WHITEPAPER

The True Cost of Cybersecurity

April 2019

APPGUARD

Cybersecurity costs are rising each year, along with breach volume. Detect-and-react strategies are becoming more complex and costly, all while failing to stem the tide. Is there a better way to identify the true cost of cybersecurity and mitigate risks more effectively?

703.786.8884
sales@appguard.us
www.appguard.us

The True Cost of Cybersecurity

Executive Summary

Here are facts most cybersecurity professionals know, or at least suspect:

- Cybersecurity costs keep rising.
- Breach volume keeps growing.
- Labor is typically the largest line item in the cybersecurity budget.
- Layered defenses correlate with endpoint protection failures.

This has been the reality for more than a decade, and while it may not be immediately obvious, there's an underlying cybersecurity strategy that results in this failed status quo. It's a reactive approach that relies on costly, time-consuming endpoint detection and response (EDR) and security information and event management (SIEM) efforts.

In this whitepaper, we'll discuss the factors that contribute to these persistent trendlines in greater detail. We'll explore the cost question from both the solution and labor perspectives, and outline an approach for determining the true cost of cybersecurity on both a monetary and opportunity basis.

And finally, we'll talk about how taking a proactive approach to endpoint protection can allow InfoSec leaders to reset cybersecurity costs. As we'll demonstrate, transitioning to proactive methods that address where overall costs originate is a better strategy. A proactive, rather than a reactive, endpoint protection strategy not only reduces costs in those areas but lowers expenses in other areas that are driven by endpoint protection incidents.

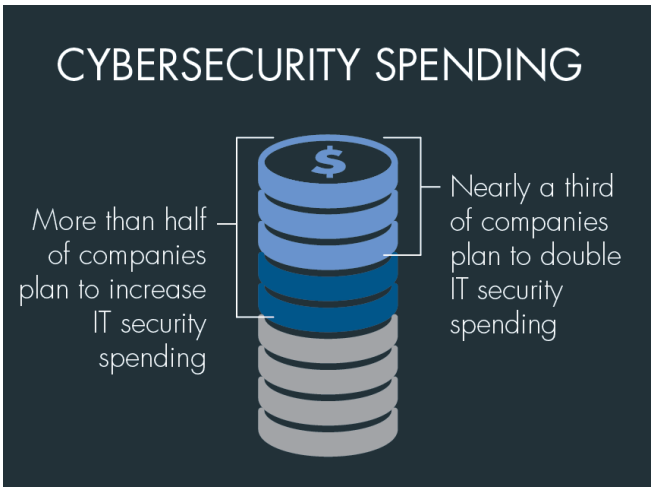
We'll never change the status quo by using the same failed strategies.

Threats and costs keep increasing

As a cybersecurity leader, your job is becoming more complex as you deal with an expanding array of threats. Data breaches are rising, and there's no end in sight. Most InfoSec professionals surveyed for the ISACA State of Cybersecurity 2018[1] report said not only did they experience higher attack volumes last year, they expect to withstand even more attacks this year.

To deal with the expanding threat landscape (as well as new regulations designed to protect privacy), cybersecurity spending is increasing.

While most CISOs welcome extra dollars in the budget, the fact is threats and breach volume keep rising along with spending.



Why current cybersecurity strategies don't work

It's a vicious cycle of failure: endpoints come under attack from new tactics, techniques, and procedures (TTPs). Defenders respond by rolling out a fresh set of tools and processes to counter new categories of attacks and vulnerabilities. This reactive strategy never reduces the volume of threats, but it does lead to cybersecurity bloat. Look at any large enterprise's current cyber defenses, you'll see many layers at the endpoint and throughout the enterprise ecosystem that have accumulated over the years. The complexity of all this makes planning, execution, and analysis more costly. Typical incident response reveals breaks in workflow and communication/coordination problems.

We've been throwing more money and people at the problem for years, so why haven't our investments made a dent in these trends?

Endpoint protection platforms (EPPs) come up short

As enterprises add new tools and incorporate practices to deal with attacks, cybersecurity tool bloat increases. A dozen years ago, endpoint protection platforms (EPPs) debuted to simplify IT and security operations. The idea was that a single agent with one management pane would be easier to handle than multiple agents and panes. Mitigating multiple attack vectors inevitably gives rise to multiple defense variations within a single agent. Consolidating multiple defense features into one agent may reduce the number of agents the organization has to test and administer, but the configuration, maintenance, monitoring, triage, investigation, and reaction chores associated with each defense feature remain a heavy burden.

Unfortunately, any gains made by agent consolidation were more than offset by EPPs' failure to effectively protect endpoints, and a whole new endpoint agent market emerged: endpoint detect and respond (EDR) solutions. EDRs are now considered a necessary feature of EPPs. But EPP feature growth isn't achieving endpoint security efficiencies—quite the opposite.

Still, too many cybersecurity professionals fall into the trap of looking at EPP feature lists rather than focusing on the value of each feature. It's understandable in a sense because threats are proliferating and new vulnerabilities are emerging, so the thinking goes, why not choose the EPP with the longest list of features to counter those threats?

The problem with that logic is it obscures the real questions we should be asking about EPPs, such as which features produce the best results and how integrating a single cyber control with others simplifies the solution.

A 2018 endpoint security trends article in CSO noted,

"COMPANIES HAVE AS MANY AS
SEVEN DIFFERENT SOFTWARE AGENTS
RUNNING ON EACH ENDPOINT, EACH OF WHICH
NEEDS TO BE MANAGED SEPARATELY."

That's expensive and time-consuming. And as we've seen, it doesn't work.

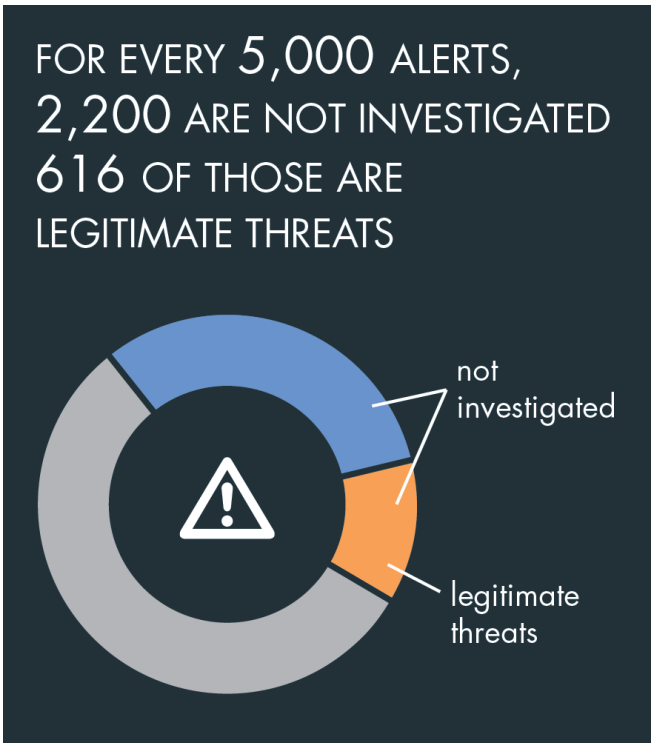
Detect and react strategies fail to deliver

In addition to proliferating EPPs, cybersecurity professionals rely on security information and event management (SIEM) to warehouse data flowing in from multiple IT and security operations sources, including endpoint log events. Alerts from tools like firewalls, intrusion detection and prevention systems, and breach detection solutions can be overwhelming.

Another category of tools, entity user behavior analytics, sprang up in response to threats that move across endpoints by stealing or hijacking user accounts/credentials. Remediation tools are also in the mix, including re-imaging, cleanup, password management, key management, backup management, and others. All add to the complexity of the *detect and react* strategy.

Alert fatigue is a serious problem, and it stems directly from the enormously complex detect and react tools organizations have deployed in a vain attempt to detect a growing list of threats.

The Cisco 2017 Security Capabilities Benchmark Study found that of every 5,000 alerts, 2,200 are not investigated, including 616 alerts for legitimate threats that aren't remediated.



The problem is that no single detection method works adequately, so multiple detection methods must be used. All of these methods combined tend to require more labor to deploy and operate. They generate yet more alerts, and no one has a large enough budget to hire sufficient personnel to handle all of the alerts. This holds true beyond the endpoint realm, e.g., for network tools such as intrusion detection systems (IDS), SIEM, and entity and user behavior analysis (EUBA).

So, current cybersecurity strategies are failing despite the annual addition of money and people. The detect and react strategies that evolved when EPP and SIEM measures failed to neutralize the threats are essentially cleaning up after the barbarians crash through the gate rather than preventing them from gaining entry in the first place.

Artificial Intelligence & Machine Learning will not fix detect & react strategies

The cybersecurity industry is now hyping machine learning solutions, and InfoSec leaders are hoping machine learning tools can "scale to the rescue," but that hope rests on a shaky premise. The fact is, **change** is machine learning's arch-nemesis and change is also the most universal enterprise characteristic. Seemingly insignificant changes in environment seriously degrade machine learning capabilities, so it's unlikely to "scale to the rescue."

It's possible that true artificial intelligence will emerge that is capable of scaling to handle the constantly growing volume of data that must be analyzed. But until then, enterprises should instead look for ways to reduce the amount of data that requires analysis. That's what a **endpoint zero trust** strategy can deliver.

A simple method to identify reaction costs points to a game changer

Instead of betting on the dubious proposition that machine learning or AI will address spiraling costs and complexity with better tools, you can tackle the issue in-house by identifying how much time your team is spending on detect and react efforts, then minimize employee hours spent running down alerts and analyzing incidents related to endpoints and beyond with a proactive rather than reactive approach.

A CSO article on false positives and alert fatigue cited an important finding from a Rapid7 report

"ATTACKERS STILL HEAVILY RELY ON USER INTERACTION. FOR INSTANCE, ON MONDAY HOLIDAYS, ALERTS DIPPED SIGNIFICANTLY, WHICH RAPID7'S ANALYSTS ATTRIBUTED TO A LACK OF EMPLOYEES INTERACTING WITH MALICIOUS EMAILS, ATTACHMENTS, ETC."

There's a simple way to identify how much effort current reactive practices entail that works for organizations of all sizes across all industries. When you calculate the difference in IT/Sec-Ops hours spent defending the enterprise on workdays vs. non-workdays, you'll have a rough estimate of the labor cost savings potential from incident avoidance. Rapid7 observations across 1,500 enterprises showed 50% fewer incidents on non-workdays.

So, by comparing the numbers of alerts and incident volumes for regular workdays with metrics gathered on non-workdays, you can get a rough estimate of what percentage of IT/Sec-Ops hours within your total IT and security operations are spent addressing security related to endpoint usage. It's typically at least half—often more. Closer analysis will reveal exactly which tools and processes consume the most IT/Sec-Ops resources. This analysis will reveal the potential impact of deploying near-perfect endpoint protection, which will reduce the IT/Sec-Ops workload on workdays to the volume experienced on non-workdays.

There are three other examples of exercises that help illustrate and quantify savings opportunities and the upper boundary on any investments on preventative approaches. These are cause and effect exercises. End users click on things that cause cyber incidents or breaches. By identifying those good and bad end users, one can compare their costs to the enterprise. The costs of supporting the "good" end users tells you the value of preventive measures that offset the choices of the "bad" end users. Similarly, looking at patch management failure costs reveal the value of a solution that mitigates those risks. Incidents involving credential theft give insight into the value of proactive approaches that avoid such incidents. Whatever ideal/actual cause and effect exercises you might perform, look at the direct cost consequences as well as the indirect. That is, what costs are NOT incurred when a failure or mistake doesn't happen.

Armed with this information, you can focus on cutting the time your IT/Sec-Ops is reducing risks caused by user activities. Then you can redeploy those forces to handle tasks that never seem to get done because everyone is too busy fighting fires. Redeploying to more strategic tasks is now possible because of a breakthrough in endpoint protection.

Focus on prevention instead of reaction

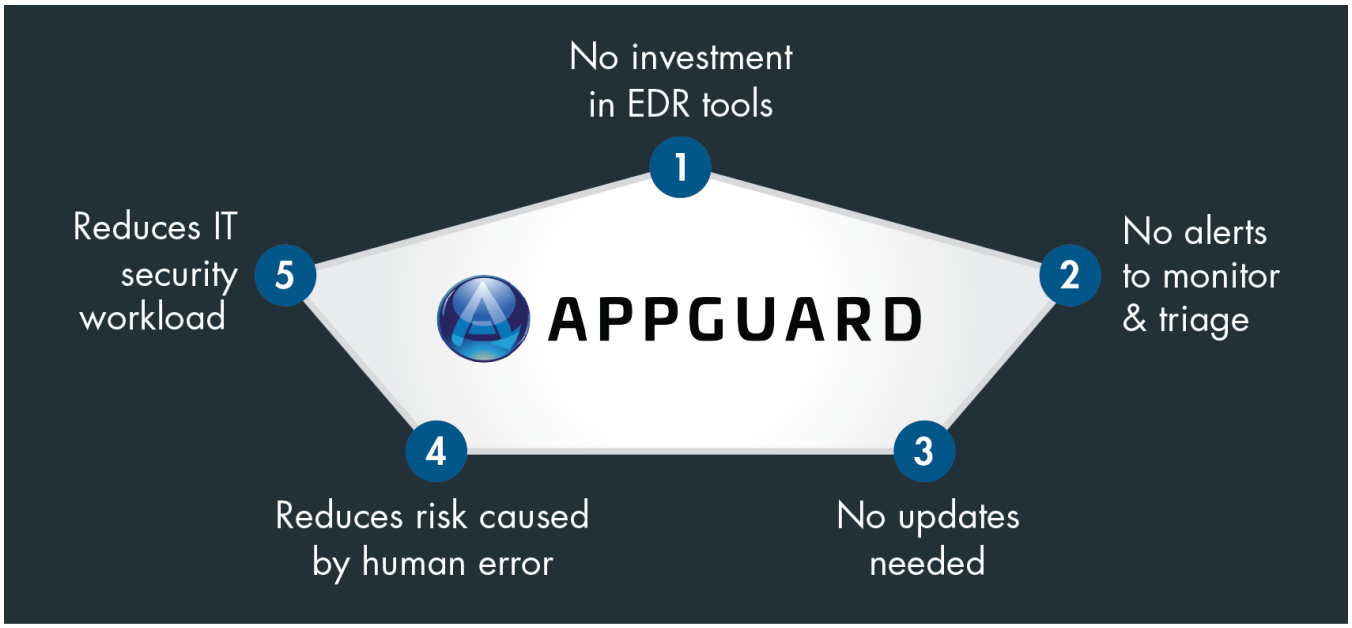
It's now possible to redirect worker hours spent running down endpoint alerts and managing incidents because there's a better alternative—a new category of zero trust endpoint protection: **AppGuard**.

An entirely new approach to endpoint protection that is based on prevention instead of reaction.

By shifting to the more proactive methods of zero trust within endpoints, you can reduce the endpoint-related workload significantly. But that's only the beginning. A zero trust endpoint solution like AppGuard not only slashes direct endpoint security costs, it reduces indirect costs. When endpoint attacks are stopped at the endpoint, downstream systems like IDS, SIEM, EUBA, and other tools generate far fewer alerts to be analyzed. That reduces the detect portion of the workload and it also cuts the react component, where staff must contain and remediate detected intrusions.

AppGuard isn't an EPP with an EDR component that requires an investment and allocation of IT/Sec-Ops hours. It's an entirely new approach to endpoint protection based on prevention instead of reaction.

It works like no other solution because all malware attacks have one thing in common: they require one or more applications to get into the endpoint and/or one or more applications to do harm. AppGuard assumes any application or utility in the endpoint can go rogue at any moment. To counter the threat, AppGuard applies zero trust concepts within the endpoint to protect it from rogue apps and utilities.



AppGuard also isolates select apps and resources to protect them from the rest of the endpoint. AppGuard is not the first product to employ compartmentalization to protect endpoints, but it's the first to make compartmentalization simple and comprehensive in one elegant solution. Sandboxing and Application Control tools effectively compartmentalize in different ways. But they require comprehensive state information about each application, which must be revised after normal lifecycle changes that constantly occur, such as updates and patches.

AppGuard's **contain and isolate** controls rely on higher level abstractions that naturally adapt to lifecycle changes. This is why AppGuard agents can go months or years without the need for policy updates. AppGuard competitors try to tell good from bad files and normal from abnormal behavior. AppGuard does neither because the possibilities are infinite. Instead, AppGuard's isolate, contain, and other zero trust controls block the intended *actions* of malware without having to recognize it or its effects. This is why it is so much more effective than alternatives, which are only successful when they are able to recognize malware or its effects.

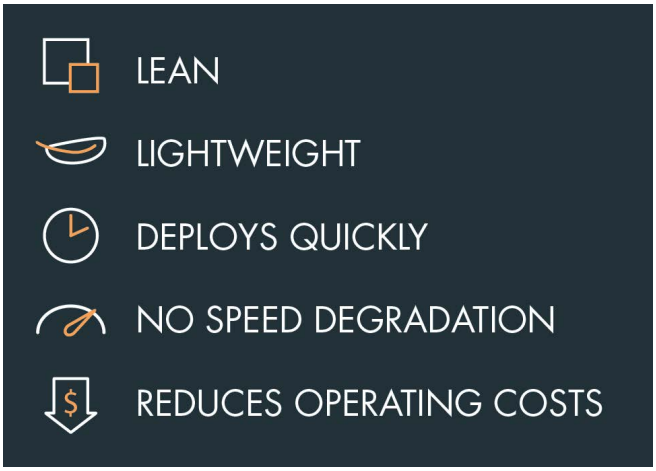
Patch management relief and more

AppGuard also tackles one of the thorniest issues IT and security operations organizations face today—patch management—through a preventive approach. Bad actors continue to exploit known vulnerabilities, and patch deployment often lags because of the complex cybersecurity workload. Since AppGuard assumes an app can go rogue at any moment, it prevents harm by ensuring adversaries

would fail to cause harm if they did succeed in hijacking an app because it was missing a patch. This means enterprises don't have to rush patches out. AppGuard doesn't eliminate the need to deploy patches, but it does give overworked IT teams breathing room to work methodically because it doesn't allow unpatched Apps to do harmful actions.

Beyond patch management

In addition to gaining patch management relief, enterprises that use AppGuard can eliminate or significantly reduce the time IT/Sec-Ops professionals spend on tasks like application white-listing, anti-exploit/memory protection, host-based sandbox and machine learning antivirus activities.



AppGuard replaces EPPs and eliminates the management overhead associated with them. Mandated scanning tools may need to remain in place for compliance, but those requirements can often be satisfied with low-cost or free tools that don't consume massive amounts of IT/Sec-Ops resources.

AppGuard overturns the unsustainable status quo.

A lean, lightweight solution that simply works

AppGuard is lean: it's 10 to 200 times lighter than alternatives in terms of CPU, memory, install size, and network bandwidth.

AppGuard can be deployed quickly. And since it doesn't scan files, it doesn't degrade endpoint speed and dramatically reduces operating costs. But most important, by addressing the root cause of tool bloat and spiraling personnel costs–chronic endpoint protection failures–AppGuard overturns the unsustainable status quo.

AppGuard not only takes less effort to deploy and operate, it also reduces the efforts required of other cyber programs, such as EDR and SIEM. AppGuard is not yet-another EPP with an EDR component "tool" that generates more alerts than your people can process. You don't have to believe the hype–just deploy it on your endpoints, and you'll see your EDR alerts plummet as AppGuard blocks attacks before the EDR agent can even detect them.

The drop in EDR alert volume will be reflected in your SIEM as AppGuard log events run through it. An AppGuard customer who was simultaneously using a leading EDR product learned this first-hand when the vendor admitted the EDR solution had failed to detect weaponized document attacks because AppGuard shut them down before they could be detected.

With this solution, you may find you can eliminate not only EDR agents but also SIEM endpoint agents. And slashing tool bloat and reducing alert fatigue can have a transformative effect on your IT and security operation.

Conclusion: Adopt a proactive vs. reactive paradigm

For more than a decade, cybersecurity vendors have offered new and additional appliances, agents, and workflows to counter the growing threats companies face. These accumulating tools and layers drive massive labor hours to detect and respond to threats.

As we've seen, the spiraling costs and labor requirements stem from a reactive strategy that is focused on detecting and responding to threats. Until now, companies didn't have other choices, so cybersecurity leaders essentially managed the fallout from attacks to contain the damage rather than shutting them down before any damage occurred.

Now there's an alternative to annually adding more detect and react tools. A simple comparison of workday vs. non-workday alert and incident volumes underscores just how much of your organization's resources are consumed by chasing down user-driven endpoint failures and alerts—expenses that until now were a seemingly unavoidable component of the cost of cybersecurity.

Isn't it time to try something different? AppGuard offers a proactive, preventive approach to endpoint protection that drastically frees valuable IT/Sec-Ops resources. That's an opportunity to reset the true cost of cybersecurity instead of letting product failure drive it higher each year.

Endnotes

[1] "State of Cybersecurity 2018," ISACA
https://cybersecurity.isaca.org/state-of-cybersecurity
[2] "Data breaches, GDPR lead 54% of companies to increase IT security spending," TechRepublic
https://www.techrepublic.com/article/data-breaches-gdpr-lead-54-of-companies-to-increase-it-security-spending/
[3] "5 top trends in endpoint security for 2018," CSO
https://www.csoonline.com/article/3275958/5-top-trends-in-endpoint-security-for-2018.html
[4] "Cisco 2017 Security Capabilities Benchmark Study"
https://www.cisco.com/c/dam/m/sl_si/events/2017/cisco-connect/pdf/ConnectSLO_What-can-you-lose_Security_2015-03-16-v3.pdf
[5] "False positives still cause threat alert fatigue," CSO
https://www.csoonline.com/article/3191379/false-positives-still-cause-alert-fatigue.html

A Blue Planet-works Company

VA Office

14170 Newbrook Drive
Suite LL-01
Chantilly, VA 20151
USA

NY Office

333 Seventh Avenue
10th Floor
New York, NY 10001
USA

Tokyo Office

(Blue Planet-works, Inc.)
Daiwa Jingumae Bldg.,
3Fl2-4-11 Jingumae
Shibuya-Ku Tokyo,
150 - 0002
Japan

703.786.8884
sales@appguard.us
www.appguard.us