

■ FEBRUARY 2019



**EBOOK**

---

# THE ECONOMICS OF CYBERSECURITY

**embark.**

**ARMOR**

# THE ECONOMICS OF CYBERSECURITY

## Tools for Financial Executives to Navigate the Cybersecurity Landscape

### CONTENT

Chapter 1: A Data Breach Can Cost You Dearly Chapter 2: The Good Stuff: IT & Security Teams Can Provide a Powerful Defense Chapter 3: More Good Stuff: How CFOs Can Mitigate Cyber Risk
Chapter 4: A Phalanx on the Digital Front Chapter 5: Diligence and Focus on Priorities Can't Lose Chapter 6: A Cautionary Tale

## AUTHORS



Armor is a cloud security company that takes the complexity out of protecting your data, whether it resides in a private, public, or hybrid cloud—or in an on-premise IT environment. We provide managed security solutions that give you a clear picture of threats facing your organization. This allows us to provide you with the people and security resources to stop attacks before they happen and react quickly and effectively when they do, keeping your data safe and compliant. Wherever you are on your cloud journey, Armor can help. We make cybersecurity simple. To learn more, visit [www.armor.com](http://www.armor.com) or follow @armor on Twitter.



Embark is a new kind of financial consulting firm disrupting the professional services industry, working with clients in both the public and private sectors. Their ultimate goal is to provide peace of mind to corporate finance & accounting leaders at various stages of an organization's life cycle. In addition to enhancing control environments for better data governance and monitoring, Embark provides financial advisory and consultancy services throughout moments of organizational change such as transactions, hypergrowth, turnover, relocation, VC/PE investment, accounting guidance changes, and more.

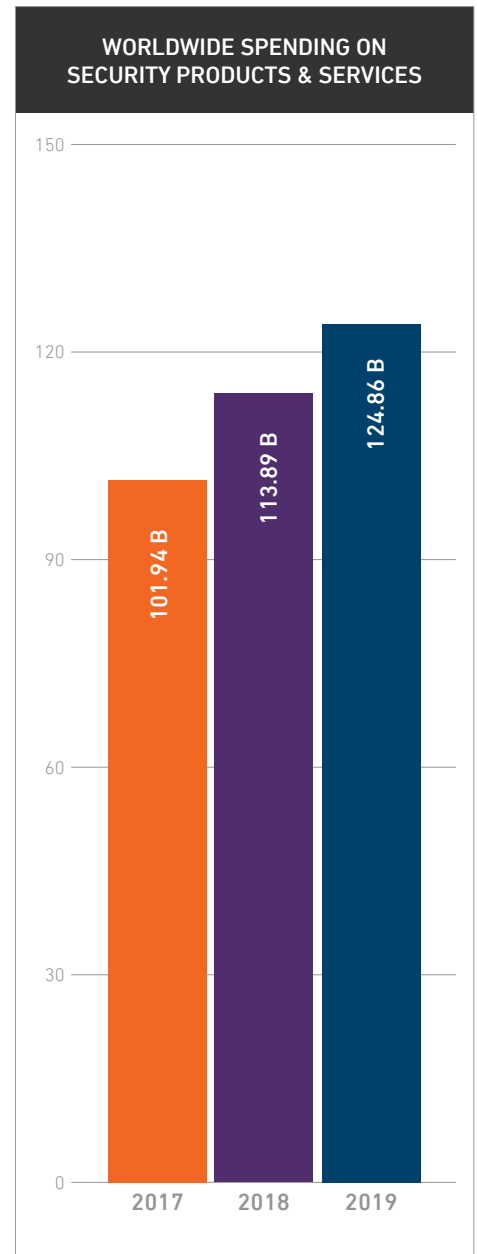
# INTRODUCTION

Cybersecurity events and incidents are a real risk to your business. In fact, the theft, copy, and use of sensitive and/or confidential data by threat actors is one of the top three financial risks businesses face today. Not only are these attacks damaging to a company's bottom line, but its brand and reputation suffer too. And this risk? It isn't going away.

According to the latest forecast from leading research firm Gartner, worldwide end-user spending on information security and risk management products and services is anticipated to reach over \$124.86 billion. Gartner is also forecasting that worldwide end-user spending for information security and risk management products and services will grow at a compound annual growth rate of 9.1% from 2017 through 2022 to reach \$175.5 billion in constant currency.

Protecting companies from data breaches is no longer just the responsibility of the CIO and the CISO. The escalating risk to the business is clear, measurable, and material. Financial leaders, including a company's chief financial officer (CFO), can ill-afford to overlook cybersecurity as a serious component of 2019 planning and must play an active role. CFOs are aligned at the confluence of operations, compliance, legal, reporting, and executive management. That lens allows the CFO a unique vantage point to direct all parties involved toward a security-focused strategy. Effective risk management requires multiple layers of defense, so not only do your company's accounting and financial executives hold responsibility, internal auditors should also participate in mitigating data loss and meeting regulatory expectations.

Understanding your cyber risk is an ongoing, cross-functional effort that must be refreshed as technology evolves. For that reason, Armor has teamed up with Embark, a Dallas-based financial consulting firm, to provide best practices for accounting and finance leaders to navigate the ever-evolving cybersecurity landscape, as well as guidelines on how to get the most from your next audit.



Gartner, Forecast: Information Security and Risk Management, Worldwide, 2016-2022, 3Q18 Update, Rustam Malik, Deborah Kish, et al., 19 November 2018.

Chart/graphics created by Armor based on Gartner research.



# PART 1

## CYBERSECURITY FOR ACCOUNTING AND FINANCE LEADERS





Companies today must be in compliance with many industry standards while also maintaining the security of their data. With ever-increasing risk to that data, breaches and leaks are now par for the course. As such, it's not enough to rely solely on your CIO to divert your company from danger. Accounting and finance leaders play a crucial role in shoring up any binary cracks in the armor.

To all of those reading these words, we urge you to take the following best practices to heart because, like it or not, they could very well keep your enterprise, stakeholders, and workforce safe from threat actors who would like nothing better than to take what isn't theirs. It's also helpful to keep in mind that working with outside financial consultants can provide added expertise and guidance to the cause to help your enterprise be as safe and secure as possible.

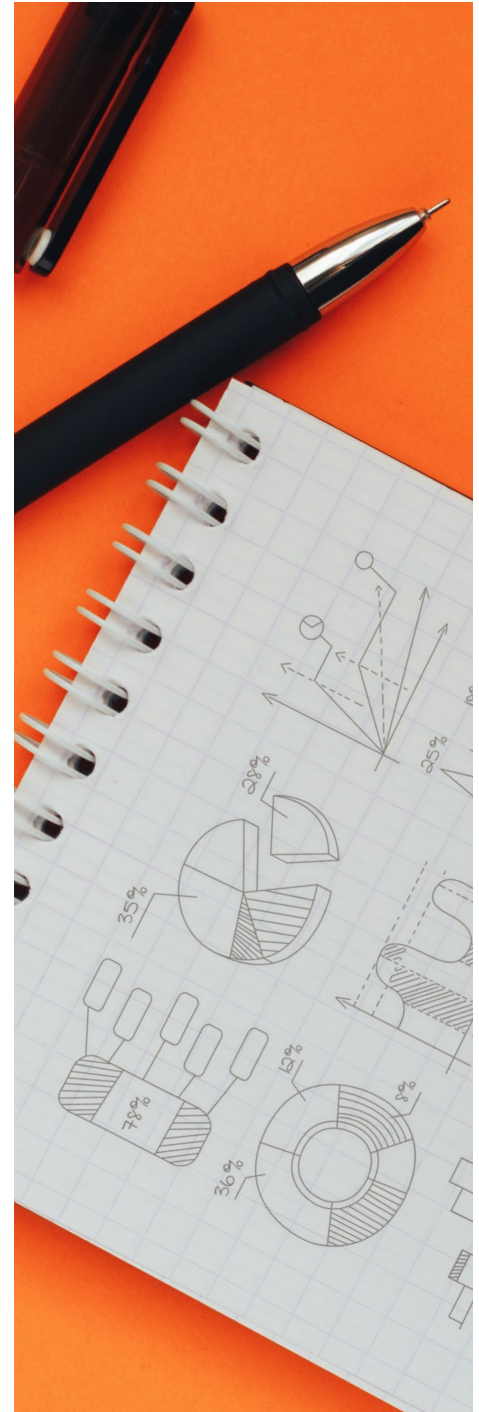
# CHAPTER 1

## A DATA BREACH CAN COST YOU DEARLY

Obviously, cybersecurity is no longer the exclusive domain of your IT department. In fact, data and system integrity as well as risk mitigation should be near the top of every CFO's list of things that keep them up at night, particularly in light of the mounting financial costs of a data breach. When factoring in the additional toll a breach has on brand reputation and loyalty, the stakes are simply too high not to take cybersecurity seriously or delay the implementation of impactful technologies wherever appropriate. Many small and medium-sized businesses do not survive a breach, and if they do, significant work and money towards improving brand reputation is required. Still need convincing on the escalating need for airtight cybersecurity solutions? These foreboding statistics should do the trick:

 <p>On average, enterprises with comprehensive security in place saw no more than a 3% drop in stock price, fully rebounding within 4 months of a breach.</p>	 <p>Firms with insufficient data security dropped as much as 7% after a breach and had yet to fully recover within 4 months.</p>	 <p><b>\$3.62M</b></p> <p>The average data breach costs enterprises \$3.62 million, according to the 2018 Cost of a Data Breach Study from Ponemon Institute.</p>
 <p>Over 70% of IT departments consider brand protection outside of their responsibilities, leaving those concerns for other harrowed departments within the enterprise. With privacy and data protection legislation being launched within the United States and around the globe, such as the EU's General Data Protection Regulation (GDPR), the cost of a data breach affects all parts of your business because most of the legislation is following the consumer.</p>		

However, it's not all statistical doom and gloom when it comes to data breaches. While many CFOs have viewed investments in IT security infrastructure as sunk costs, technology has evolved to the point where such expenditures are now growth drivers as well as security solutions. **In fact, investments in identity and security management can save as much as 40% of total technology costs, while also enhancing employee efficiency and productivity.** Of course, not all technologies and innovations are created equally, so relying on trusted digital finance experts can be like someone handing you a powerful flashlight in a pitch-black room.



# CHAPTER 2

## THE GOOD STUFF: IT & SECURITY TEAMS CAN PROVIDE A POWERFUL DEFENSE

There's no point reading this simply to terrify yourself over the inevitability of a data breach. So, on that note, we offer you some useful best practices that can help you form a powerful cybersecurity defense, beginning with your IT and security teams, and individual employees throughout all levels of your enterprise. After all, comprehensive, effective cybersecurity is the epitome of a team effort; getting everyone involved is an essential first step. That said, accounting and finance executives must educate their people on the following items on a continual basis, ensuring they are always at the forefront of the dynamic, ever-evolving cybersecurity landscape:

- **Always train and retrain team members on identifying any suspicious activity.**  
Employees play a critical role in the overall security of an organization. Most of the security events experienced by companies every year are indirectly caused by a lack of broad internal awareness and understanding of good security practices.
- **Identify, isolate, and protect the enterprise's most sensitive data.**  
What is the absolute crown jewel of your data? How is it affected by compliance regulations? But always keep in mind that compliance is an outcome of good security measures.
- **Don't suck at patching.**  
Immediately implement security patches when they are available to minimize vulnerability. It is one of the easiest ways to protect your business, as well as one of the easiest ways for threat actors to gain access into your organization.
- **Use encryption to protect both data throughout and storage.**
- **Monitor and actively manage access to any cloud services.**
- **Implement digital security measures.**  
Firewalls, malware protection, and system intrusion detection build a digital moat around your environment.
- **Ensure that you have a corporate policy concerning bring-your-own-devices (BYOD).**  
Evaluate whether or not the financial cost savings and convenience outweigh your cybersecurity risk. Implementing the right controls is essential. It's all about transparency. Educate individuals on security best practices, such as strong passwords, multifactor authentication, and the types of data that should be stored on personal devices. These practices will ensure basic security competency and help build a secure culture within your organization.
- **Mandate a signed acknowledgment of security policies and procedures.**  
Regularly test the organization on those policies to ensure a thorough understanding of the material and the stakes at hand.

If any of this elicits the reaction of "This sounds great but where do I start?" having a security-as-a-service (SECaaS) partner can come into play here. Extend your security team without having to build your own, purchase the necessary technology tools, or employ personnel to monitor and respond to incidents 24/7/365.

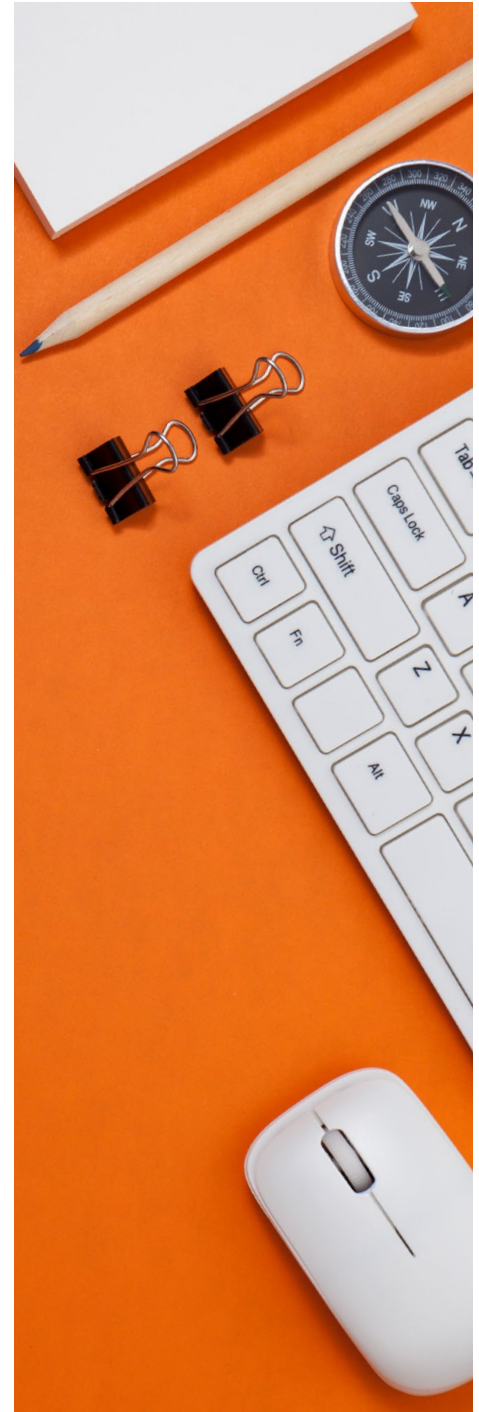
# CHAPTER 3

## MORE GOOD STUFF: HOW CFOs CAN MITIGATE CYBER RISK

Needless to say, leadership plays a crucial role in an organization's cybersecurity effectiveness. While the previous best practices apply in general to accounting and finance executives within an enterprise, the following tips are especially pertinent to CFOs as they view security as a source of added value.



- **Fully understand the risk:**  
Understand the differences between a security risk and a business risk intimately. While we're not suggesting CFOs speak the technical language of risk management in the digital environment, understanding and calculating the possible impact to your assets and reputation—as well as the different types of vulnerabilities and attackers on the prowl—will reveal the severity of the issue and provide sufficient motivation to act accordingly.
- **Communication and coordination:**  
CFOs are equal parts quarterback and offensive coordinator within an enterprise. Their view from the top allows them to see deficiencies and surpluses among all business units, reallocating talent and resources to maximize a security-focused strategy across multiple departments.
- **Cybersecurity budgeting:**  
A CFO's biggest power is holding the purse strings. Mastering the first two bullets will help CFOs effectively allocate the enterprise's resources to build a dynamic cybersecurity environment with risk mitigation in mind.





# PART 2

## EFFECTIVE INTERNAL AUDIT PROCEDURES



We've spoken about how accounting and financial executives can ill-afford to overlook cybersecurity as a serious component of 2019 planning. Now it's time to look at the critical role internal auditors play in preserving data and system integrity and recognize that they are integral to a comprehensive approach to cybersecurity.

That's because there are threat actors around every corner. They won't hesitate to black hat their way into vital corporate systems and get their hands on sensitive information. Not great for companies doing everything they can to develop and maintain a competitive advantage in a crowded, sometimes contentious, marketplace.

In our highly digitized world, cybersecurity isn't just another job for IT. It should be an additional area covered in your audit process. While internal auditors are not on the front lines of cybersecurity, their diligence play a pivotal role in keeping the organization out of harm's way.

# CHAPTER 4

## A PHALANX ON THE DIGITAL FRONT

Before we launch into a slew of extremely beneficial best practices, let's first take a step back and make sure we're all on the same page. In this context, we're defining cybersecurity as business functions and digital tools used to protect networks, computers, programs, and data from damage or unauthorized access.

Yes, that's a mouthful but, given the consequences involved, cybersecurity must be incorporated into the systems and procedures you analyze over the course of an internal audit. In other words, that definition should be taken to heart to fully understand the scope of the problem, the role you play as a component of a strong cybersecurity posture, and the tools you use to protect your environments.

Granted, no one expects you to deploy advanced antihacker tactics during your next audit but, quite honestly, that isn't why you play such a pivotal part in the cybersecurity equation to begin with. Instead, it's your acute awareness of your organization, its systems and processes that make you such a valuable weapon against theft of sensitive data.

In fact, it's the following roles, and your diligent attention and authentic desire to do right by your organization that put you in a position of importance in the ongoing battle for cybersecurity in an insecure environment:



**Protection:** It's a complicated security world. As an internal auditor, you're charged with testing and reviewing everything from BYOD policies to the security protocols in third-party contracts. Your efforts complement with effective IT governance to protect your organization as well as its data, customers, and employees.



**Detection:** Advanced data analytics and associated technologies are quickly becoming a routine part of an auditor's toolbox. Use such tools as a means of closely monitoring systems for even a hint of data security going sideways.



**Response:** When security teams only include protection and detection in their cybersecurity program, incident response (IR) often becomes a one-off solution or doesn't occur at all. When organizations treat IR separately, they inevitably introduce an additional gap or delay that consequently extends a threat actor's window of opportunity to steal critical data. As an auditor, it's imperative to ensure every aspect of a cybersecurity program is taken into consideration to provide the best defense possible.



**Continuity:** Prepare for the worst and then take measures to prevent it from ever happening. Internal auditors and security managers must ensure an organization has an adequate business continuity and disaster recovery (BC/DR) plan in place that accounts for all foreseeable risk scenarios to safeguard operations in the event of a security incident. The key to a successful BC/DR plan is to build relationships and trust across the business and among teams. This ensures that if systems go down everyone knows the plan and can effortlessly execute and address issues as quickly as possible.



**Communications:** Crisis communications play a pivotal role in mitigating the effects of a security event relative to a company's customers, shareholders, and brand reputation. Auditors can greatly assist in developing communication strategies and providing assurance checks of a communication plan's effectiveness and immediacy.







**Improvement:** Given an auditor's wide-ranging perspective on a company's operations and systems, he or she can contribute unique insights into the ongoing effectiveness of an overarching security strategy, making sure it evolves over time and continuously improves.

# CHAPTER 5

## DILIGENCE AND FOCUS ON PRIORITIES CAN'T LOSE

As discussed, internal auditors possess a singularly comprehensive view of an organization's overall well-being. Like every other aspect of a thorough audit, a careful examination of a company's security protocols requires open eyes and the underlying desire to keep the organization free from the potentially devastating effects of a security event. Along with vigilance and a meticulous approach, keep these factors in mind to gain the most benefit from your next audit:

	<p><b>Risk is in the eye of the beholder</b></p> <p>Don't waste your limited time and resources on threats and vulnerabilities that aren't risks to your organization's data and systems. Avoid prioritizing compliance over risk and only act upon those threats and security gaps that pose a substantive risk to an information asset when exploited. Don't needlessly dilute your efforts.</p>
	<p><b>People will always be the most effective defense</b></p> <p>In an industry inundated with a constant stream of technological security marvels—firewalls, encryption, malware protection suites, among many others—it's easy to lose sight of a company's most powerful line of defense. Emphasize investment in your people, increasing security awareness within your team on an ongoing basis. As useful as innovation can be at helping your company in the fight, a workforce continually educated on the evolving cybersecurity landscape will always be your most formidable ally. Your people are the moat around the castle and must be treated as such.</p>
	<p><b>Assemble and maintain a game plan</b></p> <p>Historically, if you were to ask most CFOs about cybersecurity, they would respond with a quick "sorry, not my department." However, the numbers don't lie (See Part 1). CFOs should be well aware of cybersecurity risks and the cost of a data breach. In the event of an active, real threat to your digital assets, an effective BC/DR plan must be in place to mitigate both the damage and consequences. As the internal auditor, you must determine if crisis management protocols and your company's communication plan can adequately enable business continuity if a breach occurs. Likewise, the organization must implement the proper tools to continuously monitor and detect any intrusions and, thus, maintain a vigilant digital eye continuously scanning for data breaches.</p>
	<p><b>Develop agile, scalable security strategies</b></p> <p>Methods of attack change daily, always staying a step ahead of common knowledge. Simply put, today's most effective security solutions are likely to be severely outdated in the very near future if they don't evolve in lockstep with the threats. Because of this, SMBs that run with significantly less budget and resources than enterprises, often need security-as-a-service (SECaaS) vendors. These third-party providers can help optimize a business' cybersecurity resources to help reduce excessive spend on tools and talent, while keeping the latest threats at bay. Internal auditors must gauge if security strategies and solutions are both sufficiently agile and scalable to keep up with an extraordinarily dynamic risk environment.</p>

# CHAPTER 6

## A CAUTIONARY TALE

To demonstrate the absolute need for a sound, evolving set of security protocols, you don't have to search further than news headlines for a sobering cautionary tale. Not so long ago, JPMorgan Chase, the nation's largest bank and global financial titan, fell prey to the black hats of the world, absorbing the repercussions for years afterward while standing on already shaky customer confidence ground.

Although initial estimates of the 2014 security event stated the hackers compromised roughly 1 million accounts, the actual numbers dwarfed those early figures from the bank. All told, over 76 million household accounts and 7 million business accounts were compromised in the attack, placing it among the most extensive cyber intrusions ever.

Perhaps even more foreboding, the threat actors were able to swipe a list of the many applications and programs that ran on the bank's systems which, unfortunately, the hackers could use to map out system vulnerabilities. Those vulnerabilities could very well provide entry points back into the system even years after the initial attack, meaning the hackers could possibly still regain access after JPMorgan repaired all of the known security vulnerabilities. Not good.

This is also a prime example that demonstrates that just because a business meets compliance regulations doesn't mean they are secure. This misperception is giving everyone involved a false sense of security because they checked all the boxes at the end of a laborious regulatory compliance endeavor. Considering that compliance is only meant to set the minimum bar for security, it shouldn't be a company's ultimate goal.



### THE MANY CYBERSECURITY HATS OF AN INTERNAL AUDITOR CHECKLIST

- **Protection:**  
Test and review everything from BYOD policies to the security protocols in third-party contracts to protect your organization data, customers, and employees.
- **Detection:**  
Use advanced data analytics and associated technologies as a means of closely monitoring systems for even a hint of data security going sideways.
- **Response:**  
Ensure every aspect of a cybersecurity program is taken into consideration to provide the best defense possible during IR.
- **Continuity:**  
Build relationships and trust across the business and among teams to ensure an organization has an adequate BC/DR plan in place.
- **Communications:**  
Assist in developing communication strategies and providing assurance checks of a crisis communication plan's effectiveness and immediacy.
- **Improvement:**  
Contribute unique insights into the ongoing effectiveness of an overarching security strategy, making sure it evolves over time and continuously improves.

# CONCLUSION

## HOW WE CAN HELP YOU

Accounting and finance executives; as overwhelming as some of this might sound, a deliberate and organized approach to your enterprise's cybersecurity procedures and practices will go a long way in protecting operations, stakeholders, and everyone else involved. First and foremost, adopt a structured and measured strategy in your cybersecurity, particularly with respect to your internal controls, and build your environment around it.

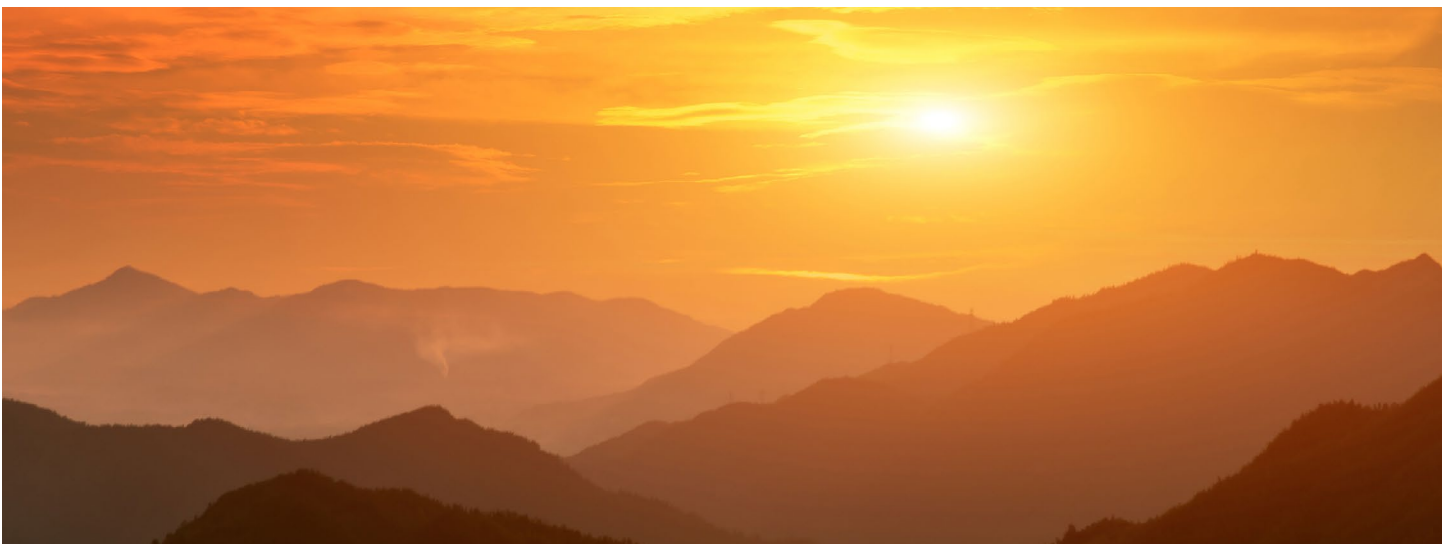
It also doesn't hurt to find a preferred partner like Armor, the market leader in cybersecurity solutions. Armor brings simple security-as-a-service to your IT environment— whether it is on premise, in the cloud, or both—in just a couple of minutes. We know security is complicated, but we can help it make simple, so you can devote assets and resources to the core of your business.

Still not convinced? Well, Armor also provides 24/7/365 access to time-tested security expertise—integrated global threat intelligence gathered from over 1,200 client environments—and is powered by our cloud security platform, the industry's first threat prevention and response platform for cloud workloads and hybrid IT. Not to mention, it has a proven ROI of 286%.

Additionally, Embark can be an especially powerful ally in the process as well, helping you make sure your data is both correct and protected before it ever touches your IT environment.

In fact, Embark can provide you with a wide variety of assistance as you construct and maintain an effective security strategy. Specifically, Embark experts can roll up their sleeves and help by:

- **Performing a readiness assessment**
- **Assisting in developing program details**
- **Identifying Emergency Response Team (ERT) vendors to fit with your specific needs and goals**
- **Making recommendations for a program management process**





[ARMOR.COM](https://armor.com) | (US) +1 844 682 2858 | (UK) +44 800 500 3167

19010204 Copyright © 2019. Armor, Inc., All rights reserved.