Cymulate

6 Ways

BAS Increases Cybersecurity ROI

Cymulate

Table of Contents

01 | Cost vs. Value: What's at Risk?

It's no surprise that annual cyber defense costs rise every year as the number and sophistication of attacks grow. Costs associated with ransomware attacks alone have increased 21% since 2018.[1]
In 2019, 85% of managed services providers (MSPs) reported ransomware as the most common malware threat, and worse, four out of five MSPs say that they themselves are increasingly targeted by ransomware attacks.

Stats vs. Costs vs. Risk
Standalone statistics provide part of the picture. But what do they mean to your organization? What's actually at risk? The Ninth Annual Cost of Cybercrime Study found the value at risk for an average G2000 company—with 2018 revenues of US$20 billion—equals 2.8% of revenues per year. The only way to hold the line on cybersecurity costs is to improve readiness, response, and risk reduction.
That's where continuous simulation with Breach and Attack Simulation (BAS) can add huge value.

Higher Costs Prevail

Security breaches rose from 130 in 2017 to 145 in 2018[2]

Enterprise ransomware attacks increased 12%[3]

Downtime costs increased by 200% year over year

Mobile ransomware attacks increased 33%[4]

Downtime costs are 23 times higher than average ransom

78% of small businesses hit by ransomware never recover[5]

[1, 2] Ninth Annual Cost of Cybercrime Study, Accenture, conducted by Ponemon, 2019
[3] Internet Security Threat Report, Symantec, April 2019
[4, 5] Pandemic Crisis' of MSP Ransomware Attacks Will Grow in 2020, Experts Say, CRN, Oct. 4, 2019

02 | Continuous Validation with BAS

BAS challenges, measures, and optimizes your security control effectiveness. With BAS data, you have quantifiable metrics and actionable insights to improve readiness, response, and risk reduction.

BAS Enables you to:

- Simulate attacks without jeopardizing production environments
- Simulate attacks across the full kill-chain including the latest attacker tactics, techniques, and processes (TTPs)
- Simulate continuously with flexibility to target specific vectors against latest threats
- Automate simulations for repeatability and consistency
- Conduct simulations at any time interval—hourly, daily, weekly, or ad hoc
- Identify gaps and evaluate controls against MITRE ATT&CK framework
- Remediate exposure using actionable insights

Continuous Assessment
While traditional pen testing and vendor-specific platform tests deliver point-in-time snapshots, BAS makes it easy to continually assess controls across the kill-chain. Security and risk management leaders should confront the threat landscape based on a continuous assessment of threat and business evolution.[6]

03 | Increase ROI with Improved Readiness

BAS challenges, measures, and optimizes your security control effectiveness. With BAS data, you have quantifiable metrics and actionable insights to improve readiness, response, and risk reduction.

Assess Readiness from an Attacker Perspective
Use BAS to simulate and measure the effectiveness of security controls already in place. Simulations assign BAS risk scores depending on how well controls are working against known and the latest threats. You can continually test your company's ability to cope with techniques that APT groups are known to use and optimize defensibility.

Gain Continuous Visibility
It's a race—almost 80% of organizations are introducing digitally fueled innovation faster than their ability to secure it against cyberattackers.[7] At the same time, the AV-TEST Institute reports that it registers over 350,000 new malware and potentially unwanted applications every day.[8]

For "Right Now" Answers to Security Posture Questions, BAS:

- Delivers 24x7x365 visibility
- Ensures controls can detect the very latest threat IOCs
- Automatically alerts team to changes in control effectiveness

6 How to Respond to the 2019 Threat Landscape, Gartner, August 16, 2019

7 Ninth Annual Cost of Cybercrime Study, Accenture, conducted by Ponemon, 2019

8 AV-TEST, The Independent IT Security Institute

Optimize Your Current Defenses
On average, enterprises rely on 80 security products,[9] each with many configuration options. How do you know if current configurations, policies, and control settings are giving you maximum protection? BAS simulations will assess effectiveness, identify gaps, and provide remediation suggestions:

- Find and remediate control mistakes like configuration errors and disconnected sensors
- Test control configurations against the latest threats
- Find gaps in controls and close them
- Test SOC alert triage and responses
- Assess MSPs to ensure they alert and respond per SLAs

Reconfigure, harden, change policies as recommended and then simulate again. You can simultaneously capture metrics that measure improvements and changes in ROI.
Metrics also identify how well your solutions work together—from attack delivery, to system compromise, to lateral movement, and beyond.

Reduce Pen Testing Costs
Pen-testing costs, scope, and resource requirements vary, with analysis and results coming later.
Use pen testing only as needed—for compliance or specific exercises—and rely on BAS to uncover blind spots and continually improve control effectiveness.
With BAS, you can automatically simulate more TTPs faster and receive immediate results.

Enhance Red Teaming
Using BAS, red teams can challenge controls faster and more thoroughly. They can simulate against a broader spectrum of malware and many more TTPs than pen testing or manual exercises.
Results are aligned with published frameworks, such as the MITRE ATT&CK™ framework, to pinpoint weaknesses and prioritize remediation.

Compare Products Before Purchase
Use BAS to make security control purchase decisions based on comparing products' effectiveness.[10]
For example, test two vendors' email gateways in parallel and decide which delivers the highest ROI.
If the current risk level is 90/100 and one product decreases risk to 50/100, you can easily correlate purchase price and risk reduction metrics to gain accurate ROI. BAS increases ROI by enabling you to:

- Improve, validate or accelerate POCs
- Test shortlisted vendors consistently for more accurate comparisons
- Test configuration QA after deployment

9 Security, Gartner Technical Professional Advice, May 17, 2018
HelpNet Security, March 30, 2018

10 Utilizing Breach and Attack Simulation Tools to Test and Improve Security, Gartner Technical Professional Advice, May 17, 2018

04 Increase ROI with Effective Response

Using BAS to test security controls provides objective, quantifiable exposure scores and mitigation guidelines. Now you have the information you need to not only remediate issues but also increase response effectiveness.

Prioritize Resources
With limited staff and resources, teams using BAS gain the insight needed to prioritize remediation tasks based on risk. Objective, empirical exposure scores and other KPI metrics let your team focus on mitigating the most critical gaps first. Improving upstream security also reduces alerts generated downstream, increasing overall ROI of the complete infrastructure.

Save Time
Automated BAS saves time in many different ways:

- Comprehensive remediation guidelines make it fast and easy for teams to efficiently mitigate the majority of risk
- Quickly create executive reports ready for presentation
- Generate technical reports instantly to accelerate planning and remediation efforts

Keep Pace with Change
IT environments change continually. Automated BAS enables you to preempt potential adverse impact of IT configuration changes, software updates, and new technology. Continuous BAS is worth its weight in gold for companies with high M&A activity. Protect—and increase—ROI of your environment by ensuring that an acquired company's infrastructure won't compromise yours. Run attack simulations to uncover and remediate gaps with just a few clicks.

Enhance Blue Teaming
Give your SOC team the advantage over threats with full kill chain APT simulations. Automated BAS enables your SOC to ensure that the SIEM and controls are correctly tuned and respond as expected. Use BAS metrics to update or fine tune playbooks and workflows as threats and the organizational environments change.

05 Increase ROI by Further Reducing Overall Cyber Risk

Cyber risk directly affects the company's brand, financials, and shareholder value. A continuous, automated BAS platform enables your team to continuously mitigate security gaps in the face of constantly evolving threats. Quantifiable risk assessments and metrics also enable you to demonstrate improvements over time and communicate effectively with executive teams and boards of directors. Security controls that do their jobs are key to preserving companies' market valuations.

Preempt Supply Chain Attacks
Attackers often use supply chain partners as paths to their true targets. Use automated BAS to challenge the controls securing touchpoints with partners, such as portals, email and web gateways, and endpoints.

Demonstrate Security Performance Over Time
Metrics from BAS over time can demonstrate how specific security investments improved security scores. Results might show that your controls work great but too many employees are falling prey to phishing attacks. Or third parties are accessing cloud resources that should be better secured. The data to document security posture in detail over time is extremely useful to calculating ROI and identifying areas for further investment.

Increase Executive Confidence
According to a 2019 survey by the Enterprise Strategy Group, 39% of executives and directors want security status reports for cyber-risk associated with end-to-end business processes, and 35% want better detail on the ROI of their security investments and planned purchases. With BAS, you can clearly communicate how decisions improved security posture or why it suffered from lack of resources. Being able to quickly and easily correlate investments with increase or decrease of risk facilitates data-driven conversations with management and data-informed investments with your budget.

Benchmark Against Industry Peers
How do you know where you stand relative to the security posture of other companies in your industry? BAS can show you. Compared to your industry, is your security posture in good shape? BAS can tell you—down to specific vectors and TTPs.

05 | Security is Critical to Organizational Success

Not all BAS benefits are directly translatable into ROI, yet they are critical to organizational success. Flexibility is crucial—to market advantage and coping with financial unpredictability. BAS adds value here as well.

Capitalize on Agility
With BAS as an element in your cybersecurity strategy, you can proactively move the organization's security posture forward. Threat actors change. Attack surfaces change. Organizational risks change. Yet, BAS lets you accurately assess security posture at any given moment and quickly allocate resources where they are most needed. When you can turn on a dime, the organization doesn't have to compromise opportunity for security.

Maximize Cost Effectiveness
Operations costs are a critical component of calculating ROI. A subscription-based BAS solution provides cost predictability. You don't need to plan for large capital expenditures or pay for costly support and maintenance contracts with diminishing functionality.

Start Now
Why wait? High ROI is measured by more than just costs. Peace of mind—for your security team and company's executives—is hard to calculate. Automated BAS delivers the insight and data you need to preserve the security you have worked so hard to create. And at the same time, add value back to the organization by reducing the amount of revenue needed to sustain peace of mind.

About Cymulate

Cymulate was established with the vision of empowering security professionals to make better decisions faster, based on real-time data. Founded and led by an elite team of cyber researchers with world-class experience in offensive cyber solutions, Cymulate is determined to become the golden standard for security professionals and leaders to know, control, and optimize their cybersecurity posture end to end. Trusted by hundreds of companies worldwide, Cymulate constantly enhances its methods to prepare organizations for any attack scenario or campaign.
With Cymulate, organizations continuously measure security performance in real-time, shore up defenses, and assure operational effectiveness.
Measuring your cybersecurity performance is fundamental towards creating a more secure organization!

Contact us for a live demo, or get started with a free trial

Start Your Free Trial

Headquarters: Maze St 3, Tel Aviv 6578931, 7546302, Israel | +972 3 9030732 | info@cymulate.com | US Office: +1 212 6522632