



WHITE PAPER

A Skeptic's Guide to Buying Security Tools

A skeptical approach to thoroughly evaluate the necessity, cost, and value of today's security control purchases.

Contents

Introduction: Do we really need another tool?	3
Question 1: Which gap takes priority?	4
Question 2: Have we found the ideal solution?	6
Question 3: Can we build a business case?	8
Question 4: What happens next?	9
Question 5: How can we be sure?	10
Conclusion	12

INTRODUCTION

Do we really need another tool?

Some of the worst security breaches happen because someone made a risky assumption:

- “No news is good news”
- Our current security stack is sufficient
- Pen tests and red teams will find all significant gaps
- A shiny new tool will fix everything

When a significant breach makes headlines, panic ensues as vendors flood our inboxes with claims that their product can avert a repeat disaster. But where's the proof?

Before you invest in another shiny new tool, take a skeptical buyer's approach to building a business case for it. Ensure you can demonstrate the need, cost, and ultimate value beforehand.

Security spending is up, but the value may not be

Budgets continue to rise, but tool sprawl and skills shortages grow faster. Installing, learning, and operating each new tool takes time and money.

Underutilized tools create waste and complexity that delay response and leave CISOs reluctant to approve future purchases. Over time, the more shelfware piles up, the more closely new purchases get scrutinized.

The skeptic's approach

Modern best practices call for continuously validating your security posture—and gaps. Life-cycle testing of current and future controls keeps your defenses in lock-step with the evolving threat landscape. This guide will take you through five key considerations from a cynic's point of view:

- Why are you considering this purchase? Can you pinpoint gaps in your current stack?
- If you have a problem a new tool claims to solve, is the tool the best way to solve it? Can you convince whoever owns the budget?
- Should you invest the time and resources? Will it help teams collaborate and be more proactive?
- Can you demonstrate that investment makes your company safer and more compliant?

And last but not least: **What makes you so sure?**

QUESTION 1

Which gap takes priority?

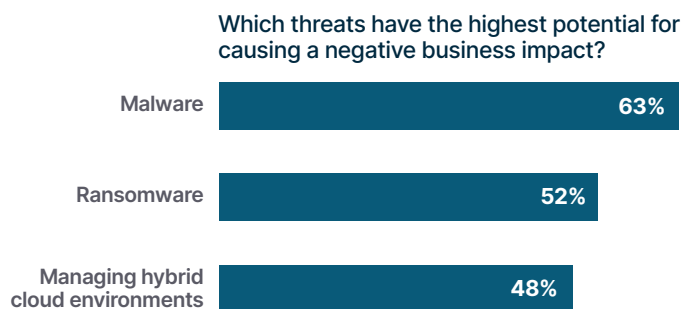
You can always find reasons to invest in more security tools. Increasing compliance requirements, rising costs, and the looming threat of ransomware continue to plague businesses around the globe. But even before signing up for another product demo, the skeptical buyer takes stock of the company's cyber risk posture and operations. Deep internal introspection should drive the decision that you need something new.

Which threats pose the most risk?

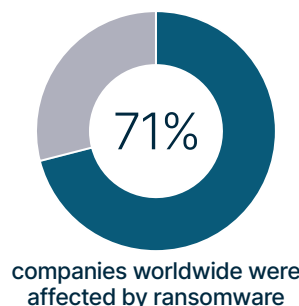
CISOs typically know which attacks will have the most significant business their companies most through:

- Downtime
- Data loss
- Mitigation and recovery efforts, including non-compliance fines
- Irreparable loss of brand reputation

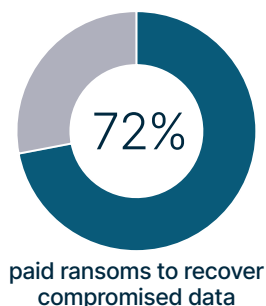
Once you confirm your organization's high-priority threats, you can move on to assess your ability to block them.



Source: S&P Global Market Intelligence, The Impact of Continuous Security Validation, 2023



Source: Statista



Source: Statista

Do we have gaps in visibility? Monitoring coverage? Skills?

Put your defenses to the test. Simulate real-world attacks to pinpoint where and how they might succeed by taking advantage of weaknesses in your defense. Assume attackers can find a way in and assess what actions they can take undetected. Can they drop command and control (C2) tools? Escalate their privileges once inside?

Realistic assessments illuminate blind spots and insufficient controls. Are detection tools adequately tuned? Did the team take the appropriate actions?

After uncovering gaps in visibility or controls, security leaders have three options:



Wait: tune existing controls and hope for the best



Find a temporary solution (and hope for the best)



Invest in longer-term solutions

What to do first?

When multiple issues can't wait, use hard data to prioritize investments. Model the likelihood and probable impact of each type of weakness getting exploited. For example, if you see your customer's personal data for sale on the Dark Web, stopping phishing campaigns and data loss prevention might take top priority.

The skeptical buyer's next question should be...

"Do we have something that does this already?"

Organizations often buy security solutions to fix specific problems but don't always leverage tools to their full potential. Take inventory, then think creatively.

Model and measure the impact of turning on more features on your firewalls or IDS. Tweak configurations to uncover untapped potential of commercial suites like Microsoft Defender.

You may very well own something—or several things—that together could fill high-profile gaps. If you can prove that you don't, move on to compare and choose the best option for your needs and operations.

The Skeptical Buyer's Checklist

Can we prove we have a gap?

Which threats pose the greatest risk?

Do we already own tools that can solve the problem?

QUESTION 2

Have we found our ideal solution?

Throwing more tools at a problem may or may not provide a solution, so you must ask:

How will we know when we've solved the problem?

Define *verifiable* success criteria up front, then assess the value of competing solutions in the context of your own environment.

Do we have the right approach?

Take a step back. Think through your strategy from a *directional* perspective.

Stopping phishing and business email compromise (BEC) may be board-level priorities, but how should you go about it? Does it make sense to invest in education, multi-factor authentication (MFA), endpoint detection and response (EDR). And if all of the above, at what levels?

To settle on the right high-level strategy, measure how well each approach prevents or mitigates phishing campaigns levied *against your unique environment*. Once you choose the best approach, you can start evaluating prospective solutions, either one by one or head-to-head vendor bakeoffs.

Which product offers the ideal solution?

Security vendors may be consolidating, but you'll find multiple options in virtually any category. Features on data sheets all sound very similar, and are backed by bold claims and "stretch goals" achievable only under ideal conditions.

Look beyond the collateral; no vendor claim is relevant if it doesn't deliver in your unique environment. Make vendors *prove* their products live up to their hype by measuring the impact on your high-priority security gaps.

CONSIDER THE SOURCE

At times it feels safer to go with established vendors, but many times the well-funded startup with a more innovative approach makes better sense. A vendor-agnostic validation platform can give you the data you need to make a better informed decision.

Is best-of-breed best for our need?

Even enterprises with deep pockets can't afford to endlessly burn budgets on technologies that are not deployed, or not fully utilized, or that create more problems than they solve. Opt for lesser-known or "best in *suite*" solutions from your current providers if it means you can:

- Avoid bringing in technologies that don't integrate with your stack
- Reduce complexity and administrative burden
- Adequately solve problems faster than you can with best-in-class solutions
- Cover multiple bases with a single investment

The Skeptical Buyer's Checklist

.....
How will we know we've solved the problem?
.....

.....
Are we taking the right approach?
.....

.....
Is the product our ideal solution?
.....

.....
Do we need best-of-breed?
.....

QUESTION 3

Is our business case solid?

Assume whoever you ask for the budget will be skeptical of making new purchases. Think like them; in fact, “out skeptic” them. Weigh the risk of not addressing known visibility gaps against the cost and impact of adding more tools or switching vendors. You don’t always need to strive for perfection, but you can’t sacrifice security just to save a few dollars, either.

A business case backed by empirical data helps strike the right balance—and convince whoever needs convincing.

Is this the best use of the budget?

Every company faces constraints in terms of budget, data privacy regulations, and risk from macroeconomic challenges. Similarly, every solution differs in price, overhead, and complexity.

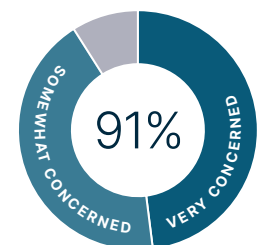
To reconcile the two, evaluate products under realistic conditions. Test performance, then do the math.

Does a lower-cost option save money if it only addresses a single issue or adds management complexity? Would it make more sense to fast-track a more substantial investment that furthers multiple objectives simultaneously?

Is the product worth the time and effort?

Every new tool comes with its own learning curve, but it’s worth the effort if it helps your understaffed, over-stressed team reduce menial tasks and complexity. As part of due diligence, consider the skills and operational hurdles of implementing new technology. If the proposed purchase means hiring or certifying specialized analysts, will it ultimately mean you can do more with less? Or will it help you reduce in other places and run leaner teams? Will it disrupt or streamline your current workflows (or both)?

At the very least, every significant investment should move you closer to achieving 100% visibility of your security posture. It’s an unreachable goal, but one you should strive for nonetheless. At a minimum, test configurations to ensure that adding additional controls, turning on new features, or consolidating vendors won’t disrupt existing processes or require more manual work downstream. Realistic testing should show whether a solution creates more headaches for your team or helps you retain top talent by reducing analysts’ load.



of respondents are very (48%) or somewhat (43%) concerned about the ongoing skills shortage

Source: S&P Global

QUESTION 4

What happens next?

What's next for your business? Where do you stand with digitalization or modernization? Do you plan to migrate critical services to the cloud? Are you entering into major mergers or acquisitions?

You can't always predict the future, but you can gauge whether new tools equip you to pivot and become more agile and proactive.

Will the solution streamline compliance?

Companies invest in cybersecurity for three main reasons:

- Something bad happened
- Their partners and peers made a change first
- Someone said they had to

This last option drives more decisions as evolving standards, frameworks, and regulations call for adopting Zero Trust security postures. Ensure new additions align with guidelines like the National Institute of Standards and Technology (NIST) **Cybersecurity Framework** and **MITRE ATT&CK** knowledge base of attacker tactics, techniques, and procedures (TTPs).

Keep watch over federal mandates like the Biden administration's Executive Order on Improving the Nation's Cybersecurity targeting critical infrastructure and the UK's Telecommunications Security Act 2021 that prescribes continuous validation of security controls. Test to ensure prospective tools streamline rather than complicate compliance efforts and keep you from making a common, costly mistake: **don't assume compliant means secure!**

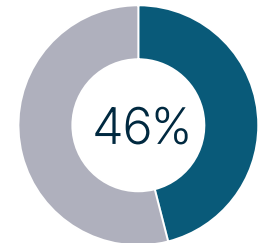
BE SKEPTICAL OF YOUR SUPPLY CHAIN

The 2022 Verizon Data Breach Investigation Report (DBIR) found that supply chain attacks and failures were responsible for 62% of known system breaches. As it becomes easier and less expensive for threat actors to mount attacks using bots and cloud computing accounts, make sure your strategic partners and potential M&A targets can prove they won't expose your environment to risk.

Can it curb insurance costs?

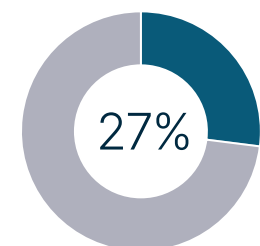
As cyber liability insurance claims and premiums skyrocket, providers hold all the cards. **RIMS** writes, "In 2022, cyber insurance became a C-level issue for commercial and government organizations. Risk managers felt fortunate if they could renew their cyber policy, maintain current coverage, and keep premium increases to below 50%."

Research from Delinea found underwriters have begun limiting policy coverage—just about 30% still covered ransomware—and demanding more assurances. Verify your security posture continuously to qualify for coverage. Testing won't automatically lower your premiums, but it pays to try!



46% of respondents said the primary challenge driving security teams is the increasing complexity/effort to comply with regulations

Source: S&P Global



27% data breach claims had exclusions within the insurance package that resulted in non-payout or partial payouts in 2022

Source: Astra

QUESTION 5

How can we prove it?

Validating your needs and capabilities continuously ensures your security stack and threat landscape evolve in tandem. The key word here is “continuous.”

You may already use multiple “point-in-time” solutions, including several that take on the role of attackers, to assess your defenses.

Outsourced Penetration (pen) testing tries to break into systems to show threat actors can gain access. Pen tests can carry a high cost—you might find a budget for only one per year—and don't simulate entire attacks. **Automated pen testing** adds scale, but still, despite

the claims of some products that offer “fully automated penetration testing.” **Red team exercises** employ similar tactics as pen testing but strike without warning. This can be an effective test, but it takes time and planning and is often not done frequently enough. And many of these approaches focus on attacking production systems that carry the risk of disrupting business processes.

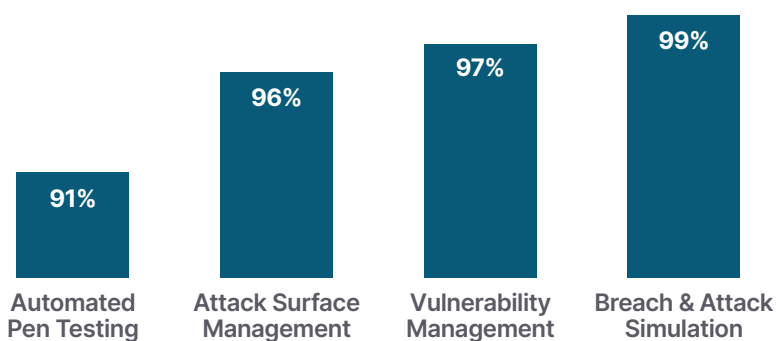
All point-in-time methods share a limitation: their results become dated the second the testing stops. **Vulnerability** and **attack surface management (ASM)** provide more continuous coverage of internal and external risk but don't simulate real-world attacks to show what might happen if weaknesses get exploited.

Breach and Attack Simulation (BAS) provides the proof

Breach and attack simulation run real-world attack scenarios against production environments to validate that controls are in place, properly configured, and working as advertised. The technique evolved from red and blue teaming to add two vital elements: automation and continuous coverage.

BAS plays a vital role in continuous security validation (CSV), an automated approach that uses security tools and techniques leveraging attacker TTPs. Industry-leading analysts recommend CSV and BAS to find and remediate risk before making new purchases.

S&P Global survey respondents believe BAS reduces business and operational risk and help analysts identify unpublished, signatureless and zero-day vulnerabilities.



Q: To what level do you agree that your current [CSV product category] tools provide a positive return on investment (ROI)? Base: Respondents with over \$750 million in revenue (n=96). Source: S&P Global Market Intelligence custom survey, December 2022.

Never assume the other guy will never do something you would never do.

Willie Mays

Organizations leveraging CSV technologies may recognize the need for a tool that can help them validate security controls and the effectiveness of other tools already in place, assisting in identifying and reducing the count of ineffective security tools.

S&P Global Market Intelligence

LIFE CYCLE VALIDATION OF SECURITY CONTROLS

BAS flags potential issues during all phases of the attack chain, anywhere on your threat landscape. Actionable insights make teams more efficient and proactive against risk from external threats as well as insider attacks and configuration drift and errors.

Simulation playbooks should feature realistic attack TTPs mapped to real threat actors so that you can run preconfigured and customized attack scenarios based on your company's environment, industry, and risk profile. BAS automates tedious aspects of red and purple teaming and captures data used in threat modeling and hunting. The right platform facilitates and promotes team collaboration to speed remediation and improves ROI.

THE EVIDENCE NEEDED FOR COMPLIANCE, INSURANCE, AND BOARD-LEVEL REPORTING

After you invest in updating your stack, BAS provides empirical data to demonstrate value. This might include achieving faster incident response (IR), improved resilience, and a stronger security posture. Because it's both automated and continuous, BAS has the potential to:

- Democratize cyber insurance
- Fast-track the M&A process
- Streamline compliance efforts
- Verify the security of supply-chain partners

Should BAS be our next addition?

According to Gartner, "Breach and attack simulation tools help make security postures more consistent and automated."

The SafeBreach BAS platform:

Integrates easily with your current stack: SafeBreach works with your existing endpoint, network, cloud, email, data loss prevention (DLP), and other controls so analysts can correlate simulated attacks against alerts and events. The platform also synchronizes with intelligence feeds and providers to ensure simulated attacks reflect the latest trends and telemetry.

Promotes collaboration with workflow management and security orchestration and response (SOAR) platforms to accelerate the response.

Provides complete use case coverage to identify high-risk vulnerabilities, detect lateral movement, and address every stage of the attack kill chain. IT can safely simulate attacks against on-prem defenses and public or private cloud infrastructures without disrupting environments.

Augments your security team and provides a simple way to train your defenders.

CONCLUSION

The skeptical buyer's bottom line: "Are we safer today than we were yesterday?"

When cybersecurity works, nothing happens, but every attack surface has gaps—and most teams lack the cycles to find and prioritize them—until it's too late. Before approving a new purchase, or asking someone else to do that for you, use CSV and BAS to remove all doubt that your recommended solutions will:

- Fix the problem you're looking to solve (and hopefully others)
- Streamline workflows and reporting
- Measurably improve your security posture and processes
- Make your team more collaborative and proactive

FEATURE / USE CASE	Automated			
	VM	PT	ASM	BAS
Scalable testing	●	◐	◐	●
Vulnerability / configuration scanning	●	◐	●	○
Real-world attack simulation	○	◑	○	●
Continuous, automated testing	●	◑	◑	●
Non-destructive tests	◑	◐	●	●
Real-world attack simulations from attacker's viewpoint	○	◑	○	●
Deep, highly customized attack testing	○	◐	◐	●
Attack surface-based discovery and risk identification	◐	○	●	○
MITRE ATT&CK TTP-based testing	◐	◐	◑	●
Single platform support for cloud & on-premises testing	○	○	○	●

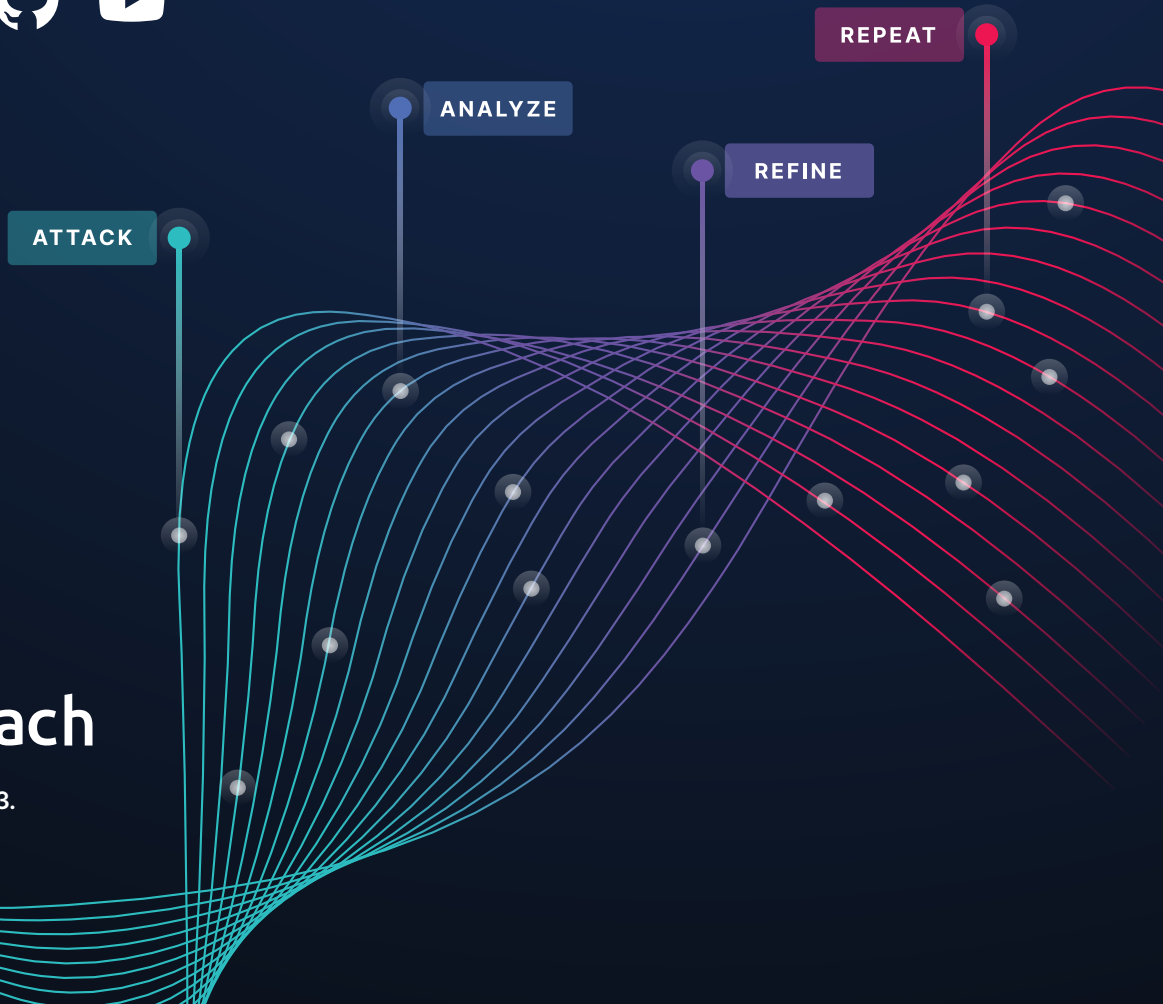
See for yourself

Check out SafeBreach.com for more resources to help you to optimize your existing security stack, and schedule a personalized demo now to discover how the SafeBreach BAS solution can help you to evaluate future security purchases.

About SafeBreach

Combining the mindset of a CISO and the toolset of a hacker, SafeBreach is the pioneer in breach and attack simulation (BAS) and is the most widely used continuous security control validation platform. SafeBreach continuously executes attacks, correlates results to help visualize security gaps, and leverages contextual insights to highlight remediation efforts. With its Hacker's Playbook™, the industry's most extensive collection of attack data enabled by state-of-the-art threat intelligence research, SafeBreach empowers organizations to get proactive about security with a simple approach that replaces hope with data.

Learn more at SafeBreach.com.



All content ©SafeBreach 2023.
All rights reserved.