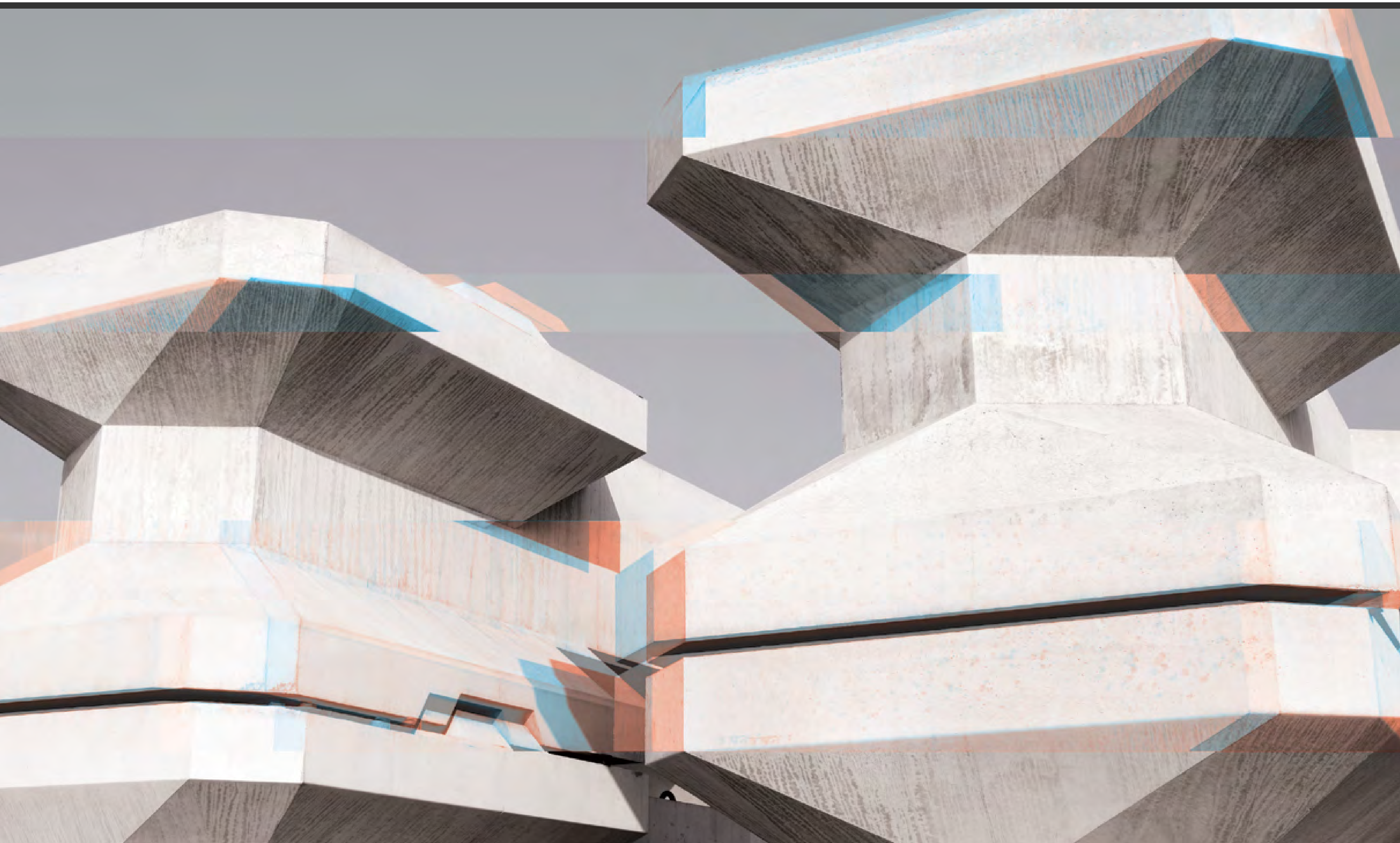
Are you a security-first organization?

FIGHTING THE URGE TO PRIORITIZE COMPLIANCE



Understanding regulatory intent

Industry and government regulations were originally developed to help businesses spot gaps in data security, but for many companies they have the opposite effect. When businesses focus more on avoiding penalties than on developing strong security, vulnerabilities are not prevented — they are created.

Unsurprisingly, some organizations misunderstand the purpose of regulations. These companies view compliance checklists as step-by-step directions for a solid security posture, assuming that if they can complete a checklist, they must be secure.

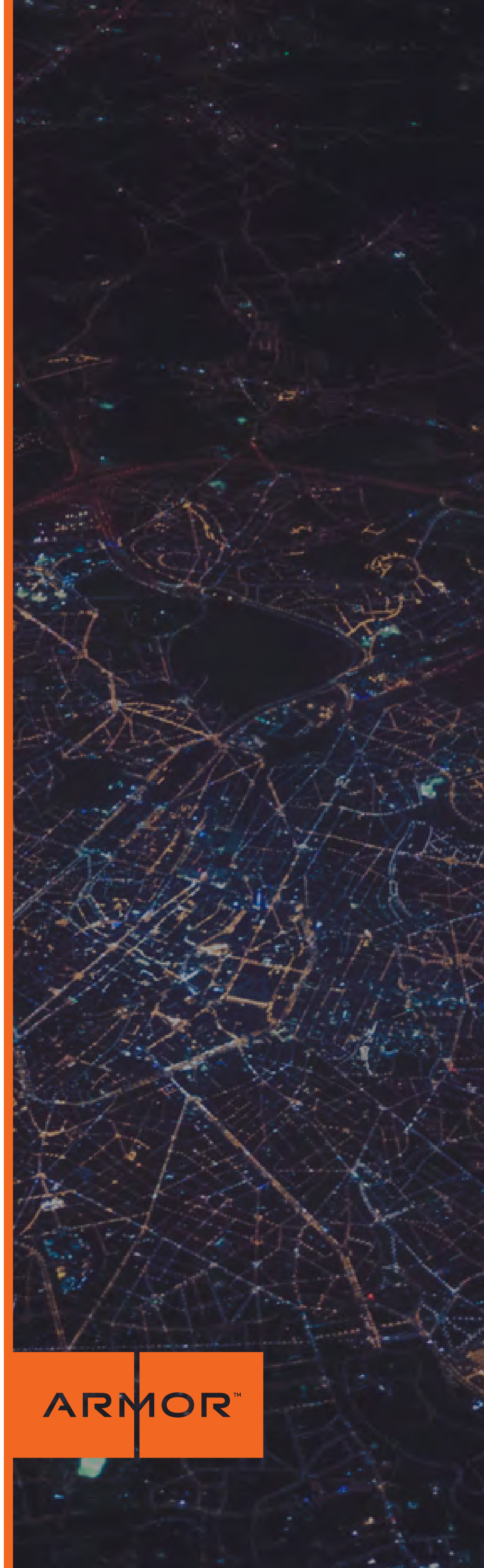
But this is a reverse approach; regulations are not intended to tell businesses how to structure their security efforts, they are intended to be used as a guide against which the chosen security structure can be checked.

While regulations may be perceived as being overly complicated and difficult to comply with, many only require businesses to meet a minimum level of security. Businesses that meet compliance at the minimum level end up spending significant sums of money to achieve the illusion of security rather than real security. And they may not even know it.

The urge to prioritize compliance is understandable; after all, a breach *may* happen, but an audit *will* happen. A focus on avoiding penalties, a misunderstanding of the purpose of regulations and the tendency to meet the bare minimum requirements are all signifiers of a compliance-first approach. None of them deliver real security.

The letter of the law may be followed perfectly, while the spirit of the law — to protect data — is overlooked.

> "... regulations are not intended to tell businesses how to structure their security efforts, they are intended to be used as a guide against which the chosen security structure can be checked."



Security-first in action

A safer approach is to put security first. A security-first approach is built around choosing the right solutions and services with the knowledge that a solid security program will naturally align with regulatory requirements. When security is first, compliance will follow. A look at just a few PCI and HIPAA standards will shed light on the gaps created when compliance is prioritized over security.

1 APPLICATION SECURITY

Relevant to: Companies that use Web applications, cloud services or software-as-a-service (SaaS).

Requirement

PCI DSS Requirement 6.6

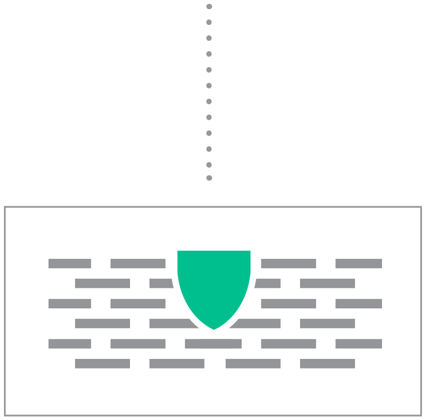
For public-facing Web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods:

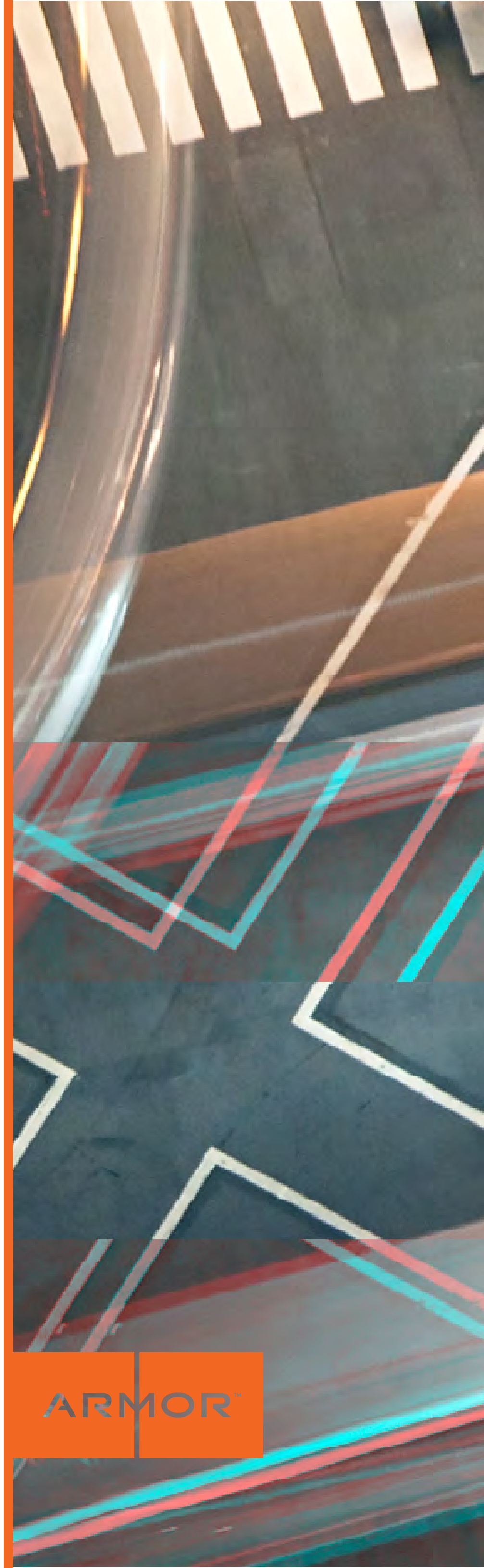
- Reviewing public-facing Web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes.
- Installing an automated technical solution that detects and prevents Web-based attacks (for example, a Web application firewall) in front of public-facing Web applications, to continually check all traffic.

PCI DSS COMPLIANT

Control

Deploy a Web Application Firewall (WAF)





Consequences: Compliance-First

A company geared toward meeting compliance rather than creating truly strong defenses can conduct a manual review of its Web applications once a year and meet compliance.

A business that chooses this minimal option — as many certainly do — is secure at one moment in time each year, and only then if the manual review is conducted meticulously.

Although your company may not have made changes to its Web-facing applications, hackers have been working through the months to crack application defenses, and any third-party vendors involved in the delivery of those apps may have been making changes to their own systems that leave doors open into your systems. A system that is secure on Friday may be breached on Saturday.

Benefits: Security-First

An important component of a security-first approach to securing applications is an automated Web application firewall (WAF), which must be constantly updated to protect against the latest exploits and can also protect against some unknown exploits.

In addition, most WAFs 'learn' to identify attack vectors, block malicious behavior and recommend security policies, but they have to be set up to do those things. Just implementing a WAF may meet requirements, but a WAF that is not properly configured, promptly patched and constantly tuned will deliver neither reliable protection nor a full return on investment (ROI).

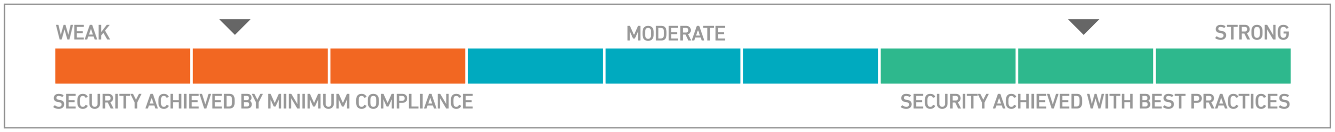
Businesses that receive and transmit personally identifiable information (PII) through their websites, such as online banks and healthcare exchanges, should consider WAFs to be a mandatory component of their security system; otherwise, they are degrading the integrity of their data collection practices. They should also have a plan to configure and maintain their WAFs in a way that delivers the best security and greatest ROI.

Business Objective Served

- Securely leverage data as a business asset

What's at Stake?

- All data accessed via a browser
- All systems that share databases in common with a Web interface



WEAK

MODERATE

STRONG

SECURITY ACHIEVED BY MINIMUM COMPLIANCE

SECURITY ACHIEVED WITH BEST PRACTICES

2 USER AUTHENTICATION

Relevant to: Every company that handles electronic health records.

Requirement

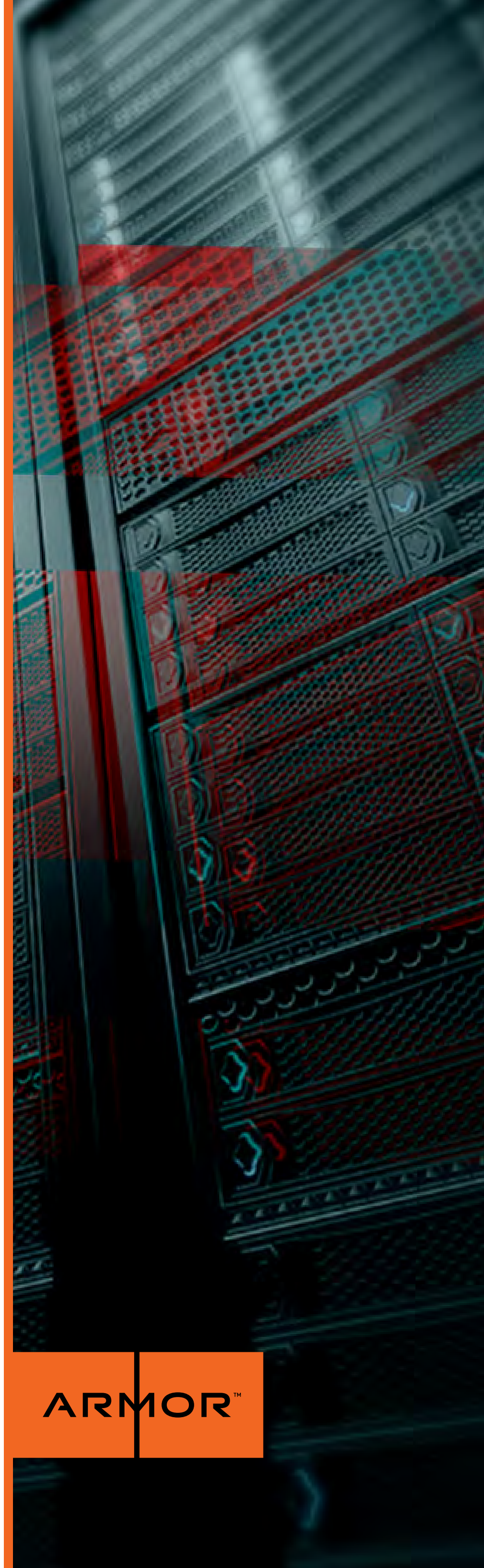
HIPAA/HITECH §164.312(d)

Implement procedures to verify that a person or entity seeking access to electronic protected health information (ePHI) is the one claimed.

HIPAA
COMPLIANCE

Control

Multifactor Authentication



Consequences: Compliance-First

All an organization needs to do to comply with this standard is require a username and password to access protected health records.

But these user credentials alone are not secure; they can be stolen through social engineering or keystroke-logging software, intercepted in transit or hacked by automated software that tries thousands of combinations (e.g., brute force) until the correct password is discovered.

Benefits: Security-First

Most successful compromises come from inside an organization, often via credentials that have been socially engineered without a user's knowledge. If only a username and password are required, however, even an authorized insider can still do damage.

For instance, an administrative user may access records beyond his or her authorization level, either accidentally or maliciously. A security-first approach would require the use of multifactor authentication for access to all sensitive records. Multifactor authentication requires a user to present at least two proofs of identity in the form of something a person knows, like a password; something a person has, like a key card; or something a person is, like a fingerprint.

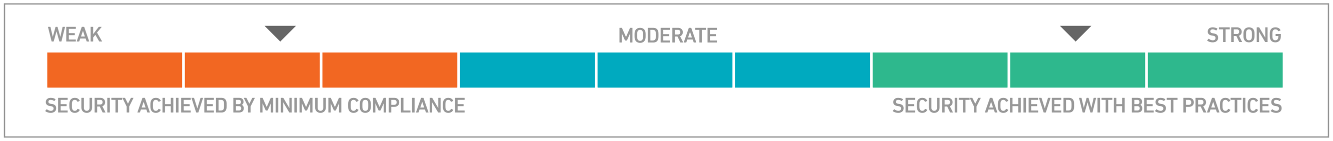
A security-first approach would also notice and alert security analysts when restricted records were accessed by any user at all. In addition to securing the confidential records subject to regulation, multifactor authentication helps prevent corporate espionage, sabotage and the theft of corporate data.

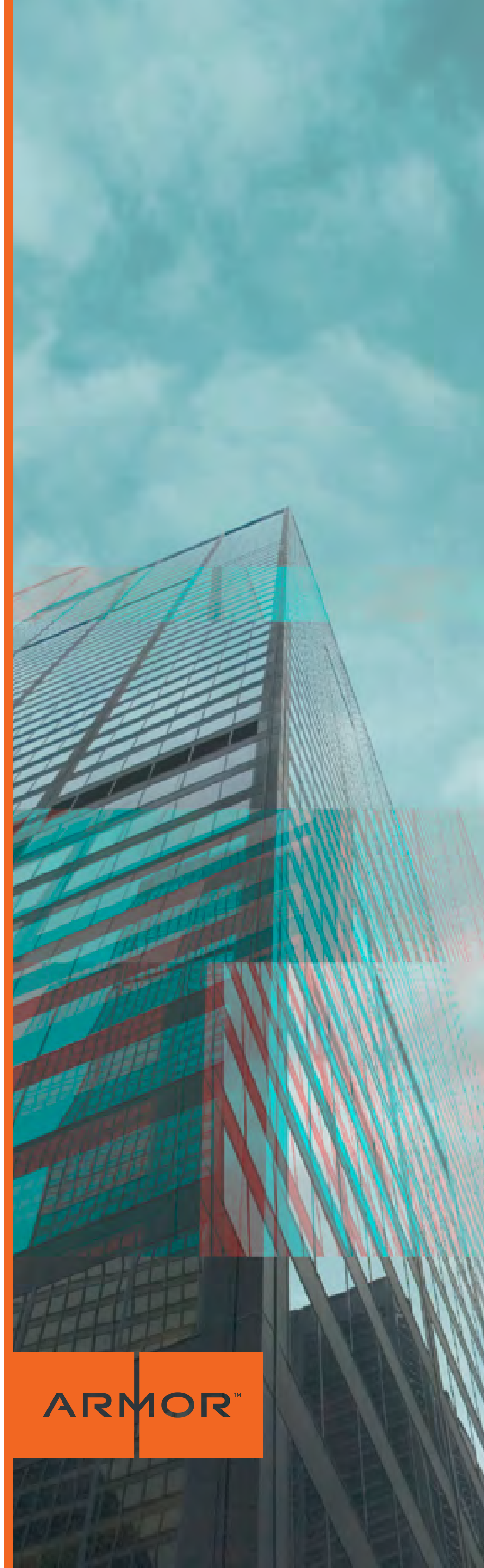
Business Objective Served

- Employ cost-effective controls

What's at Stake?

- Any data accessible to insiders of any authorization level
- Intellectual property
- Corporate secrets


WEAK
MODERATE
STRONG
SECURITY ACHIEVED BY MINIMUM COMPLIANCE
SECURITY ACHIEVED WITH BEST PRACTICES



3 DATA ENCRYPTION

Relevant to: Every company subject to PCI DSS or HIPAA.

Requirement

PCI DSS 3.4.1

If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.

PCI DSS COMPLIANT

Control

Role-Based Encryption

Consequences: Compliance-First

Businesses running operations in the cloud may assume that full-disk encryption (FDE) is a bullet-proof approach to meeting regulatory requirements. FDE encrypts data when it is written to a disk, and the data stays encrypted while the computer is powered down. This is a good approach for laptop security because laptops are usually lost or stolen when they are powered off in transit.

Many storage-area network (SAN) vendors include FDE as part of their solutions, touting this form of encryption as a suitable security measure for servers.

However, servers aren't like laptops; they are rarely powered down, and especially not if they are part of a cloud computing environment. In the cloud, there is no discrete physical hard drive assigned to a server, so your environment is exposed to malware and other threats all the time.

Companies taking a compliance-first approach may feel assured that FDE will secure their data, but in reality they are exposed at every moment their production servers are live.

Benefits: Security-First

A security-first organization would choose role-based encryption, either instead of or in addition to FDE. In role-based encryption, data at the application, file and database level is encrypted before it is written to disk and only decrypted for authorized accounts accessed with validated credentials. The data is protected while the server is operating and whether the server is physical or virtual.

Organizations using role-based encryption need to heed best practices for key management. Some businesses leave the management of their encryption keys to their vendors, creating the risk of their keys being used by a malicious insider or other attacker who has gained access to the vendor's environment. An organization should be the only party with access to its keys.

Keys should be stored separately from encrypted data. If the keys are stored in the same logical volume as the data they are intended to protect, an attacker can access both the data and the key needed to decrypt it in a single event.

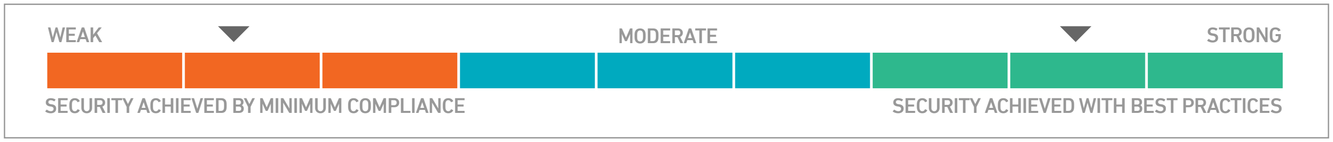
The encryption has to be transparent to users. If users have to enter complicated keys and passwords each time they need to access sensitive data, they will find ways to get around the inconvenience. In the process, they will create risk. Transparent encryption methods are the most secure method.

Business Objective Served

- Incorporate transparent security into the live environment

What's at Stake?

- Production environment
- Business-critical systems
- Data assets
- Intellectual property


WEAK
MODERATE
STRONG
SECURITY ACHIEVED BY MINIMUM COMPLIANCE
SECURITY ACHIEVED WITH BEST PRACTICES

The real requirement is strong security

These are just a handful of rules, and yet the weaknesses that emerge when they're completed with a compliance-first approach are considerable. Imagine the length of a compliance checklist and it's easy to see how an organization can unknowingly create a cascade of vulnerabilities as each item is ticked off.

In the end, a successful audit means little if real security hasn't been achieved.

The logic of a security-first approach is clear. Companies that embrace a security-first mindset automatically achieve compliance, so audits are less cumbersome and fines are prevented. Along the way, a safe environment is created for their customers so the risk of litigation and brand damage is minimized, while security can be planned holistically so operations can be streamlined and wasteful spending reduced.

"Companies that embrace a security-first mindset automatically achieve compliance, so audits are less cumbersome and fines are prevented."

Don't just follow the rules. Think about the purpose they are intended to achieve and serve that purpose with a strategic security plan that protects not only the assets covered by regulations, but your organization as a whole.

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™