WHITEPAPER

How to Optimize Your Cybersecurity Stack

October 2019

APPGUARD

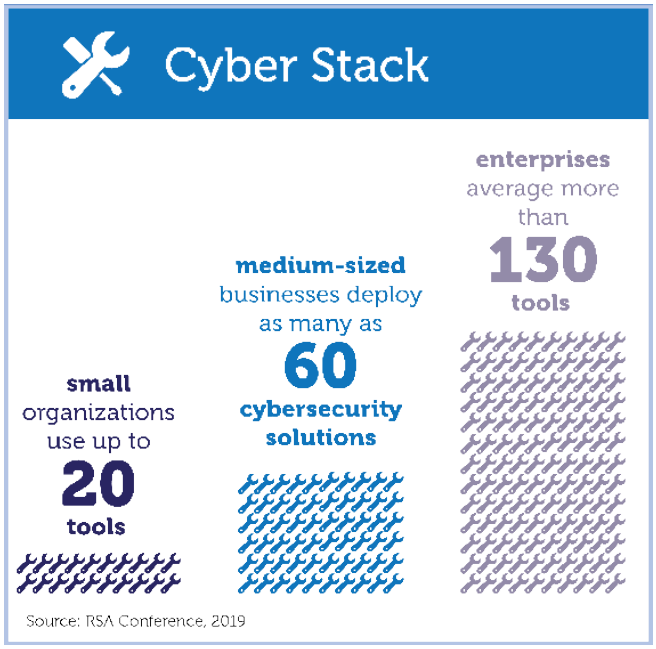
With data breaches up 54% and multiple terabytes of records exposed by hackers in recent months, spending on cybersecurity by worried company leaders is also reaching new heights. Your cybersecurity stack might be expanding, but is it up to today's complex challenges? Learn how various classes of security tools and techniques overlap and find out how a strong foundation can help you optimize your cybersecurity stack while keeping costs under control.

sales@blueridgenetworks.com | 1-800-722-1168 | BlueRidgeNetworks.com

Executive Summary

Companies keep adding more tools and people to their cyber programs, yet breaches and cybersecurity spending continue to increase. This paper explores why some tools can be eliminated and how others can have reduced workloads by deploying preventive controls at the endpoint.

Cybersecurity spending is spiraling upward as IT/Sec-Ops decision-makers scramble to field new tools to counter emerging threats. During an RSA Conference 2019, [1] speaker estimated that small organizations use up to 20 tools, medium-sized businesses deploy as many as 60 cybersecurity solutions, and enterprises average more than 130 tools.



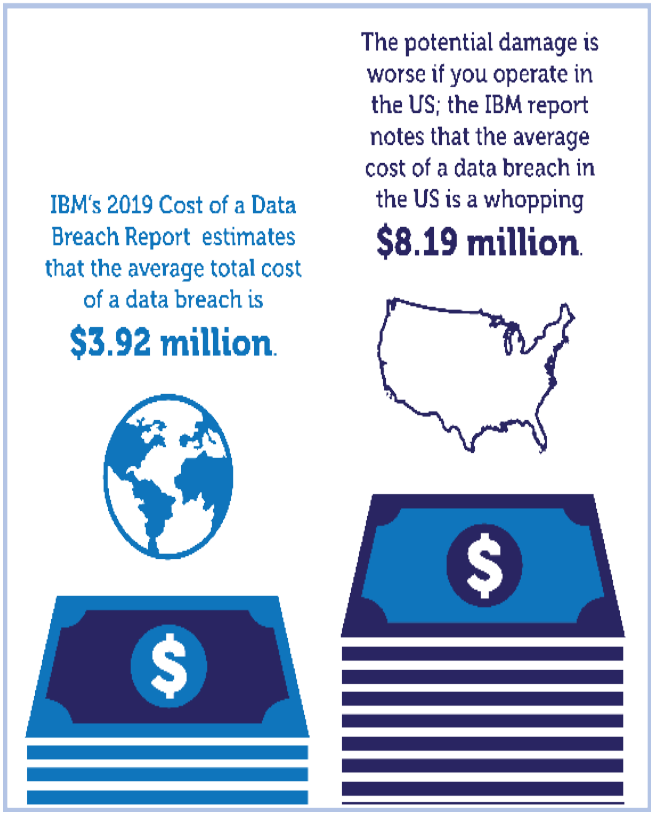
But deploying more cybersecurity solutions won't necessarily make your organization safer. The key to creating a safer environment is to build a strong foundation, inventory the cybersecurity stack with an eye toward eliminating redundancies and use labor resources more efficiently. By optimizing your cybersecurity stack, you can operate safely in a connected world — and control your budget.

In this whitepaper, we'll take a look at the scale of the cybersecurity challenge and some of the tools commonly deployed to reduce risks. We'll discuss a new approach to cybersecurity to rightsize the stack and use resources more effectively. We'll review impacts at the endpoint, network, data, and IT/Sec-Ops levels. And finally, we'll discuss how building the cybersecurity stack on a strong foundation can reduce costs and risk.

By optimizing your cybersecurity stack, you can operate safely in a connected world — and control your budget.

Data Breaches and Costs Are Increasing

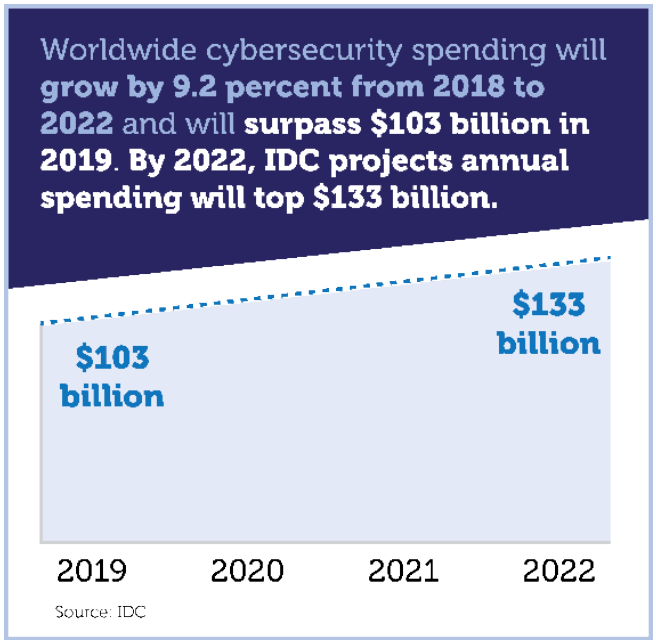
Data breaches increased by 54% in the first half of 2019,[2] according to a recent article in TechRepublic. Giant data breaches like those at Capital One[3] and Equifax[4] exposed highly sensitive personal information on hundreds of millions of consumers, and the settlements will likely cost those companies hundreds of millions of dollars.



Meanwhile, the average cost of a data breach is soaring. IBM's 2019 *Cost of a Data Breach Report*[5] estimates that the average total cost of a data breach is $3.92 million. The potential damage is worse if you operate in the US; the IBM report notes that the average cost of a data breach in the US is a whopping $8.19 million.

Cybersecurity Costs Also on the Rise

Predictably, rising costs and risks are leading companies to spend more on cybersecurity.



Companies in the US are expected to spend the most to counter cybersecurity threats, followed by organizations in China, Japan, and the UK. Larger companies (defined in the IDC report as organizations with 500 or more employees) will spend the most. Federal government organizations and manufacturers will account for about 20% of the spending total.

Technologies, Processes, and Manpower Companies Use to Mitigate Risk

So, what kind of tools are companies using to mitigate cyber risks? Your organization's IT/Sec-Ops team likely uses an array of technologies and processes to mitigate threats. To protect endpoints, companies typically use some or all of these approaches and technologies:

- Endpoint detect and response (EDR) solutions
- Native OS antivirus
- Native OS firewall
- Machine learning antivirus
- Application whitelisting/control
- Anti-exploit
- Host intrusion prevention system
- Behavior analytics
- App sandbox/virtualization
- Patch management
- Password management
- Disk encryption
- Device control
- Data loss prevention (DLP)
- Backup

To mitigate threats to networks, companies deploy a range of technologies and processes that typically include the following:

- Network sandbox
- Unified threat management
- Next-generation firewall
- Breach detection system
- Email security and proxies
- Software-defined networks
- Intrusion detection system
- Federated identity

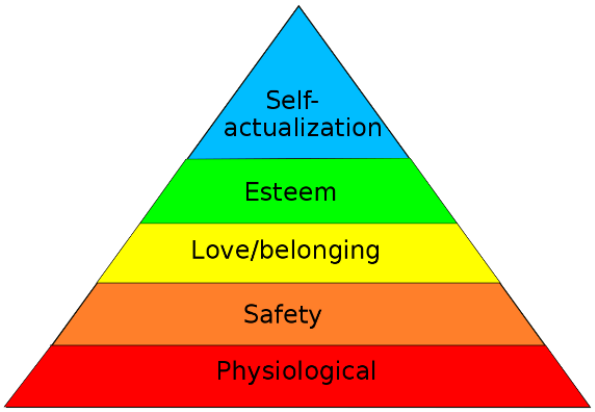
Companies also deploy an array of tools and techniques to safeguard their data, including user entity behavior analytics and security information and event management (SIEM) agents. IT/Sec-Ops teams also engage in remediation and network admission control activities, quarantine endpoints, and respond to alerts to mitigate risks.

In addition, IT/Sec-Ops teams are spending hours on threat intelligence and hunting activities, managing incident responses, alert monitoring, and leading security awareness training (or outsourcing that function to vendors). When viewed in their entirety, it's easy to see how all the tools and techniques currently in use can create overlaps and require considerable triage and maintenance, while still leaving gaps that allow hackers to breach sensitive data.

There's a Better Way to Manage Risks and Reduce Costs

One reason costs are out of control is that vendors tend to put too much emphasis on *products*, creating a mindset that emphasizes technology over resources. This leads to the misconception that the latest product or class of products will solve the data breach problem once and for all. Experience demonstrates unequivocally that this isn't true.

There's a better way to manage risks and reduce costs. It starts with getting out of reactive mode, focusing on prevention, and organizing the cybersecurity solutions stack according to a hierarchy of needs. Remember Maslow's hierarchy? That iconic pyramid illustrated a theory of human motivation for generations of psychologists, positing that foundational needs must be met before higher aspirations could be fulfilled.



A similar concept can drive the creation of a sound cybersecurity strategy. By building the cybersecurity stack on a strong foundation, IT/Sec-Ops leaders can manage risks more effectively and take control of costs. Prevention should form the foundation of the cybersecurity solution stack — a preventive solution will stop attacks at the endpoint before they strike. Detect and react tools require constant monitoring and triage. Because this technique relies on signature and pattern-based data, there is no guarantee it will stop the next attack. A preventive approach eliminates the risks and costs associated with detect and react.

AppGuard can serve as a strong foundation because it takes a fundamentally different approach to cybersecurity, protecting operating systems through kernel-level policy enforcement. With dynamic isolation and inheritance technologies, AppGuard prevents breaches by blocking applications from performing inappropriate actions while allowing them to continue with normal ones.

Replacing or Enhancing Cybersecurity Products and Approaches

With a zero-trust approach, AppGuard's controls prevent malware from causing harm — preventing harmful action before it sends an alert that requires a staff response. AppGuard doesn't depend on signature or pattern-based data as new malware threats emerge, because it blocks all malicious actions and adapts in real-time, eliminating multiple alerts.

AppGuard serves as a lifetime patch, even against sophisticated attacks. AppGuard agents can run for months and even years, all without policy updates or massive resource consumption. The AppGuard agent is lightweight and with its unique preventive approach, replaces or enhances many different types of endpoint and network security products and methods while reducing costs.

AppGuard on Endpoints

By deploying zero-trust principles within the endpoint, AppGuard replaces or eliminates the need for the following techniques and tools:

- Machine learning antivirus
- Application whitelisting/control
- Anti-exploit
- Host intrusion prevention system
- Behavior analytics
- App sandbox/virtualization

Once installed, AppGuard either replaces or enhances the function of these protections on the endpoint:

- Native OS antivirus
- Endpoint detect and response (EDR)

AppGuard also enhances the operation of the following tools and techniques in endpoints:

- Patch management
- Password management
- Disk encryption
- Device control
- Data loss prevention (DLP)
- Native OS firewall
- Backup

Functions like patch management and password management will always be necessary, of course, but AppGuard relieves the pressure on overworked IT/Sec-Ops teams by alleviating alert fatigue and hours spent on triage.

Networks

AppGuard's preventive, zero-trust approach replaces or eliminates the need for the following tools and techniques in networks:

- Network sandbox
- Unified threat management

After installing AppGuard, IT/Sec-Ops leadership can either replace the following systems or keep them in place with AppGuard functioning as an enhancement:

- Next-generation firewall
- Breach detection system
- Email security and proxies

AppGuard enhances the function of the following tools and systems:

- Software-defined networks
- Intrusion detection system
- Federated identity

AppGuard's preventive approach protects data by replacing or enhancing user identity behavior analytics and enhancing security information and event management (SIEM) agents. By shutting malware down at the kernel level and preventing apps from performing malicious functions, the need for IT/Sec-Ops to perform these activities is reduced, and in many cases, eliminated.

For IT/Sec-Ops teams, AppGuard alleviates alert fatigue,[6] which is a huge problem that prevents professionals from investigating legitimate issues by overwhelming them with false alarms. It eliminates signals generated from EDR solutions and SIEM agents by taking care of issues proactively and reduces the chatter from intrusion detection systems.

As a foundational cybersecurity technology, AppGuard replaces anti-malware solutions at the endpoint and provides immediate relief on patch management, alerts, incident response, and disruptions caused by endpoint quarantines. It relieves the burdens remediation and network admission control activities currently impose on IT/Sec-Ops teams.

Replace or Enhance Your Cyber Stack with AppGuard

Labor	Skills	Cyber Stack w/o AppGuard	Cyber Stack w/ AppGuard	Labor	Skills
5	5	EDR	Optional	2	5
5	3	Patch Management	Enhance	2	2
2	4	Network/Cloud Sandbox	Eliminate	none	none
5	4	Intrusion Detection System	Enhance	2	4
4	4	Next-Gen Firewall			
5	5	SIEM	Enhance	2	5
3	2	UEBA		2	2
5	5	Incident Response	Enhance	2	5
3	5	Threat Intelligence	Enhance	2	5
5	5	Threat Hunting	Enhance	2	5

Higher labor and skills attribute to higher costs.

APPGUARD

Conclusion: AppGuard Is a Strong Foundation for a Cybersecurity Stack

Deploying a foundational solution like AppGuard can be transformational for a company's cybersecurity posture. With its preventive approach, AppGuard creates a strong foundation upon which IT/Sec-Ops leaders can build a rational cybersecurity stack by replacing or enhancing numerous reactive techniques and tools with a single proactive solution.

Labor is typically the top-line expense in a cybersecurity operation. AppGuard not only eliminates a significant portion of the products and appliances IT/Sec-Ops teams use to mitigate threats, it frees those professionals to work on more strategic tasks (like higher-level threat intelligence and hunting) by stopping the incidents and alerts that routinely bog
IT/Sec-Ops professionals down.

To get an idea of how much noise can be eliminated with a strong cybersecurity stack foundation, take a look at the volume of alerts generated on a workday versus a non-workday. When AppGuard is installed, IT/Sec-Ops leaders can reasonably expect a similar drop in volume on workdays that they currently see on non-workdays — that's how effectively AppGuard shuts down threats. This gives IT/Sec-Ops more time to address cyber readiness at every level.

If you're ready to optimize your cybersecurity stack, explore how AppGuard can allow you to reduce the size of your cybersecurity stack, cut resources usage, and lower labor costs while increasing security at your organization — all at the same time. With a strong foundation, you can build a strong cybersecurity stack that works for your company.

Endnotes

1: "RSA 2019: Most Organizations Use Too Many Cybersecurity Tools," BizTech
https://biztechmagazine.com/article/2019/03/rsa-2019-most-organizations-use-too-many-cybersecurity-tools

2: "Data breaches increased 54% in 2019 so far," TechRepublic
https://www.techrepublic.com/article/data-breaches-increased-54-in-2019-so-far/

3: "100 million Americans and 6 million Canadians caught up in Capital One breach," ZDNet
https://www.zdnet.com/article/100-million-americans-and-6-million-canadians-caught-up-in-capital-one-breach/

4: "What You Should Know About the Equifax Data Breach Settlement," Krebs on Security
https://krebsonsecurity.com/2019/07/what-you-should-know-about-the-equifax-data-breach-settlement/

5: "2019 Cost of a Data Breach Report," IBM
https://www.ibm.com/security/data-breach

6: "False positives still cause threat alert fatigue," CSO
https://www.csoonline.com/article/3191379/false-positives-still-cause-alert-fatigue.html