Acquia

EXPERIENCE DIGITAL FREEDOM

SECURITY AND PERFORMANCE FOR OUR CUSTOMERS: WHY IT MATTERS

TABLE OF CONTENTS

INTRODUCTION

A protected customer is a happy customer. Professionals from countless industries — technology, education, pharmaceuticals, financial services — will tell you the same thing: security is critical. It is vital that organizations take note, because failing to appreciate the consequences of a breach can be catastrophic for both employees and customers. The evidence in support of data privacy and security controls has never been more clear:

- Researchers at the University of Maryland found that the average computer with internet access faces an attempted cyber attack every 39 seconds. One in three Americans is affected every year.
- Approximately 65 percent of cyberattacks are aimed at small- and medium-sized businesses, according to a report by the Kelser Corporation, a technology consulting firm.
- The Ponemon Institute has found that the average cost of a single cyberattack is $5 million USD

In other words, whether it's from malware, phishing, botnets, ransomware, a password attack, or denial-of-service attack, threats to cybersecurity are evolving as quickly as security solutions. And these threats are not insignificant — the Ponemon Institute has found that the average cost of a single cyberattack is $5 million USD. Facebook lost 3 percent of its market value after it was revealed that 50 million accounts were compromised. Sony incurred $1.25 billion in expenses from lost revenue, compensation, and legal fees after a 2011 data security incident.

The advent of new data privacy frameworks such as GDPR add new layers of complexity to industry standards and certifications, including HIPPA, FERPA, SOC, and PCI, so it can be understandably difficult for many businesses to navigate this web of regulation. Furthermore, many obstacles stand in the way of security compliance: staff resources and time, expertise, and of course, funding. CyberSeek finds that more than 300,000 cybersecurity jobs in the U.S. remain unfilled, and an ISACA survey finds that 95 percent of companies report a disconnect between their current and desired cybersecurity culture.

However, the cost of noncompliance has proven to be greater than the expense to implement necessary controls. For example, the annual cost of noncompliance has increased by 45 percent since 2011, setting back businesses, on average, $14.8 million USD and results in 2.71 times the cost of maintaining or meeting compliance requirements.

Together, these facts highlight a hard — if often overlooked — truth about the essential nature of security and compliance standards, and it is commonly understood the customer experience is only complete when such standards are in place. As evidenced above, particularly in a globalized world, the risks and related costs are too high to let the privacy and security of your customers' experiences and data take a backseat.

Fortunately, the potential for positive returns on your investment is similarly high. Compliant and secure digital systems sets the foundation of trust in your brand. In this e-book, we will explore both the needs and expectations of your customers as well as the various security standards a business should have in place. Finally, we will share how Acquia supports security and compliance.

GREAT EXPECTATIONS

A positive digital experience for users should be engaging, reliable, personalized, and efficient. However, if your user's experience isn't secure, everything else becomes irrelevant. Your users expect trust first and foremost — the other ingredients of the recipe are secondary. They expect that the personally identifiable information they share with you will be private and secure. In effect, you should consider their security the foundation of your relationship — not an afterthought or encumbrance.

When you're conceptualizing and planning your customer experiences, security must be an essential part of that process. Incorporating digital security into your workflow and priorities will ensure that you never have to beg for your customers'.

End-to-End Security

Digital security is far from one-dimensional. When thinking about how to secure your customer data, you must approach it from multiple angles to ensure protection from the beginning to the end of the customer's experience, as well as throughout any interactions.

For example, you may need to be able to scale from one to many sites, or from traditional to decoupled sites. You may be required to deploy content with a content delivery network, or CDN, which is a network of distributed servers that delivers digital content to users across geographic locations to provide high availability and high performance.

> *If your user's experience isn't secure, everything else becomes irrelevant*

DDoS Protection

A DDoS (Distributed Denial-of-Service) attack is an attempt to cripple a computer resource with a high volume of congestion. By exhausting the resources available to a network, application, or service, an attacker hopes to render your resource unavailable to genuine customers. Think of a DDoS attack as a traffic jam that clogs up a highway, preventing traffic from arriving at its intended destination. In the event of such an attack, interruptions to your site may occur and customers will then be rendered unable to interact or complete purchases with your business.

A successful DDoS attack exploit kit and attack services can be bought for about $500 on the dark web, yet such an attack can cost you and your customers much greater in breached data. Furthermore, your customers likely depend on uptime for revenue, as well to keep the lines of communication and information open. If your resources are unavailable, customers may look elsewhere for assistance. A successful attack could even lead to a violation of a your SLA with customers.

Furthermore, DDoS and data theft go hand-in-hand. According to a Neustar and Harris Interactive report, 92 percent of survey respondents who experienced a DDoS attack also reported theft of intellectual property or customer data. In other words, there is more at risk than downtime. It’s not uncommon for a hacker to use a DDoS attack as a distraction while they look for a bigger prize.

Typically, successful DDoS mitigation ensures that you are able to identify nefarious activity and divert such traffic in another direction, as well as filter out such traffic before it gets too close. This requires stringent analysis of security logs.

> ***According to a Neustar and Harris Interactive report, 92 percent of survey respondents who experienced a DDoS attack also reported theft of intellectual property or customer data.***
>
> neustar harris interactive

Bot Management

A recent study has reported more than half of web traffic today comes from bots, which are lines of code that perform automated tasks. Not all bots are created equally. Google has “good” bots, for example, that index the content that shows up in search results. Yet, there are many “bad” bots, which are very good at impersonating humans.

Bad bots are created for several reasons. They might try to spam a website comment section or a contact form. Or, they might be designed to expose or steal data or perhaps shut down entire websites. This is where Bot Management comes in. Bot Management has two objectives. First, it will identify whether incoming traffic is coming from a human or a machine. Second, it will control or block non-human traffic as needed. Bot management has truly become an essential aspect of modern digital security.

Web Application Firewall

A WAF (web application firewall) filters and monitors HTTP traffic between web applications and the broader internet and protects applications from many kinds of cyber attacks. A common WAF strategy utilizes pattern-matching software to ensure that inbound and outbound traffic has good intentions. A major strength of a WAF is the minimization of false positives — they are adept at adapting to the needs of ever-evolving web applications.

A WAF is as a way to protect valuable data from malicious hackers as well as protect the vulnerabilities in your resource that your web developers may not have noticed or had the time to fix. Cloud-based WAFs usually scale easily, whether from small-to-large or one-to-many websites.

Rate Limiting

Rate limiting controls the amount of traffic to or from a network. It is a useful safeguard against mistakes as well as threats, preventing any one user (or groups of users, such as a geographic segment) from retrieving a level of information that may overload the network for all users. It is also a widely used technique for maintaining data flow. For example, if an individual user attempts to exceed a set rate limit, they will either have to wait until the limit resets (based on a chosen time frame) or contact the web administrator.

Rate limiting is essential to safeguard against burst attacks, which are a type of DDoS attack. Some refer to burst attacks as “Hit-and-Run DDoS” because they consist of repeated short bursts of high-volume attacks, as high as gigabytes per second, at random intervals sometimes lasting hours or even days. A 2018 Radware study found that burst attacks are becoming more prevalent — for example, a major U.S. cellular carrier reported a tenfold increase in burst attacks in the preceding year.

Protecting against a burst attack requires some different preparation than your typical DDoS mitigation. While most DDoS solutions do mitigate against burst attacks, many DDoS solutions aren’t precise enough, which results in a high number of false alarms. Therefore, a relatively new approach, known as Behavioral DoS (BDoS) Protection technology, has become an essential tool for ensuring digital security from burst attacks. This advanced technology utilizes machine learning to analyze large datasets of traffic, detect anomalies, and adapt algorithms accordingly to protect digital assets.

radware

> ***Burst attacks are becoming more prevalent — for example, a major U.S. cellular carrier reported a tenfold increase in burst attacks in the preceding year.***
>
> **— 2018 Radware Study**

Secure Sockets Layer (SSL) and Transport Layer Security (TLS)

Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are cryptographic protocols that keep internet connections secure and protect sensitive data that are sent between two systems, such as a server and a client or two servers, from being accessed or modified by a third party via encryption. However, SSL/TLS protocols also fulfill another important business purpose — authentication. SSL/TLS protocols provide you with confirmation that you are sending information only to the intended recipient, not an imposter.

An SSL/TLS certificate, which can now be freely obtained, is the only method to ensure the protection and authentication that these technologies offer. Websites that utilize an SSL or TLS are easily distinguished with the https:// convention (as opposed to http://). When you obtain a certificate for your website, a visitor will notice that the web browser displays a padlock icon to the left of your URL anytime they access your website. This icon indicates the security of the connection and communicates to visitors that you value the connection and their privacy.

It's also worth noting that the benefits of the SSL/TLS extend beyond this important feature. Some browsers mark websites that lack such a certificate as unsafe. Starting in July 2018, Google has started this practice via its Chrome browser. Furthermore, the benefits extend to SEO — Google rewards sites bearing an SSL/TLS certificate with a slight boost in their search rankings.

TLS specifically has also become an integral cog in the security of devices connected through the Internet of Things (IoT). As more "things" come online, the connections between them require additional layers of security. TLS, along with encryption, provides a trusted level of security for data transmission.

Secure Access *WITH* a VPN

A virtual private network, or VPN, is an encrypted connection over the internet from a device to a network. This encrypted connection has two main functions — to safely transmit sensitive data between the device and network and prevent unauthorized users from eavesdropping on the traffic. VPNs are widely used in corporate environments as they allow employees to work remotely while freely accessing their company's network. The VPN acts much like a middle-man, retrieving data from an employee before transmitting it to the corporate network and vice versa.

It's unlikely that the average company will require clients to use a VPN when accessing their website. But that doesn't mean they're not an essential aspect of digital security and have great impact. VPNs provide total privacy when surfing the web, working with sensitive digital data, or using applications such as Skype without being monitored or tracked. This is achieved because the IP address is fully blocked from being accessed by other users — whether it is a state agency or a hacker. A VPN effectively protects all data and information, including customer data, internal documents and communication, and intellectual property.

Safely transmit sensitive data between the device and network and prevent unauthorized users from eavesdropping on the traffic.

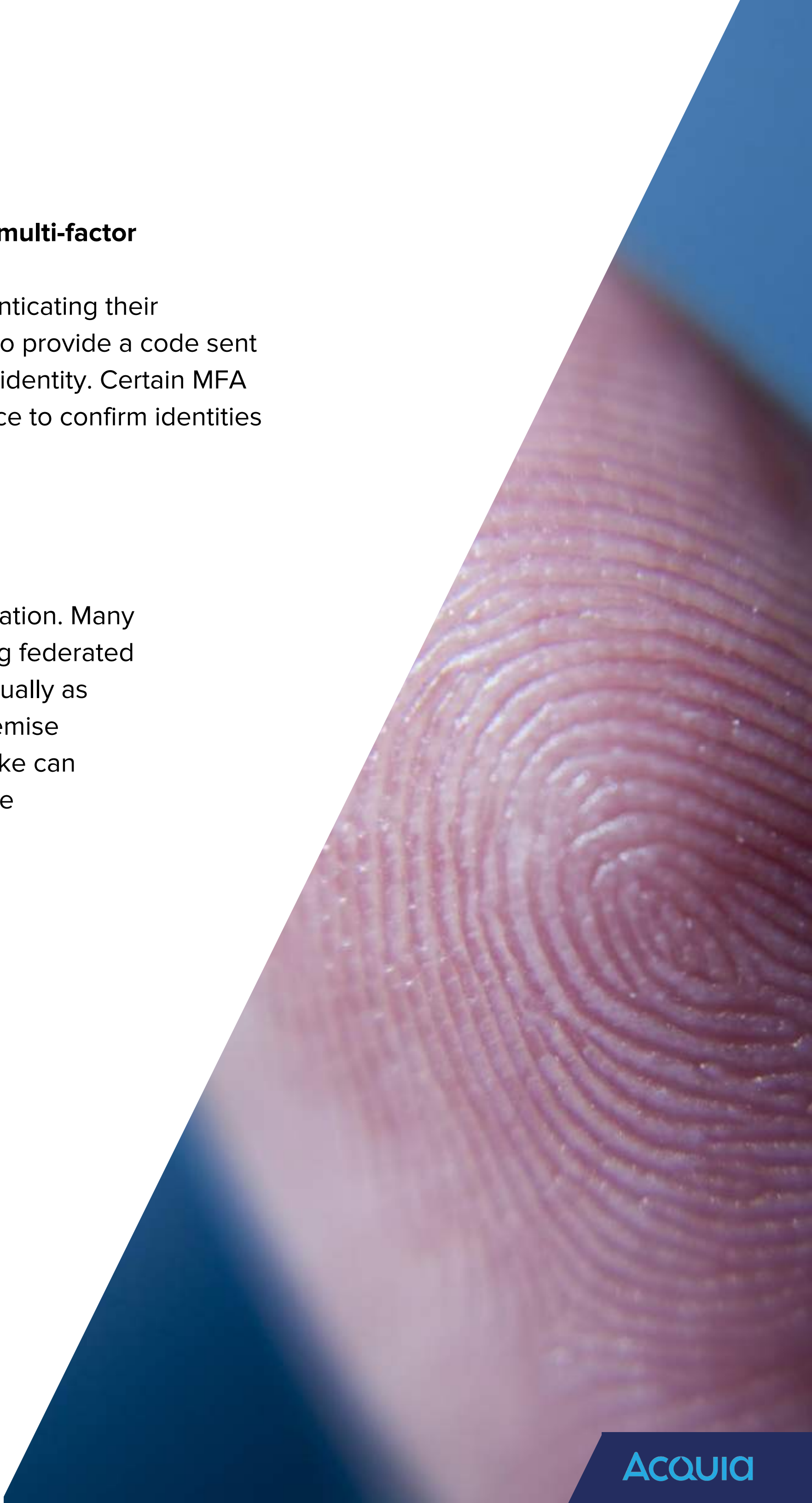
Multi-Factor Authorization (MFA)

Another tool that more organizations are deploying to enhance digital security is multi-factor authentication.

MFA ensures that a user is only granted access to a system after successfully authenticating their identity using evidence beyond a password. For example, a user might be required to provide a code sent to a registered cell phone number or email address or answer questions about their identity. Certain MFA clients have an app that members of an organization may download on a smart device to confirm identities with push notifications.

Secure Access ***WITHOUT*** a VPN

A VPN isn't the only way to provide secure remote access to members of an organization. Many companies utilize an application gateway, often engineered by a third party, featuring federated authentication with a single sign-on process for this same purpose. This system is usually as simple as providing an icon or tile for authenticated users to access a specific on-premise application. One major benefit of this approach is that users and IT administrators alike can avoid the hassle of having to install and maintain VPNs. Another advantage is that the web-based nature means that identity management and access control are easily streamlined and automated.



SECURITY THROUGH REGULATORY STANDARDS

In a globalized world full of cyberthreats and digital vulnerabilities, it's no surprise that governments and regulatory bodies have mandated various privacy standards to ensure that organizations protect users' data. Such frameworks have become an essential part of a legitimate business strategy in certain sectors and many firms are required to comply with multiple frameworks to abide by local and/or international laws. These same firms likely expect service providers to understand and account for the intricacies of such regulation. The following are some examples of standard regulatory frameworks.

Service Organization Control

The Statement on Standards for Attestation Engagements No. 16 (SSAE 16) is a body of standards created by the American Institute for Certified Public Accountants. It provides guidance as to how a certified public accountant (CPA) should undertake an audit of a third-party service organization, e.g., a cloud service provider. Such regulation is necessary since third-party service organizations hold a wealth of sensitive client data.
Within the SSAE 16 lies composition of Service Organization Control (SOC) certifications.

A service organization may attain SOC certifications via an audit to demonstrate that their internal data management system will keep their clients' data secure. Two key certifications are SOC 1 and SOC 2. SOC 1 Certification indicates that a third party (CPA) has audited an organization and concluded that it is in compliance and properly managing the information of its clients. SOC 2 Certification takes this recognition to the next level — it vouches that your company has proper internal controls for the management of data at various levels and over time.

The Federal Risk and Authorization Management Program

The Federal Risk and Authorization Management Program (FedRAMP) is a standardized approach that the U.S. federal government deploys to determine whether a cloud offering is sufficiently secure to be used in a contract by a federal agency. Third-party assessment organizations can use the guidelines offered by FedRAMP to make that decision.

FedRAMP is a mandatory framework for cloud deployments and service models within all federal agencies. Cloud service providers that want to demonstrate their commitment to the FedRAMP principles may pursue FedRAMP certification for their cloud service offerings. This can be a predictably long and bureaucratic process, but cloud service providers that attain such a certification can signal their commitment to security to governmental and non-government customers alike.

The General Data Protection Regulation

The General Data Protection Regulation (GDPR) is a body of legal rules governing organizations that work with data belonging to individuals from within the European Union. The aim of the GDPR is to guarantee citizens greater control over how their personal data is collected and used. Organizations must ensure that all data are gathered legally, with the consent of users, and under strict conditions. The GDPR dictates that consent to collect data must be "freely given, specific, informed, and unambiguous." Failure to protect this data from misuse can result in significant penalties.

This framework, implemented in May 2018, applies to any organization in the world that holds an establishment in the EU, offers goods and/or services to citizens of the EU or monitors the behavior of individuals in the EU. The European Commission, which authored the legislation, also compels organizations to keep close tabs on the location of every stored megabyte of customer data.

EU Cookie Regulations

In 2011, the European Union issued a directive to all member states about how to regulate the use of cookies. Since then, most member states have established laws based on this directive. Any European resident who uses cookies on a website must notify visitors about the cookies, as well as what the cookies are used for, and acquire consent before placing cookies on their device.

In general, if a user does not provide consent, placing cookies on their device is breaking with European law. However, cookies deemed “strictly necessary” to the function of a website and the services requested by visitors to a website are allowed.

Health Insurance Portability and Accountability Act (HIPAA)

Congress enacted the Health Insurance Portability and Accountability Act (HIPAA) in 1996 to set standards for the privacy of personal data related to healthcare. It is a national framework that supersedes any related state laws, unless they are more stringent. HIPAA outlines specific processes for healthcare providers, health insurance companies and any other entity with access to personal medical data to safely store, access and/or transmit such information electronically.

Non-compliance with HIPAA can result in civil or criminal penalties. Consequently, healthcare organizations tend to take HIPAA very seriously and expect their employees to do so as well.

However, in a world increasingly reliant on technology, the advent of fitness-tracking apps has posed challenges to HIPAA compliance. In 2009, Congress passed the Health Information Technology for Economic and Clinical Health Act (HITECH) to broaden the reach of HIPAA, absorbing such digital tools in its scope.

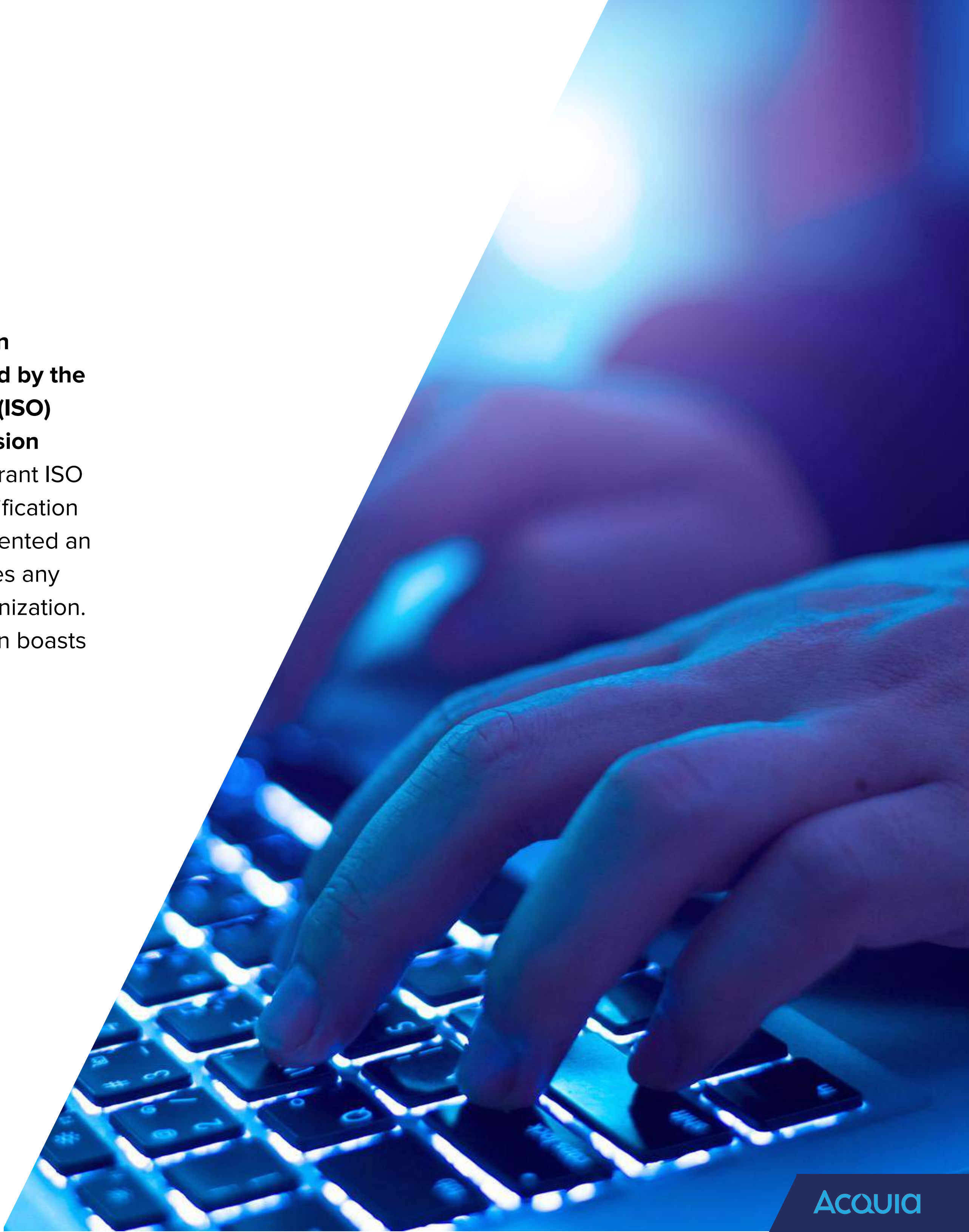
Federal Education Records Privacy Act

The Family Educational Rights and Privacy Act (FERPA) is a federal law governing who can access student information. The law states that parents have the right to access their children's education records until they are 18, as well as the right to initiate amendments to such records and control how an educational institution shares their child's records. However, when a minor turns 18 years old or matriculates at a post-secondary institution, the rights of the parent are transferred to that of the student.

Naturally, universities and colleges must strictly adhere to FERPA guidelines and may not share identifiable data about a student with anyone but that student. While FERPA does not require institutions to adopt specific privacy mechanisms, it does mandate the use of "reasonable methods" to safeguard student records. These precautions protect students against identity theft, fraud and extortion.

ISO 27001

ISO 27001 is a security standard for information management security systems (ISMS) published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Numerous bodies around the world may grant ISO 27001 Certification through an audit. Such a certification demonstrates that your organization has implemented an ISMS that thoroughly and systematically examines any risks, threats and vulnerabilities facing your organization. Furthermore, an ISO 27001–certified organization boasts a comprehensive suite of security controls and processes.

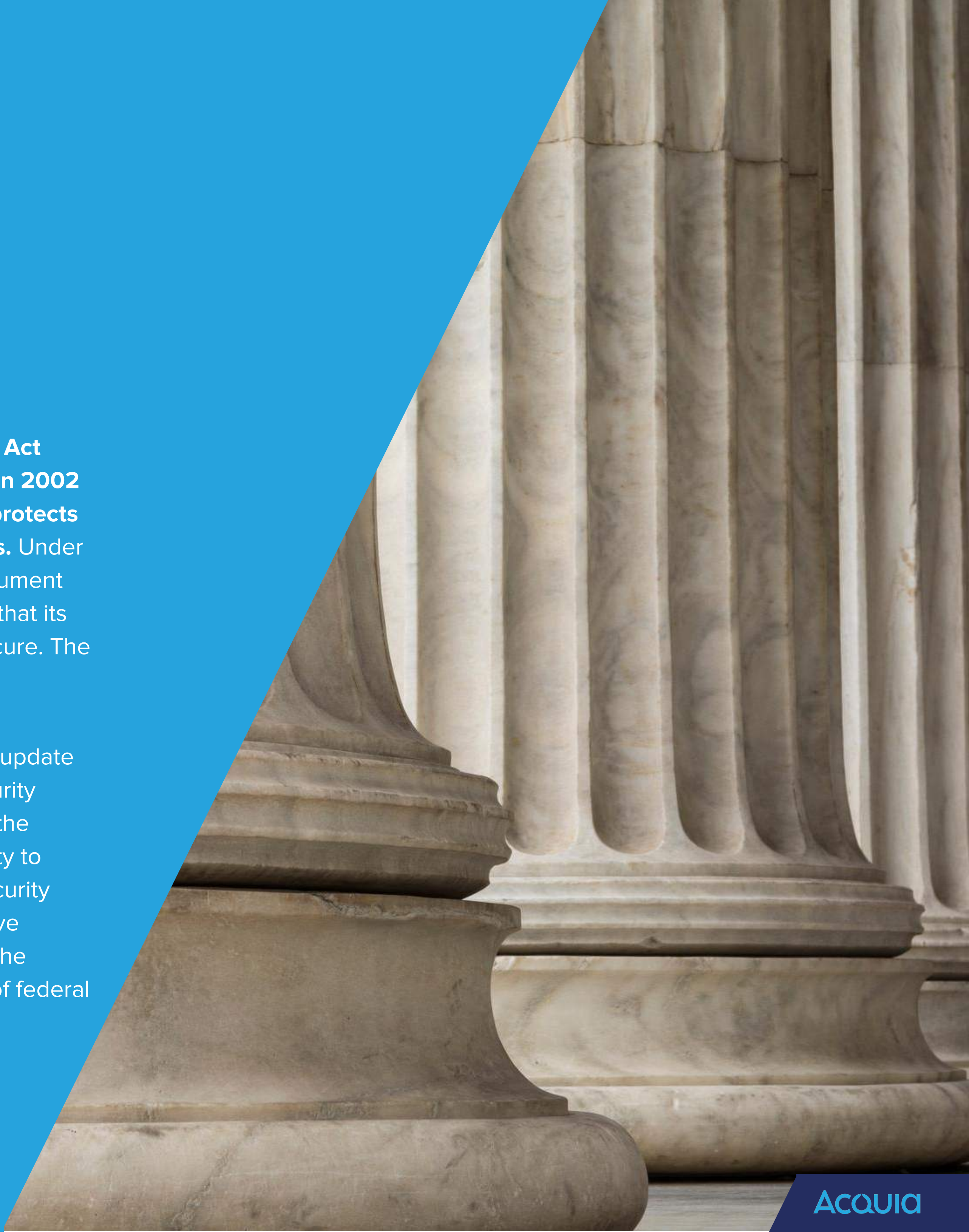


FISMA COMPLIANCE

The Federal Information Security Management Act (FISMA)

The Federal Information Security Management Act (FISMA) is legislation that was signed into law in 2002 as part of the Electronic Government Act that protects government information, operations and assets. Under the act, every federal agency must develop, document and implement a thorough process for ensuring that its information systems and data held within are secure. The act also necessitates the annual review of such programs.

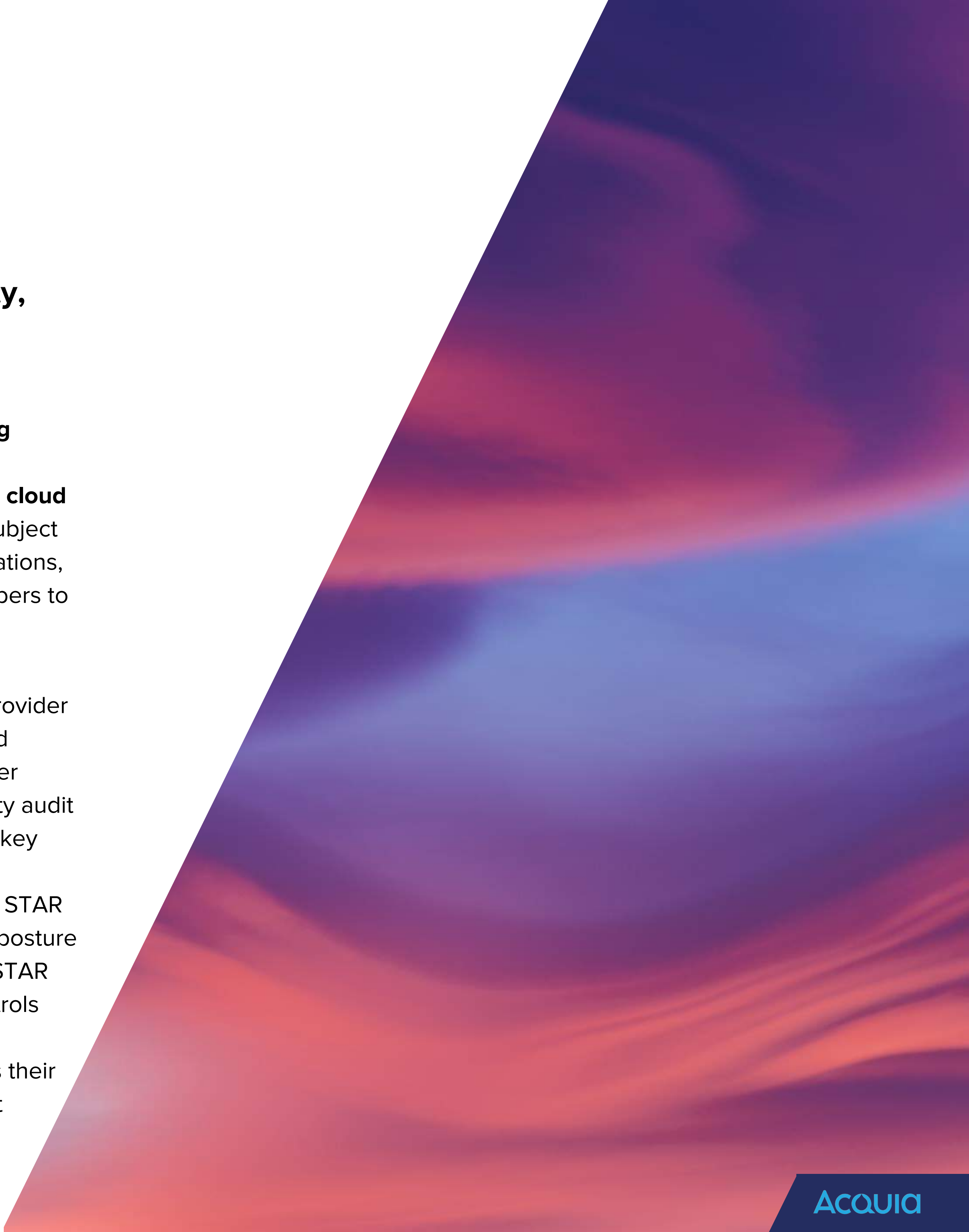
More recently, the U.S. government released an update to FISMA known as the Federal Information Security Modernization Act of 2014. The update codified the authority of the Department of Homeland Security to administer the implementation of information security policies for non-national security federal Executive Branch systems as well as clarified the role of the Office of Management and Budget in oversight of federal agency information security practices.



The Cloud Security Alliance Security, Trust and Assurance Registry (CSA STAR)

The Cloud Security Alliance (CSA) is the leading organization dedicated to defining and raising awareness of best practices to facilitate secure cloud computing environments. CSA harnesses the subject matter expertise of industry practitioners, associations, governments and corporate and individual members to offer cloud security-specific research, education, certification, events and products.

CSA operates the most popular cloud security provider certification program, the CSA Security, Trust and Assurance Registry (STAR), a three-tiered provider assurance program of self-assessment, third-party audit and continuous monitoring. STAR encompasses key principles of transparency, rigorous auditing and harmonization of standards. Companies that use STAR indicate best practices and validate the security posture of their cloud offerings. The publicly accessible STAR registry documents the security and privacy controls provided by popular cloud computing offerings. Furthermore, it allows cloud customers to assess their security providers to make the best procurement decisions.



Payment Card Industry Data Security Standard (PCI-DSS)

The Payment Card Industry Data Security Standard (PCI-DSS) is a body of standards drafted in 2007 to ensure that credit card information is maintained in a secure environment. The PCI-DSS is administered by the PCI Security Standards Council (PCI-SSC), an industry consortium composed of representatives from large financial companies such as American Express, Discover, MasterCard, and Visa.

Any organization that accepts, processes, stores or transmits cardholder information is beholden to the PSC-DSS. The council can fine a company it deems not to be in compliance up to $100,000 per month throughout which they are in violation.

ACQUIA EMPOWERS SECURITY AND COMPLIANCE

Acquia is deeply committed to digital security. Therefore, we strictly and enthusiastically adhere to a comprehensive compliance portfolio that validates the security of our platform. This compliance portfolio includes a variety of industry-specific audits and certifications performed by independent third parties. These independent evaluations rate the design and operational effectiveness of Acquia's security controls.

Acquia has also demonstrated success in protecting its customers. For example, in April 2018, Acquia blocked its users from 500,000 attack attempts during one week thanks to quick action by the development team in response to a Drupal security vulnerability cited as SA-CORE-2018-002. This is just one example of Acquia's commitment to security. Below are some of the most relevant services and products that Acquia offers its users in need of secure cloud solutions.

In April 2018, Acquia blocked its users from ***500,000 attack attempts during one week thanks*** *to quick action by the development team*

Acquia Cloud

CREATE AND MANAGE HUNDREDS OF SITES IN ONE PLACE

Acquia Cloud is a Drupal-tuned application lifecycle management suite with a complete infrastructure to support Drupal deployment workflow processes, from development and staging through to production. Acquia Cloud includes powerful developer user interfaces, secure server access using SSH, and automated deployment from a version-controlled code repository. It runs on proven open-source technologies that Acquia has selected, tested and optimized for Drupal. With Acquia Cloud, Acquia delivers comprehensive Drupal infrastructure support from a single vendor.

Acquia Cloud Site Factory®

SECURE. SCALABLE. SUPPORTED.
THE LEADER IN ENTERPRISE DRUPAL HOSTING.

Acquia Cloud Site Factory provides a multisite platform for digital technology organizations to efficiently deliver and govern many digital experience websites at a global scale. Ready and flexible, Acquia Cloud Site Factory creates a platform to support standard processes for building, provisioning and maintaining many websites and provides digital platform teams the visibility, trust and control for operating global websites as a service with a centralized, cloud management console.

Regulatory Compliance

All Acquia Cloud products and services are compliant with the following regulatory frameworks and policies:

HIPAA

FISMA

ISO 27001

FedRAMP

PCI DSS

CSA STAR

SOC 1

SOC 2

EU

PRIVACY

Acquia Cloud subscribers seeking additional layers of security and/or compliance may benefit from additional Acquia products.

Acquia Cloud Edge

The Acquia Cloud Edge platform secures your applications with protection against DDoS attacks, a Web Application Firewall (WAF), and high-speed DNS. Two products are offered within the Acquia Cloud Edge suite: Acquia Cloud Edge Protect, which examines web traffic looking for suspicious activity, and Acquia Cloud Edge CDN, which ensures that visitors interact with your application at the fastest possible speeds in any location globally. Acquia also offers a number of add-ons for the Cloud Edge platform:

- **Acquia Cloud Edge Accelerated Mobile Pages:** Accelerated Mobile Pages (AMP) improves the performance and security of mobile links. This add-on provides publishers with an AMP cache that is constantly updated with the latest improvements, and when it is used, publishers receive the performance benefits of AMP without having to give up control of the domain from which their content is served.
- **Acquia Cloud Edge Access:** Access allows users to secure, authenticate, and monitor user access to any domain, application, or path on Acquia Cloud Edge. Customers can quickly apply application-level user access permissions using existing single sign-on providers.
- Acquia Cloud Edge Argo Smart Routing: Argo Smart Routing improves performance with dynamic routing that finds the fastest traffic path within your network. Argo's Smart Routing algorithm uses real-time network information to route traffic across the fastest paths available and maintains open, secure connections to eliminate latency imposed by connection setup.
- **Acquia Cloud Edge Firebolt:** Firebolt allows customers to speed up and secure their advertisement websites to create a more reliable method for delivering content to consumers, resulting in an increase in conversion rates.
- **Acquia Cloud Edge Load Balancing:** Load Balancing improves network performance and redundancy by balancing traffic across multiple servers and routing to the closest geolocation. Load balancing distributes traffic across servers that are located at either single or multiple origin locations across the globe to ensure high availability of applications.
- **Acquia Cloud Edge Transport Layer Security (TLS):** The TLS add-on creates a secure connection between a client, such as a IoT device or a mobile app and its origin.
- **Acquia Cloud Edge Subdomain Support:** Subdomain Support allows customers to customize the features for that subdomain as if it was a top-level domain (TLD). The Subdomain Support add-on can assist with any arbitrary domain name underneath a TLD, for example, .com, and subdomain, such as .co or .uk. With the Acquia Cloud Edge Subdomain Support add-on in this example, the .co and .uk domains would have the same features as a TLD.
- **Acquia Cloud Edge Workers:** Workers allows customers to write V8 JavaScript code that is securely run at the network edge. The JavaScript code uses a derivative of the W3C standard Service Workers API running on the Acquia Cloud Edge servers to perform actions such as route, filter, or respond to HTTP requests that would otherwise need to be run on the customer origin in the Acquia Platform. In short, Workers sits behind Acquia Cloud Edge's core security services, and with advanced filtering logic, it can give customers more immediate control over how they interact with Acquia's security services.

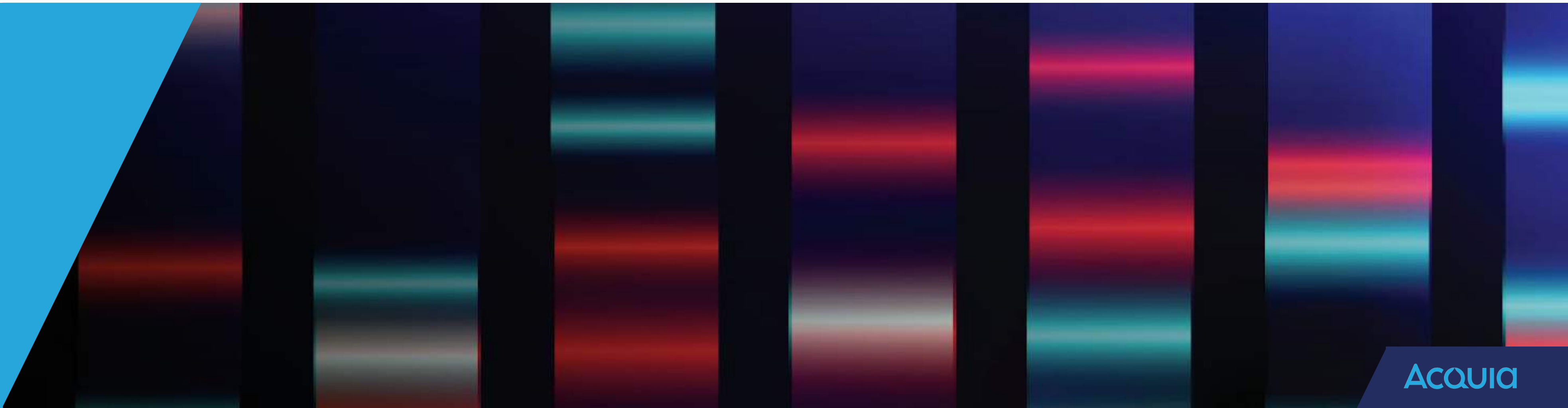
Acquia Cloud Shield

This platform ensures that your applications run in a dedicated, logically isolated section of the Acquia Cloud platform, adding more network-level security and capabilities to the stack. Acquia Cloud Shield gives you the benefits of Acquia Cloud platform-as-a-service, combined with extra security benefits and capabilities including IP address whitelisting for subscribers who must restrict access to the servers in their subscription.

Acquia Lift

Acquia Lift lets you track your customers' behavior throughout their buying journey — from anonymous visitor to loyal, repeat customer. Acquia Lift unifies customer content and profile data from multiple sources to deliver in-context, personalized experiences across any channel or device. Acquia Lift offers several packages to personalize your content for customers.

To strengthen and deepen Acquia's commitment to data protection, Acquia has implemented tools within Acquia Lift to be GDPR compliant. GDPR doesn't prevent personalization, but as mentioned above, it does change the way marketers collect personal data. Acquia's personalization solution provides the tools for our customers to configure data collection properly, such as the ability to set cookie duration, set visitors to do not track, anonymize profile, and hash any identifier.



SECURITY

Good security practices protect your site from hacker attacks. Drupal has good security built in if used correctly.

Best Practice

Once you begin to configure your site you might introduce new security issues. Plan configuration so that only trusted users have permissions that involve security risks.

- Keep core and contrib modules updated. You may not opt to do some module updates if the fixes or improvements have no direct effect on your site, however you should always apply security updates as soon as possible. Subscribe to security announcements on Drupal.org.
- Use strong passwords. Passwords are the most likely candidates for points of failure in your site security.
- Use the Password Policy module to devise a set of constraints before your users set their passwords.
- You can also set passwords to expire.
- Limit file uploads and what files are served. Limit the file types allowed and limit uploads to trusted users only. Check your permissions for specific content types and files types allowed in field uploads.
- Use the Security Review module and Acquia Insight. The Security Review module will analyze your site configuration and report methods for fixing errors. Use this module only on a staging or test site. Disable and remove the module on production sites. Our service, Acquia Insight, provides additional site configuration and security checks as well.

Plan configuration so that only trusted users have permissions that involve security risks.

CONCLUSION

No matter your industry or expertise, your team likely expends a lot of time and energy on two tasks: building customer trust and anticipating customer needs. These are essential goals for any brand, yet companies too often cut corners when it comes to digital security, which is a key ingredient in achieving both objectives. The privacy and security of your customers' experiences are the bedrock of your professional relationships.

It is in an organization's best interest to perform due diligence on any vendor's compliance with applicable industry standards and regulations, and as a vendor, we work just as diligently as you do to build trust with our customers. We are deeply committed to the digital security of our customers. Our secure platforms, as well as our track record, prove it.

We are also equally committed to anticipate your needs. This is critical in a time of ever-evolving technologies, privacy policies, and emerging cyber threats. Irrespective of the regulatory landscape or the newest or greatest telecommunications platforms, Acquia is prepared to adapt and evolve, just as you have. Whether your company requires a general framework compliant with your industry's regulatory structures to hit the ground running or a sophisticated solution tailored specifically to your needs, Acquia offers a comprehensive suite of platforms and services.

In short, we are committed to a complete digital experience for you and your customers. We are proud that our offering of products provides the backbone of a myriad of secure cloud computing applications, empowering a diverse array of organizations with digital solutions. We look forward to collaborating with you and empowering complete digital experiences for you and your customers.

```
.use_x = False
d.use_y = True
od.use_z = False
tion == "MIRROR_Z":
_mod.use_x = False
or_mod.use_y = False
ror_mod.use_z = True

selection at the end -add back the
or_ob.select= 1
ifier_ob.select=1
y.context.scene.objects.active = modi
rint("Selected" + str(modifier_ob)) #
    #mirror_ob.select = 0
```

ABOUT ACQUIA

Acquia is the open source digital experience company. We provide the world's most ambitious brands with technology that allows them to embrace innovation and create customer moments that matter. At Acquia, we believe in the power of community — giving our customers the freedom to build tomorrow on their terms.

acquia.com

Acquia