ARMOR™

THE FIRST TOTALLY SECURE CLOUD COMPANY™

‘But I was compliant’

INVESTING IN TOP-DOWN SECURITY TO BUILD A COMPLIANT BUSINESS

Compliance is never enough

Businesses face mounting pressures to protect their data. Attacks are increasingly sophisticated and organized, and the stakes are higher. No longer is the typical hack focused on defacing a website; now, attackers are stealing and selling valuable data in exploits that can do more than just embarrass a company — they can destroy it.

When there's a problem, the human response is to seek a solution. So, the consequence of more breaches is more regulations. This is borne out by an increasing number of regulatory agencies issuing their own requirements; creating an extremely complex web of requirements that businesses are not always sure how to address.

Many of the rules are not overly detailed because regulatory agencies don't want to get mired in having to keep up with new threats and technologies. As such, they provide high-level requirements such as, "ensure the confidentiality, integrity and availability of all (fill in the blank) data and protect it against all reasonably anticipated threats."

At the same time, regulations are written, monitored and enforced in different ways by different regulatory agencies, leaving businesses struggling to understand if they're in compliance.

The challenges are understandable. Taking the path of least resistance is not. No matter the confusion.

It's a story you'll watch unfold time and time again. The breach. The headlines. The confusion. The public apologies. The finger-pointing. And it's often followed by some form of the following:

"But I was compliant."

Compliance does not equal security

While businesses may not fully understand their compliance requirements, they do understand the impact of regulatory fines and damaged reputations. To prevent those pains, organizations tend to focus on ticking off the boxes of a compliance checklist, assuming that if compliance is met, their data must be safe.

But when companies lose sight of the intention behind the regulations — to safeguard sensitive data — and treat compliance itself as the primary objective, gaps are created between their perceived level of security and their actual level of security.

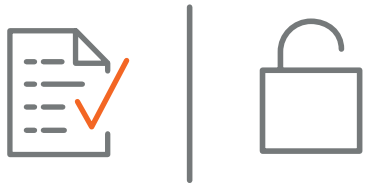
They think they're safe, but they're not.

Consider the number of strong brands that have suffered infamous breaches; most of them had been judged as compliant, but compliance wasn't enough to prevent attacks that cost millions of dollars and immeasurable damage to their reputations.

Since compliance is simply a method to demonstrate how your security program meets a specific set of criteria — at a specific point in time — a better approach is to focus on security first.

If your security program is strong, compliance will be addressed. And it will be done so in a way that supports a healthy business instead of draining resources in the pursuit of tick marks on a checklist.

"... when companies lose sight of the intention behind the regulations — to safeguard sensitive data — and treat compliance itself as the primary objective, gaps are created between their perceived level of security and their actual level of security."



Security is the horse, compliance is the cart

When a company marks the boxes on its compliance checklist and considers its security activities to be complete, it is not only leaving itself open to the loss of intellectual property and business-critical data, it is also building inefficiencies into its security efforts.

A security-first approach is holistic, so everything from the tactical mapping of controls to the strategic planning of its risk management program work in concert. That streamlines security operations, which reduces costs, increases value and produces better results.

Continuous security & compliance

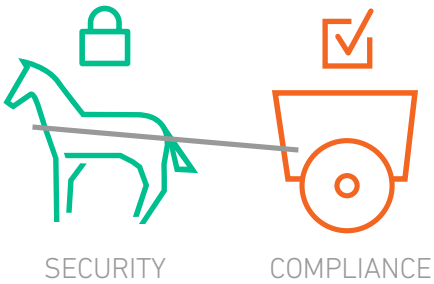
Security and compliance are not static endeavors. You don't, for example, install a firewall and then never revisit the configuration. Likewise, even though compliance is typically measured once a year, it is supposed to be maintained continuously.

Unfortunately, the threat landscape evolves in real time, outpacing updates to regulations and capabilities of security tools. This requires that organizations be constantly vigilant to ensure that their security posture remains strong by keeping their controls current and measuring their compliance on a more frequent basis.

A prime example of the many organizations that don't embrace this approach, a popular U.S.-based home improvement retailer successfully passed compliance assessments but still fell victim to an attack that went undiscovered for six months.

If the company had an effective and current security and compliance program, it would have been continuously updating its controls and monitoring its environment. Its network would have more likely remained stay secure while also meeting regulatory requirements. Such was not the case.

"A security-first approach is holistic, so everything from the tactical mapping of controls to the strategic planning of its risk management program work in concert."

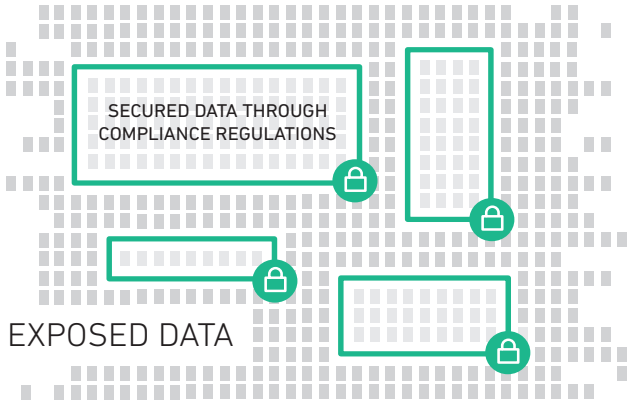


Complete data security

Regulatory requirements protect specific types of data. However, companies own more types of data than what are covered by regulations.

In fact, a business's proprietary research, product strategies and other sensitive data may be its most valuable assets. But companies that rely on regulatory checklists to guide their data protection strategies leave a great deal of that valuable information exposed.

A security-first approach does not segment data solely according to compliance requirements; it also classifies data according to its sensitivity, location, attractiveness to attackers and other factors. The end result is that all of a company's data is protected appropriately, including the data subject to regulations. Compliance is met and the enterprise is safeguarded in its entirety.



Reduced expense

A compliance-first approach leads to the purchase of tools that may or may not be effective in concert with other security efforts.

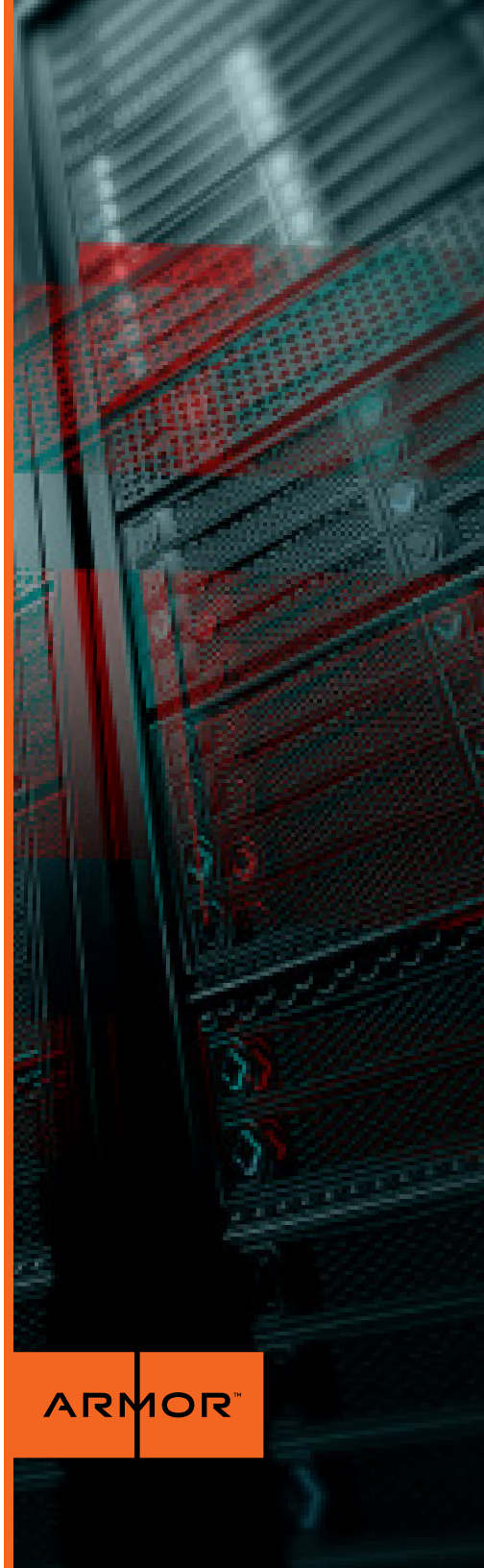
In addition, because there is so much overlap between regulatory standards, companies may make redundant purchases that eat up budget without meaningfully improving security.

Running a patchwork of products raises payroll costs as consultants and specialists are hired to research, select, purchase, implement and manage each new tool. But the worst expense a compliance-first approach can create is the expense of a breach, and the cost of a breach is likely to far exceed the amount that a strong security program would have cost in the first place.

A security-first approach drives a sensible purchasing strategy. Security investments are no longer a jumble of tools purchased to meet a string of standards in one or more regulatory documents; instead, investments are part of a strategic effort that serves a real-world demand beyond the need to avoid fines.

The entire business is protected — not just the areas subject to regulation — and that leads to a greater return on investment.

Relying on regulatory checklists to guide data protection strategies leave a great deal of that valuable information exposed.



Simplified audits

For companies using a security-first approach, demonstrating compliance is a reporting exercise rather than a scavenger hunt. The auditor only has to map the existing documentation of the controls to the regulatory requirements and describe how the requirements were met.

This allows third-party assessors to validate compliance more quickly and be less disruptive to the organization; resulting in reduced hard and soft audit costs.

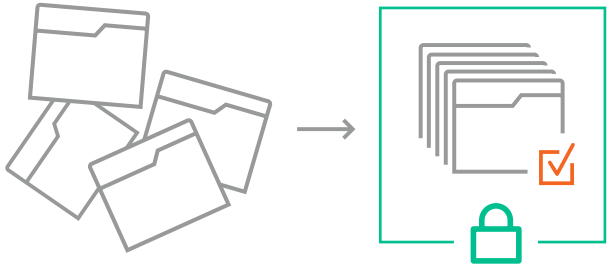
Streamlined management

Managing security in a compliance-first organization shifts authority from those who most need it — the highest level of security personnel in the company — and places it in the hands of the chief compliance officer or the general counsel.

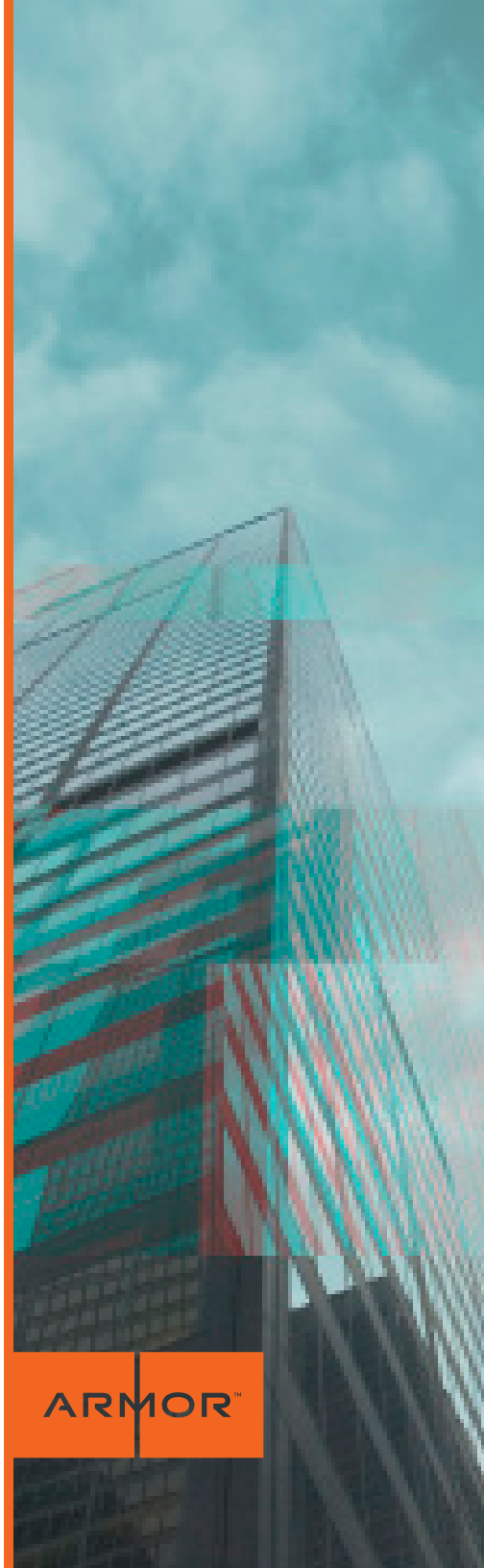
Certainly, the compliance executives need to work closely with the security leaders, but security strategies and investments require the specialized knowledge of a CISO, CSO or security director.

After all, few compliance executives are likely to have the deep level of technical expertise necessary to ask the right questions of a cloud provider or to select the right hypervisor-based network firewall.

In a security-first organization, security managers can keep compliance personnel up to date on purchases and work with them to identify which regulatory requirement is met at the time of purchase. That gives the enterprise a constant and complete understanding of its regulatory status, and audits are no longer a source of disruption and expense.



For companies using a security-first approach, demonstrating compliance is a simple reporting exercise



A checklist is not a defense

There is no instance in which a security-first practice is weaker than a regulatory standard; the security-first approach is shaped by the realities of the threat landscape.

Since threats are constant, monitoring and mitigation are ongoing activities. A company that only reviews its security posture annually is exposed for the other 11 months to any number of threats, while a security-first company proactively monitors its assets continuously and responds to threats immediately.

Since threats are evolving, configuration updates and patches are implemented and managed with diligence in a security-first environment. As new threats arise, the company knows its methods will keep it as secure as possible.

A company that waits until an audit is impending before it verifies its network diagram is consistent with firewall configuration standards or that its patch management program is properly documented creates uncertainty. Patches may be installed without being tested first, and that can crash business-critical systems. In the scramble to meet compliance, a business can do more harm than good and still fail in its goal of marking off a line on the checklist.

Since threats are complex, third-party software and IT vendors are included in a security-first program; regulated companies that don't ask for an Attestation of Compliance (AOC) from their vendors and perform the appropriate due diligence are, in effect, spending money to create risk. A security-first approach includes procedures for onboarding and monitoring vendors so the company doesn't become collateral damage if a vendor is breached.

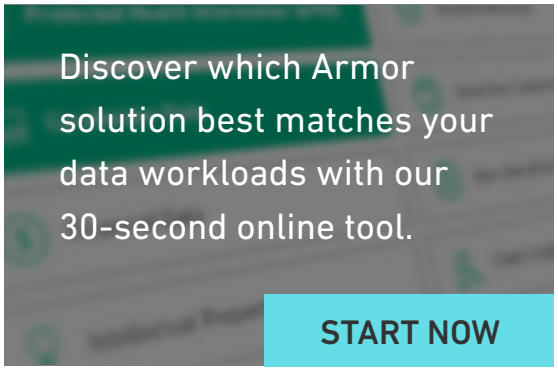
Take a holistic approach to security

Businesses don't exist for the purpose of achieving compliance; they exist to serve their customers and create value for their shareholders.

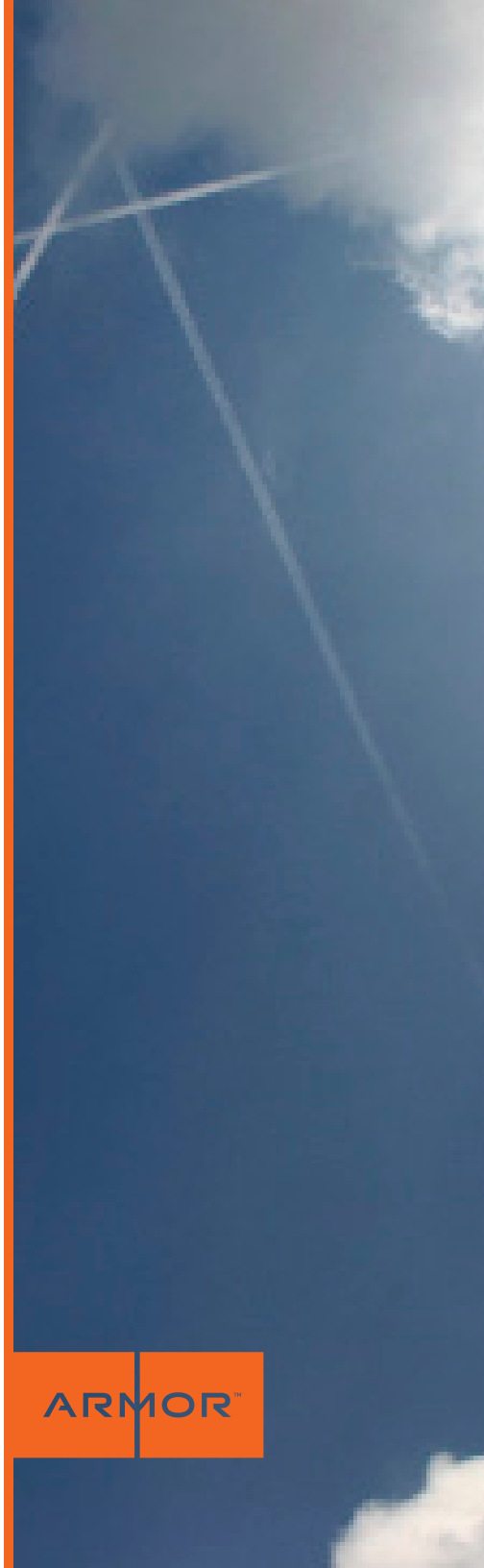
The best way to achieve those objectives, while still meeting regulatory requirements, is to stay focused on the reason behind the rules: to protect sensitive data.

Organizations that look beyond the checklist and take a holistic approach to their security are in the best position to ensure the security of their data and the health of their businesses.

This is the key to leveraging security to build a successful and compliant business.



"A security-first approach drives a sensible purchasing strategy. Security investments are no longer a jumble of tools purchased to meet a string of standards in one or more regulatory documents ..."



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™
THE FIRST TOTALLY SECURE CLOUD COMPANY™