ARMOR

BETWEEN YOU AND THE THREAT

Take back the initiative

IT'S TIME TO FOCUS ON OUTCOMES. NOT TOOLS. | CEO VANTAGE POINT

CHRIS DRAKE | **FOUNDER & CEO | ARMOR**

A prologue: defending the chocolate makers

Imagine any successful enterprise or business — large, small, domestic or international. Regardless of their region, industry or revenue, these organizations store, process, manage or use sensitive data workloads. From online retailers and financial institutions to banks and consumer food chains, the majority of companies are now tasked with defending their data.

Should the organization fail, they're responsible. Not their IaaS provider. Not their hardware suppliers. Not their intelligence experts. Not their forensic vendors. It's on them.

On the surface, this responsibility sounds reasonable — and to a point, it is. But visualize the multitude of companies that operate globally. Shoe manufacturers. HVAC suppliers. Healthcare organizations. Online retailers. Restaurant chains. And even chocolate makers.

Yes, chocolate makers.

A global chocolate brand recently stated how much of a burden it was — on their business, resources and budget — to deploy the necessary security safeguards and technology to properly defend their company and customer data.

Instead of focusing on their core chocolate business, they were dedicating massive dollars and significant resources to hire cybersecurity specialists, procure technology hardware and assemble a full-time security operations center.

All this energy being spent by … a chocolate maker. Something has to change. Something has.

"Should the organization fail, they're responsible. Not their IaaS provider. Not their hardware suppliers. Not their intelligence experts. Not their forensic vendors. It's on them."

A fragmented security paradigm

Never before in the history of the tech industry has a "solution" put as much burden on the customer's shoulders to gain the promise they were expecting — especially at such high costs.

Roughly $100 billion is spent on cybersecurity each year and the data breaches are increasing in both frequency and cost. Organizations cannot buy their way out of this problem. Many have tried and failed.

For years, customers have been sold on the idea that technology will protect them. The industry conveniently omits the investment, complexity and commitment necessary to properly implement even a single point solution — much less integrating all the necessary tools, processes and controls required for a complete security strategy.

Building a sound, secure environment takes true cybersecurity professionals and fine-tuned processes.

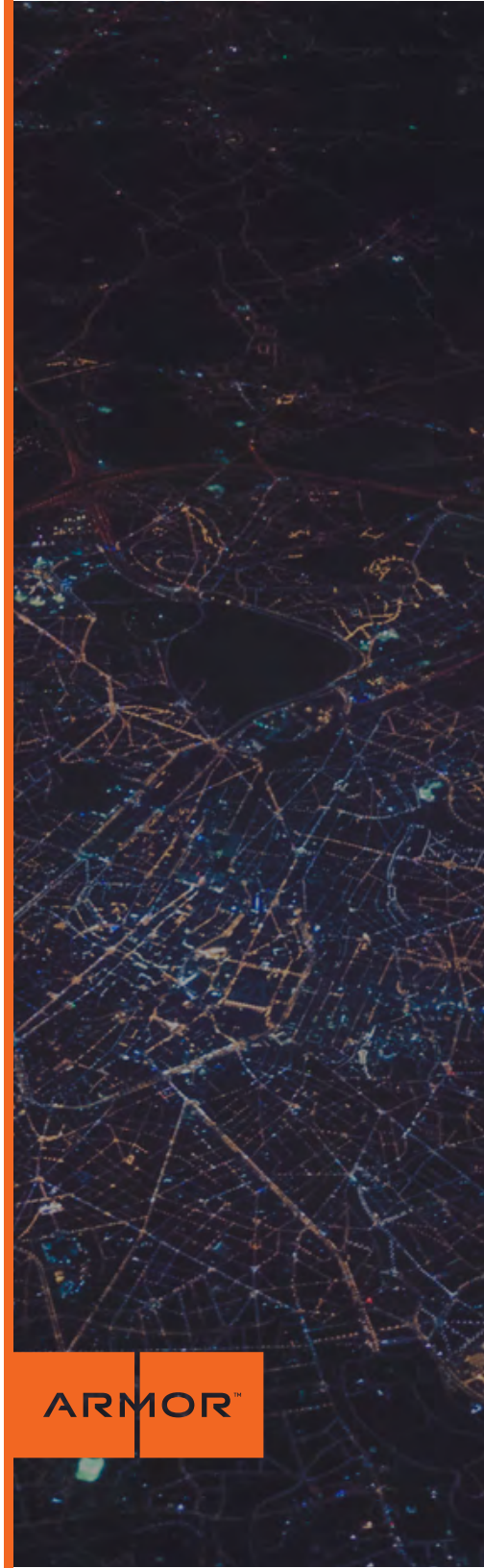
Despite evidence to the contrary, organizations continue to believe these promises. But threats are simply too advanced. Malicious criminal groups are cycles ahead of the organizations trying to leverage this technology to stop them. But it's not their fault. It's the only way these organizations have ever known.

To be clear, this trend is not because of a lack of innovation or technology (although there are still many opportunities to improve the technology used to defeat threat actors). The root cause stems from a wide talent and expertise gap. In fact, by one estimation the U.S. alone is short some 200,000 cybersecurity professionals.

Even if a single enterprise sought to invest in closing the talent gap, they'd have to pay top dollar to lure them away from existing firms.

Organizations have doubled the number of full-time security employees since 2011, but this growth still pales in comparison to the overall IT headcount and there's no way to currently evaluate the quality of these hires. And, as expected, the meager bump has had no effect on stopping threats.

> "By modest estimates, more than 209,000 cybersecurity jobs in the U.S. are unfilled, and postings are up 74 percent over the past five years."
>
> PBS NEWSHOUR



1. With more than 200,000 unfilled jobs, colleges push cybersecurity," Kirk Carapezza, PBS NewsHour, January, 22, 2015

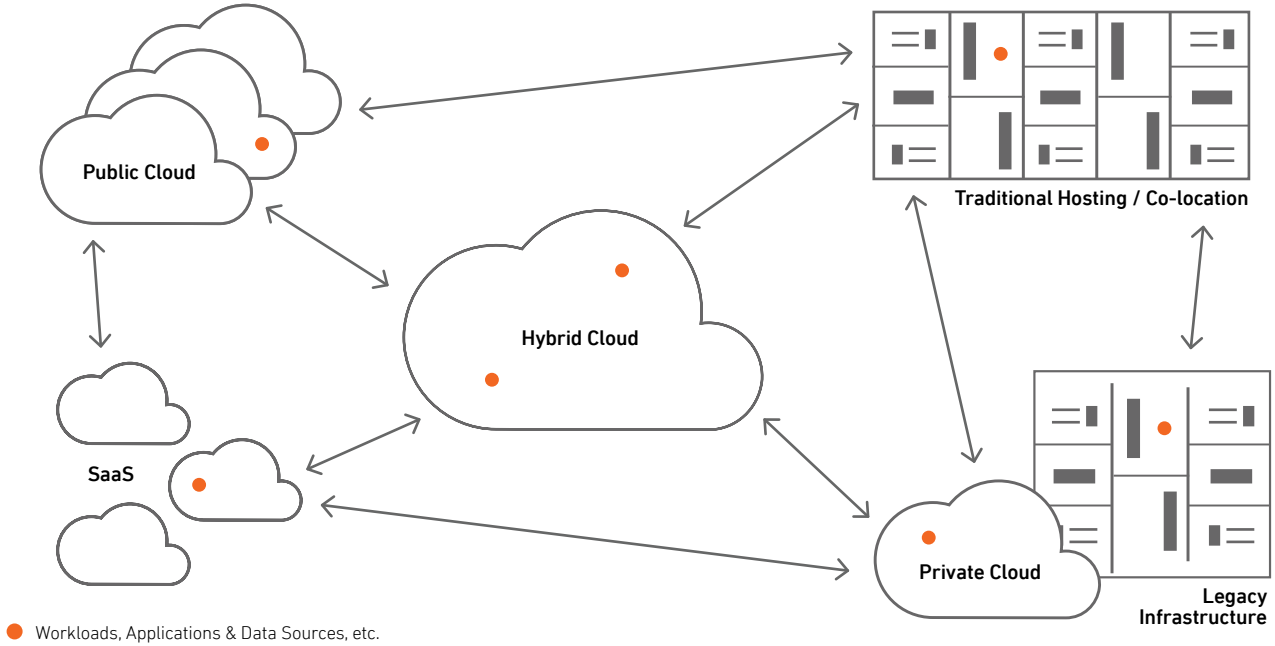
The mystery of responsibility

Enterprises neither want to be in the security business nor can they afford to deviate from their core business in the current global economy. But when they do attempt to solve this massive challenge in-house, roles and responsibilities are shrouded in confusion.

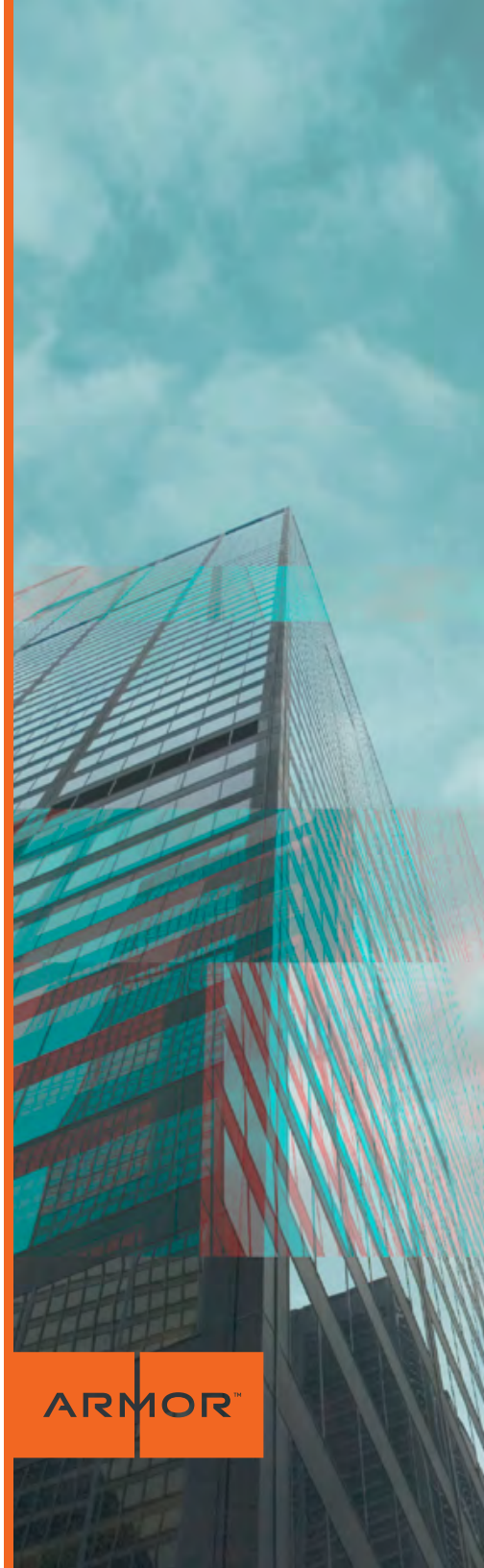
The variety of infrastructure deployment options creates significant complexity. Even once a commitment to security is made, data is classified and a strategy is created, the chore of actually executing it is overwhelming.

Do they deploy to a public cloud? Mix in a dedicated server? Augment some responsibilities to a co-location provider? What about the legacy infrastructure? Mix and match it all with a hybrid cloud approach?

A Security Complex



Executives and IT directors are tasked with integrating and securing a variety of environments.



It's a very tangible challenge C-level executives and IT directors face every day — and this is assuming these roles and responsibilities have even been defined.

Unfortunately, who is responsible for what is often a mystery. According to an exclusive Ponemon study, 42 percent of IT decision-makers say their organization's security operations team are "rarely" involved in evaluating cloud service providers. That's a critical, industry-wide problem.

"While organizations believe security and compliance are important, they clearly are not taking steps that are best handled by IT and IT security to ensure confidential and sensitive data in the cloud is secure," noted the study. "Instead, they are mostly dependent upon the cloud provider or end user to achieve these objectives."

Yet market conditions have left them with few options. And because they were forced into this predicament there is growing tension — and even mistrust — between customers and point security vendors (and even between the different security companies).

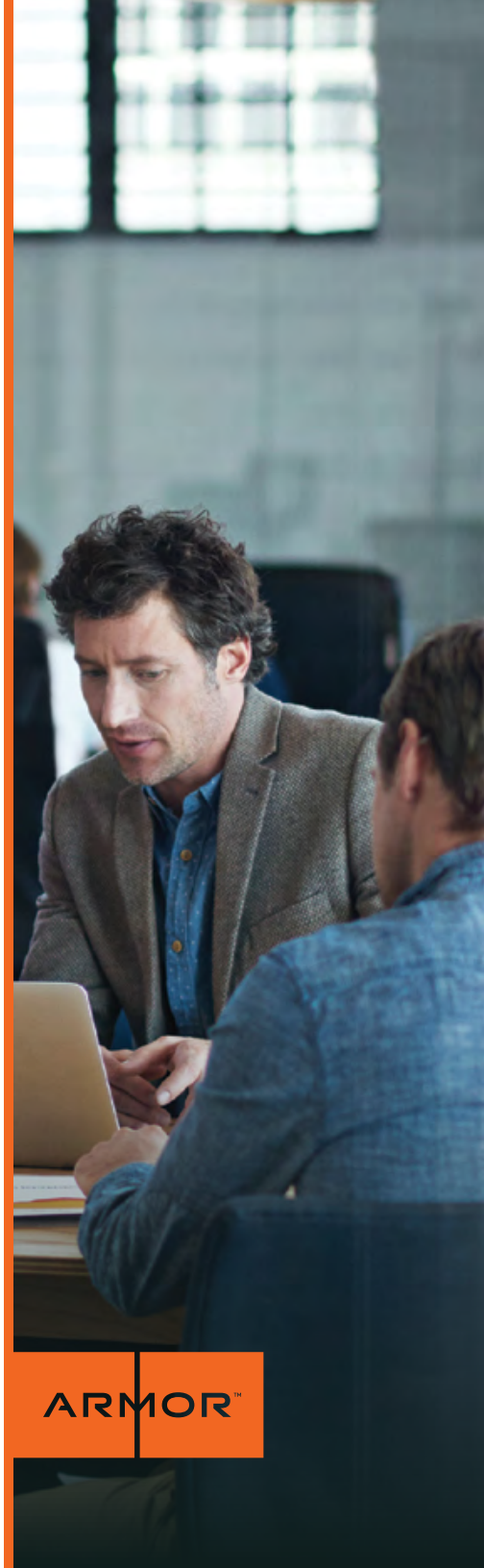
Regardless of trends or current behavior, customers want to be able to focus on their core business. Again, they all strive to find just a single unique security expert that will share responsibilities and defend their organization at all costs.

That's it. A true risk partner.

Spend Cycle

To date, organizations globally are spending $100 billion annually on cybersecurity tools and services — and still losing the war. That figure is projected to jump to $170 billion by 2020.

But history has proven that spending doesn't equal safe outcomes.



2. "Cloud Security: Getting It Right," Ponemon Institute (sponsored by Armor), July 2015.

A market of tools, but not technique

So, let's apply the assumption that the C-suite, board of directors, stakeholders and necessary business decision-makers have aligned to make enterprise-wide security a priority. This is a major achievement, but only part of what's required to significantly defend an organization and its critical data workloads.

The investment and commitment — not just in technology, but human resources — to build a truly secure environment can be overwhelming.

The market is saturated with tools. Organizations remain bombarded by hundreds of security vendors offering one-dimensional point solutions. Others, such as commodity cloud or infrastructure-as-a-service providers, are bolting on security features in attempts to get a slice of that growing market.

The end organization is on its own to integrate and manage all this technology within their environment — all without a single security gap.

NAVIGATING THE SECURITY MARKET

SECURITY LAYER	FEATURE/FUNCTIONALITY	# OF VENDORS FOR TOP SECURITY TOOLS
PERIMETER	IP Reputation Filtering	4
	DDoS Mitigation	8
	Web Application Firewall	16
NETWORK	Segmentation	People & Process
	Firewall	16
	Vulnerability Scanning	18
	Secure Remote Access	17
	Encryption in Transit	People & Process
	Intrusion Detection	10
SERVER / OS	Hardened Operating System	People & Process
	OS Patching	People & Process
	AV / AM / Adv. Threat Detection	18
	Log Management	15
	Time Synchronization	People & Process
	File Integrity Monitoring	8
	Encryption	8
	DLP	13
	Configuration Management	People & Process
	Host Intrusion Detection	10
VIRTUAL MANAGEMENT	Hardened Hypervisor	People & Process
	Isolated Management	People & Process
SECURITY OPERATIONS	Privileged Access Management	22
	Security Monitoring (SIEM)	People & Process
	Threat Intelligence	People & Process
	Incident Management	People & Process
	Security Device Management	People & Process
	Certified Ethical Hacking	People & Process
	Security Architecture	People & Process
	Vulnerability Management	People & Process

Vendors develop competencies and tools that are most valuable and beneficial when paired with those in the cybersecurity trade (i.e., not their normal customer).

In most cases, customers have already invested in much of this technology. Options are so numerous — all promising security — that the very term becomes more and more diluted.

And while tools are necessary components of the greater security view, they absolutely must be aligned with properly trained security professionals and tested processes.

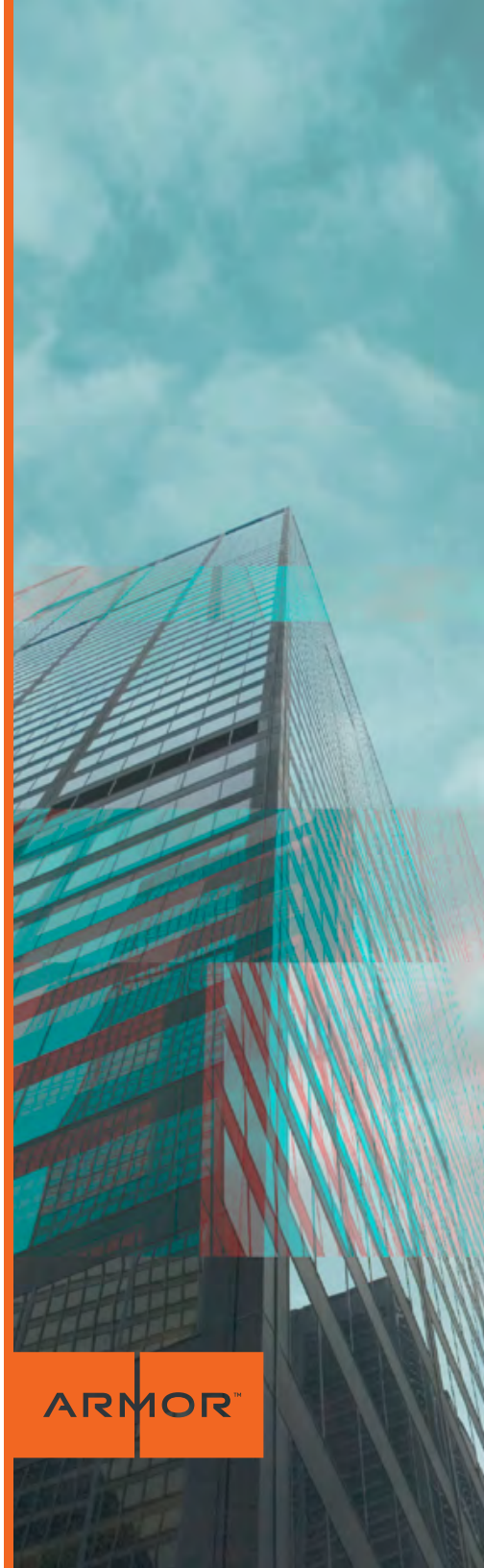
What makes security so challenging is the need to constantly monitor and maintain those security controls and technology to take into account new vulnerabilities, threats, attack vectors and other aspects of the constantly changing security environment. And this is only attainable via tried and true processes.

Ask the chocolate maker. It's illogical to demand that each and every organization become cybersecurity experts. Corporations and security-conscious organizations desperately require security outcomes — and someone to share risk and responsibility.

Pairing Talent & Technology with Technique

Even when the commitment to security is made, the arduous task of pairing technology with true cybersecurity professionals is overwhelming. In the end, customers are left with three major objectives to realize a true, effective security posture for their environments.

- **Collect Tech**
  Procuring, integrating and managing security tools is expensive and time-consuming for organizations.
- **Find Talent**
  Recruiting, hiring and keeping the required cybersecurity professionals is incredibly expensive.
- **Build Processes & Techniques**
  Pairing technology and talent to threat intelligence, defense and related underlying systems is a major undertaking; if executed improperly, this likely leads to critical vulnerabilities for threat actors to exploit.



Fight for your customers

We were always going to come upon this crossroad: an intersection between hands-off security vendors, commodity cloud players and forced DIYers.

With faceless technology at the end of each path, none of these choices were optimal for organizations under more and more attacks. And unrelenting scrutiny.

Each cybersecurity company — from the CEO and CSO to the network engineers and threat analysts — should take it as a challenge to offer customers more. And in the processes, share more of their burdens, too.

It's a call to arms to ignite a much-needed shift in how cybersecurity experts serve customers. I will stand between you and the threats that target what you worked so diligently to build. It's yours. Not theirs. And we'll work tirelessly defending it with you.

IT'S NOW ABOUT OUTCOMES.
AND IT ONLY COMES FROM ARMOR.

"I will stand between you and the threats that target what you worked diligently to build. It's yours. Not theirs. And we'll work tirelessly defending it with you."

CHRIS DRAKE
FOUNDER & CEO | ARMOR

About Chris Drake

As the founder and CEO of Armor, Chris Drake oversees the growth, direction and innovation of the company's advanced cyber defense solutions and managed secure cloud infrastructures. He fights the status quo every day and ensures that the "smart creatives" at Armor are protected for the benefit of its customers. He understands and accepts the awesome responsibility customers have placed in Armor to protect their most sensitive data.

Drake began his career by serving as a paratrooper in the U.S. Army's storied 82nd Airborne Division. While at Fort Bragg, N.C., Drake built some of the U.S. Army's first private secure websites.

After leaving the military, Drake established TargetScope, an interactive marketing and Web development company that oversaw hundreds of websites and applications containing critical data. After hearing of clients getting hacked at other hosting providers, Drake saw a clear need in the market for a truly secure cloud.

In the first few years, Drake led the company to 100 percent growth three years in a row, establishing the company as the industry's leading secure managed cloud provider. He served as the company's CTO in 2014 to help drive its continued innovation and returned to the CEO post in March 2015.

Along the way, Drake became a sought-after speaker and writer on topics surrounding the cloud, security and compliance. He's often quoted in major industry news sites and speaks at leading industry events.

In 2013, he won the Tech Titans Emerging CEO award, which is given to the top chief executive of a successfully emerging business. Drake was acknowledged as one of the top "40 under 40" business leaders by the Dallas Business Journal and received the University of North Texas Distinguished Young Alumni Award. He holds a Bachelor of Business Administration in marketing from the University of North Texas.

US 2360 Campbell Creek Boulevard, Suite 525, Richardson, Texas 75082 | Phone: +1 877 262 3473
UK 268 Bath Road, Slough, Berkshire SL1 4AX | Phone: +44 800 500 3167

ARMOR™
BETWEEN YOU AND THE THREAT