Overly Managed Security

Brian Murphy, CEO

Re-thinking the Problem

Over the past ten years, the cybersecurity market has exploded with tools, technologies, platforms, and service providers, who got into the business of security for the same reason most people get into any business: to help solve a problem.

In most cases, the technologies are useful and the service providers are well-intentioned. Yet, the core issues of cybersecurity haven't gone away. It's still more expensive to be "good" than to be "bad" in cybersecurity. Security teams still struggle to fully optimize their technologies in a way that best meets their specific business needs. Organizations still have to make the choice between increasing visibility across their environment or normalizing their spend. And security teams continue to be inundated by too many unnecessary alerts to glean meaningful insights that best serve their larger organizations.

What if we're thinking about the challenges in the wrong way?

The cybersecurity issues facing most enterprise organizations won't be solved by simply adding more tools or more people. The real problem is that we've underestimated what our security tools and our security teams can do. What organizations need is the ability to automate the security operations function to increase visibility, gain access to different types of data outside of restrictive point technologies, and to create an infrastructure where it's easier to onboard and interchange team members as needed.

The solution requires a new approach to security that makes best use of the valuable tools and talented individuals we already have—in ways that haven't yet been defined.

Uniform Solutions for Unique Organizations

No two businesses are alike. **In almost every case, two organizations of the same size, within the same industry, that have the same compliance, regulatory, risk or threat concerns will still have different IT environments and approaches to security.**

One company may have grown through acquisitions, requiring the merging of many different network architectures. Another may have grown organically over a 50-plus year period, adding in various mainframe and storage infrastructures along the way that may not easily integrate with the latest cybersecurity technologies on the market.

Both companies in this example have talented security professionals capable of vetting the many security technologies available in the market. Both companies usually can get the budget they need to purchase those technologies. Yet, both companies may still face the same monotonous day-to-day maintenance and monitoring of the technologies and still may not get the data visibility they need. They may be constrained by the fact that their tools can't talk to each other. They still face increasing and unpredictable costs to access their own data.

Meanwhile, the security industry continues to produce more and more tools. These tools are being created by brilliant technologists, who are pushing the envelope of what is possible. But they still face the challenge of designing technology products that must utilize one code-base to solve problems for many organizations. These organizations must then try to fit the uniform tools to their own unique infrastructures with their own business needs. As a result, organizations may end up using the tools in different ways than they were intended, with the tool taking the blame.

The Security Information and Event Management (SIEM) tool is the poster child for this type of misaligned reputation. The SIEM has been sold as the single pane of glass for the better part of two decades, and in almost every case it fails to live up to that billing because it can't possibly manage all the data types across a diverse set of enterprise architectures. **The reason: there isn't a standard install when it comes to the enterprise. The SIEM is a powerful tool with a valuable place in the security eco-system, *but it can't do it all*.** The same can be said for the rise of the advance endpoint technologies, UEBA, etc. More tools, same issues.

In an effort to help bridge the gap between the capabilities of the tools and the outcomes organizations expect, countless managed security service providers have emerged. But not unlike the tools, too many service providers have adopted a similarly standardized "one-size-fits-all" approach in the name of scale that dilutes the service they were brought in to provide.

Instead of getting the individualized outcomes an organization expects from its tools or its service provider, the security team often ends up on the outside of a black-box filtering service with too many meaningless alerts and too little analysis. Or, the service provider narrows the scope of data too much, leaving fewer alerts, but even less meaningful visibility.

The reality is, most security teams in enterprise organizations know exactly what visibility they need and how certain pieces of data are relevant to the overall business. They don't need someone else's proprietary solution telling them what to do. They need the ability to tie it all together.

The Costly Data Dilemma

Complicating the challenge is the increasingly expensive proposition of choosing to increase data visibility or normalize the security spend. Because many security technologies price on throughput or storage, the only way for a security team to see more of its own organization's data is to buy access to it. And every tool requires a decision on access independent of all other tools.

As the data is accessed, it still has to be normalized between tools and technologies. Parsing data for this purpose is complicated. The manufacturers of the security technologies can't do it well, which is why APIs are limited, and maintenance and upkeep takes time and resources. As a result, there are many data sources that are left on the table, rather than being used to make practical security decisions.

The current approach is to just attach the words, "Artificial Intelligence" or "Machine Learning," to a solution, expecting an algorithm to solve these complex problems without changing the premise of the issue. There is no doubt that AI and ML will have a significant impact on cybersecurity, but it won't be automatic. The technology still needs to learn and develop, and it still requires a significant investment of time and effort from security teams to normalize data for this technology and then "teach" it through use-cases. **We can't do to AI and ML what we did to SIEM—expecting a promising technology to be the solution for all our issues as an industry and then blaming it when it doesn't live up to these unrealistic expectations.**

Workforce: The Scapegoat

Amid these issues, some suggest we simply need to hire our way out. Cybersecurity has been called *"The fastest growing job with a huge skills gap."* Similar headlines echo this fear and uncertainty in the wake of every major security breach. But just as buying more tools won't fix the fundamental challenge of tools not performing correctly for unique organizations, simply hiring more people isn't the answer either. The truth is, if there were suddenly one or even two million more skilled cybersecurity professionals in the industry, security teams would still struggle to fit homogeneous security tools into unique organizations. They would still struggle to create custom processes that can drive meaningful business outcomes. Data visibility would still be limited by total cost of ownership.

The problem isn't that we simply need more people. The problem is that existing security teams can't perform to their fullest capabilities because they are often overwhelmed with monotonous alerts caused by tools being misconfigured or not being used in the ways they were intended. Security teams are spending their days on high-time, low-brain alerting functions, leaving little time for higher-value contributions to the organization, which results in high turnover rates among individuals who are wired to be engaged and challenged. **Why shouldn't the security industry take advantage of ways to automate monotonous activities in a way that's customized to the business's needs, driving more visibility to more meaningful information and creating more value for everyone?**

It's no different than other industries that require individualized integration to be successful, such as with ERP systems, websites, or custom databases. None of these functions would exist without significant automations, nor would they be successful without the ability to customize and scale them according to the organization's needs. Even if there was a wealth of skilled talent in ERP or web development fields, there's no amount of talent that would make a one-size-fits-all ERP tool or standard website to work for every distinctive business.

Re-write the Rules

There are more technologies, more tools, more service providers, more skilled individuals than ever in the security space. The solution isn't more. *The solution is that we have to stop forcing security tools to work in ways they were never intended*. We have to stop blaming workforce shortages for our shortfalls as security providers. We have to reject the notion that throwing tools or money or people at the issue will make it go away.

What we need is the ability to design individualized outcomes that fit every unique organization regardless of the technology it uses, how the organization is structured, or how long ago its infrastructure was configured. Organizations should expect their security service providers to customize, automate and innovate any of their existing technologies behind the scenes so the organization's team members can focus on functions that take full advantage of their talents and their business knowledge. Organizations should demand more data visibility without having to continue paying more for it, through a variety of options to ingest and distribute that data differently.

The truth is, the only service provider that matters is the security team within each organization—working to serve its own business, enabling it to provide food, healthcare, critical infrastructure or other services to its own consumers. We as an industry owe it to them—the real service providers—to deliver on that responsibility.

It's time we make the customer the platform, providing continuity and visibility that fully leverages the technologies and team that already exists.

ReliaQuest is pushing the boundaries of IT security—past allegiance to any one security tool, workforce limitations, or definitions of existing market categories. Our technology is delivered as a customized service, allowing enterprise security teams to stay agile without compromising quality. It maximizes investments organizations have already made, adding access to broader sources of data. We transform organizations into their own security platforms—providing unmatched visibility while normalizing spend. ReliaQuest operates 24 hours a day, 365 days a year from Security Operations Centers in Tampa, FL, and Las Vegas, NV. ReliaQuest's model is recognized by industry experts as the emerging standard for large and complex organizations. The company has received numerous accolades for its commitment to maintaining a positive company culture. In 2017, ReliaQuest was named a national Great Place to Work®, listed as one of FORTUNE Magazine's Top 100 Medium Workplaces and ranked No. 171 on Deloitte's Technology Fast 500™, a list of the 500 fastest growing technology companies in North America. Also in 2017, ReliaQuest CEO Brian Murphy was named EY Entrepreneur of the Year for Florida. In January of 2018, ReliaQuest was named one of the Best Workplaces in Technology by FORTUNE Magazine and Great Place to Work.

BRIAN MURPHY
Founder and CEO
ReliaQuest

(800) 925-2159 **www.reliaquest.com** **info@reliaquest.com**