in compliance management (e.g., HIPAA, PCI DSS). If a business doesn't already understand the strengths and weaknesses of its security posture and relies completely on the MSSP, it continues to leave gaps in its defenses.

Little Help Post-Intrusion: MSSPs are predominantly preventative. They will not actively threat hunt for indicators of compromise (IOCs) on the network, and they won't optimize incident response in the event of an undetected breach.

Part 5: The Next Frontier: Cloud Security

Cloud applications and tools are mostly affordable, and easy to deploy and use. They offer flexibility for growing companies to meet increasing demand seamlessly. The cloud knows no downtime or location restrictions, so employees can conduct business 24x7 from wherever they are. According to Flexera's 2020 State of the Cloud Report, 94% of organizations use either a public or private cloud environment, and Verizon's 2020 Data Breach Investigations Report states that 24% of all breaches now involve cloud assets.

With use of the cloud nearly ubiquitous among businesses, and the cloud now responsible for a growing number of breaches, the talent to secure those environments is becoming increasingly difficult to find. Recent research from Enterprise Strategy Group (ESG) shows that cloud security expertise is the single most acute skills shortage facing the cybersecurity industry today.

A cloud services provider does have some responsibility to secure the cloud, but it is only responsible for ensuring its own infrastructure and applications are secure. That doesn't mean cloud resources are automatically protected against cyberthreats. Insider threats, hijacked accounts, distributed denial-of-service (DDoS) attacks, and advanced malware still pose viable risks to cloud-based assets and can disrupt business operations and harm essential data.

Leading cloud providers such as Amazon Web Services (AWS) , Microsoft Azure, and Google Cloud Platform™ have all developed resources such as APIs and robust logging to help businesses monitor data traffic and cloud network activity. However, the onus is still on the organization to provide both the instrumentation and the expertise needed to spot threats.

Cloud Security

94%

of organizations use either a public or private cloud environment

24%

of all breaches now involve cloud assets

Part 6: The Five Pillars of Effective Security Operations

For organizations that seek to embrace the concept of security operations and develop a more strategic approach to security, they can incorporate the following five pillars of security effectiveness into their operations. This will ensure better workflows, enhanced protection against potential breaches, and more secure cloud environments.

01

Broad Visibility

Organizations can't protect what they can't see. Too many businesses have blind spots that result in critical security events being missed. Organizations should make certain they have total visibility into their environment. Their security capability should be vendor-agnostic and span endpoint, network, and cloud. Better yet, all that telemetry should be streamed to a single, central cloud platform where it can be stored for compliance and analyzed by the human insight of cybersecurity experts along with machine learning/artificial intelligence tools to drive both reactive and proactive security outcomes.

02

24x7 Coverage

Perhaps the biggest inhibitor to taking the operational approach to security is the skills shortage. There simply aren't enough cybersecurity professionals to go around. Companies should ensure they find a way (typically through partnership) to have 24x7 monitoring, threat detection, rapid response, and proactive risk management to keep their organization safe at all times.

03

Access to Expertise

It isn't enough to have eyes on glass. Organizations must be able to consult with certified cybersecurity experts on a variety of topics—both in terms of scheduled meetings as well as on demand. Companies should get quick answers to questions about any aspect of their security program, and the representative who responds to the call should know the environment well enough to provide sound solutions. This could be in-house expertise, but it could also be a named external resource that is an extension of the organization's IT team. This expertise should accelerate every security task, thus improving metrics like mean time to detect and mean time to respond.

04

Strategic Guidance

Security is a journey, not a destination. If organizations never step back from tactical actions, like detection and response, they never see the big picture. Organizations should learn lessons from their incidents and alerts, considering what that means for their overall security program. They should continually review their architecture and configurations in an effort to minimize their attack surface and they should deploy proactive countermeasures to further harden the environment against future attacks.

05

Continuous Improvement

An organization's security program should get stronger and more resilient over time, with a focus on achieving operational effectiveness. That requires a critical eye in reviewing the processes, people, intelligence, and technology that define its security operations effectiveness. This can only happen if companies put a security strategy in place and diligently benchmark their progress against it.

The Best Way to Achieve Effective Security Operations

For organizations to improve the effectiveness of their security operations, they must be aware of their strengths and weaknesses to take the right path along their security journey. While some organizations may have the internal capacity to achieve these five pillars of security effectiveness on their own, the reality is many organizations will have to partner with experts to improve their security operations.

Arctic Wolf has focused on the operational approach to cybersecurity since our founding. We realized early on that security isn't solely a tools problem or a staffing problem; it is an operational problem. We built the Arctic Wolf Platform and created the industry's first Concierge Security Team to deliver critical operational capabilities like Arctic Wolf® Managed Detection and Response (MDR), Managed Risk, and Managed Cloud Monitoring to our customers.

We are unique in the industry because the Concierge Security Team not only works around the clock to protect customers from threats, it also plays a strategic role. Our Concierge Security engineers are named resources who develop a unique understanding of an organization's environment over time. They use this knowledge to continually assess their overall security posture and work proactively to ensure that your business always improves and constantly adapts to the threat landscape.

Many organizations have limited financial resources to build an internal security operations center and hire the highly-sought cybersecurity experts they need. the Arctic Wolf approach to security operations provides a uniquely effective way for organizations to protect their endpoints, networks, and cloud services from today's growing threats.

About Arctic Wolf

Arctic Wolf® is the market leader in security operations. Using the cloud-native Arctic Wolf™ Platform, we provide security operations as a concierge service. Highly trained Concierge Security® experts work as an extension of your team to provide 24x7 monitoring, detection, and response, as well as ongoing risk management to proactively protect systems and data while continually strengthening your security posture. For more information about Arctic Wolf, visit arcticwolf.com

[1] https://momentumcyber.com/docs/CYBERscape.pdf

[2] https://www.csoonline.com/article/3337459/the-problems-plaguing-security-point-tools.html

[3] https://www.gartner.com/document/3834578

[4] https://www.av-comparatives.org/tests/business-security-test-2019-august-november/

[5] https://www.sans.org/reading-room/whitepapers/analyst/membership/39060

[6] https://pages.riskbasedsecurity.com/2019-midyear-data-breach-quickview-report

[7] https://www.schneier.com/essays/archives/1999/11/a_plea_for_simplicit.html

[8] https://engage2demand.cisco.com/LP=14948

[9] https://www.absolute.com/media/1935/2019-endpoint-security-trends-report.pdf

[10] https://www.ibm.com/security/data-breach

[11] https://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data

[12] https://www.gartner.com/document/3981264?ref=solrAll&refval=248392296

[13] https://www.ponemon.org/blog/the-economics-of-security-operations-centers-what-is-the-true-cost-for-effective-results

[14] https://info.flexera.com/SLO-CM-REPORT-State-of-the-Cloud-2020

[15] https://enterprise.verizon.com/resources/reports/dbir/

[16] https://www.esg-global.com/hubfs/pdf/ISSA-ESG-Press-Release-2018.pdf

[17] Amazon Web Services, the "Powered by AWS" logo, [and name any other AWS Marks used in such materials] are trademarks of Amazon.com, Inc. or its affiliates in the United States and/or other countries.

ARCTIC WOLF

SOC2 Type II Certified

AICPA SOC

ISO 27001 CERTIFIED CYBERGUARD COMPLIANCE

Contact Us
arcticwolf.com
1.888.272.8429
ask@arcticwolf.com