Security and Digital Experience: A Guide for Marketers

Contents

Introduction

Securing a company's data and digital properties is clearly the job of the security experts in IT. So what, you might ask, does that have to do with marketing?

While IT must focus their efforts on keeping websites, networks, and applications secure, the entire organization should be concerned about security. This includes finance, HR, marketing, and any department that invests heavily in technology or works with sensitive data.

Still, marketers should care more about security for one big reason: Security issues can have a huge impact on brand perception and the digital experience you deliver.

When sensitive customer data is stolen, it degrades trust in the brand. When data or site content is altered, it puts the brand's compliance at risk and can even expose it to legal liability. Malware, ransomware, and other types of cyberattacks, like distributed denial of service (DDoS) and zero-day attacks, can compromise site or application performance — and even shut down service completely. When a brand suffers such an incident, their customers may look for an alternative to their products or services.

Even if the incident is relatively minor, knowledge that a company's security solutions and protocols have failed can quickly tarnish a brand. Marketing can and should do things to ensure customer data integrity, guarantee site performance and availability, and control brand perception.

In this e-book, we will explore the types of security risks that most marketing teams should take accountability for. Along the way, we will lay out concrete steps marketers can take to address these risks so they can ensure ongoing, positive, and engaging digital experiences for their audiences.

Building Trust: Security and Customer Expectations

Companies collect and store massive amounts of customer data. This includes everything from personal profile data to credit card and other financial information. For customers to share this information at all, they need to have a baseline trust in the brand, and that isn't easy to come by.

As revealed in our most recent customer experience trends report, "Create Engaging Customer Experiences. Launch Faster.," only half of consumers (51%) trust that all brands will handle their personal data properly.

In order to communicate the trustworthiness of a brand effectively, marketers need to ask themselves the following questions:

- Can customers trust us with their data? Can we verify that?
- What kind of response will customers expect if we experience a data breach?
- What does it mean to our customers if our website, applications, or services are not readily available? What are we doing to prevent that?
- How can we best reassure customers that their data is safe with us?

While the answers to these questions will guide messaging around security, brand trustworthiness begins with ensuring data is secure and that compliance with all relevant regulations is maintained.

Categories of Risk: Three Types of Risk Facing Your Organization

Risk to Data Integrity

Data needs to be trustworthy, which means companies need to prevent data from being unlawfully accessed or altered in any way. Such alterations could range from a juvenile prank, where someone accesses a website and changes the content to something inappropriate, to important data records being changed to hide criminal activity.

Risk to Data Availability

Customers will expect that your website and other digital services are available at all times. Distributed denial of service attacks and ransomware attacks can affect the availability of such data.

This could prevent customers from accessing any personal data they have stored on your site — or using your site at all.

Risk to Data Security

For regulatory and legal reasons, brands need to ensure their data cannot be stolen. Data integrity and data security both require that access to data be strictly controlled and monitored.

Phishing attacks are a common way bad actors get around such controls. These attacks generally take the form of emails sent to unsuspecting employees containing malware cleverly disguised to look like official company communications.

Sometimes, bad actors also assume a brand's identity and contact customers, tricking them into compromising their own data.

Your organization's security team likely already spends a great deal of time assessing and mitigating the risks just described. It's marketing's job to not only heed these risks, but to also think about the impact they can have on current customers, potential customers, and the brand.

Security and Compliance

Security and compliance are not the same thing.

Compliance means abiding by the standards of specific regulations, which may or may not pertain to security. Security involves preventing unauthorized access to – and use of – a company's data and technical resources. Security also implies securing an organization's physical assets and premises.

Make no mistake: an organization could have the world's most secure servers and architecture, but still be non-compliant with industry regulations.

Likewise, you could have a system that is compliant with every law and regulation, but not sufficiently secure.

It should go without saying that protecting your customer's data is paramount, but remaining compliant with worldwide regulations may be critical to the health of your business. If an organization violates the European Union's General Data Protection Regulation (GDPR) it could be fined up to $11 million or 2% of a company's yearly revenue (whichever is greater).

More serious violations can accrue fines of up to $22 million or 4% of a company's yearly revenue (again, whichever is greater). In 2022 alone, the European Union levied a record €2.92 billion in penalties.

The United States has also begun imposing fines for violations of its data privacy protections. The California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA), for instance, levy fines of $2,500 on the low end, while the Colorado Privacy Act (CPA) can levy a fine of up to $20,000. The Virginia Consumer Data Protection Act (VCDPA), on the other hand, falls somewhere in the middle; the regulation can levy a fine of up to $7,500.

Just remember that none of this legislation is written exactly the same, so it's important to follow the guidelines in the areas you conduct business.

The bottom line is that every organization needs to account for both security and compliance.

Assessing Risk: A Marketing Perspective

Unlike most marketers, security professionals are accustomed to thinking about vulnerabilities, risks, and threats. But the truth is, everyone has good reason to prioritize security. Recent research published by IBM found the average cost of a data breach has increased to $4.35 million. So, when marketers start thinking about security, they also need to focus on proactively managing risk.

Many brands take a reactive approach when it comes to risk. Unfortunately, this increases the likelihood of an eventual security incident and means that the brand will end up doing even more work to repair its reputation. It can also result in damaging PR if a brand is held legally liable for the event, financial consequences aside.

The key to managing risk is being proactive. This starts with carefully identifying the risks that apply to you and your business.

There are two aspects of risk that marketers should account for:

- The probability that a particular security event might occur.
- The consequences, in terms of customer experience and brand reputation, if such an event occurs.

Assessing risk in this way is contextual. While a clothing retailer and a multinational investment firm may face some similar kinds of security risks, the threat posed to the brand will be very different in each case.

Different Brands, Different Risks

While both companies store sensitive customer data, the type of customer information held by an investment firm will bear little resemblance to that held by a retailer. Since an investment firm handles its clients' financial portfolios, a data breach could result in identity theft and financial calamity — an outcome that would strike at the heart of its brand.

The clothing retailer, on the other hand, may have customers' demographics and credit card information stored. But credit cards can easily be canceled and the potential inconvenience and financial losses are unlikely to be severe.

Similarly, if a hacker removed, altered, or manipulated content on a retail website, it would be a nuisance, but the consequences would be manageable. However, banks and other organizations in heavily regulated industries, such as legal services or pharmaceuticals, may suddenly find themselves out of compliance with relevant regulations.

At the same time, disruptions to service might affect a retailer more than an investment firm. For any organization that depends heavily on e-commerce, a cyberattack may freeze business until the issue is resolved. In such an event, retailers would likely lose a significant amount of sales and possibly future customers.

At the end of the day, an ounce of prevention is worth a pound of cure. As the examples above highlight, anything a brand can do to avoid a significant security incident pays dividends, not only when it comes to customer experience and brand equity, but also in terms of the bottom line.

Choosing the Right Tools: Focus on Security

Marketing can be a valuable partner to IT when it comes to security, primarily by prioritizing security when selecting tools and platforms that support the digital experience. Here is a basic framework for approaching tool and platform selection from a security perspective.

Do Your Research

What are other companies like yours (in terms of size, industry, and so on) doing to ensure the security of their digital properties? What vendors and services do they use and trust?

Marketers must ensure the solutions they're using meet the highest industry standards for security and regulatory compliance. To this end, it's in an organization's best interest to perform due diligence on vendor compliance with applicable industry standards and regulations.

SLAs

Platform and hosting companies offer service level agreements (SLAs) outlining what their clients can expect to receive in terms of services and site availability (uptime). SLAs are crucial to ensuring a platform will stay up and running without interruption. SLAs also offer peace of mind that a vendor has the right people and practices in place to resolve any disruptions as quickly as possible.

Since every organization is different, you need to make sure an SLA meets your particular needs and expectations. In many cases, vendors will offer more than you need or expect. For example, the industry standard is "three nines" (99.9% uptime), but many vendors offer "five nines" (99.999% uptime) or more. It's up to you to decide what those other two nines are worth!

You should also ask vendors to demonstrate that they can and will meet their SLAs.

Vendors should be able to provide regular reports on the performance metrics agreed upon in the SLA, as well as a real-time status page and transparent historical information regarding service downtime.

Finally, vendors should be prepared to offer compensation for downtime and/or failure to meet defined requirements in the SLAs.

Support

While SLAs are important to have in place, ongoing support is even better. The degree of support you need will be based on your organization's size, scope, and internal resources. If you don't have the in-house expertise and personnel to rapidly respond to critical security issues, it is crucial that your solution provider does.

Compliance

When you rely on a partner to host or maintain your sites, you essentially outsource both security and compliance to them. This means ensuring they follow all standard best practices when it comes to security, from user authentication to timely patching, and that they are compliant with and accredited for specific regulatory frameworks such as CCPA, FedRAMP, GDPR, HIPAA, ISO 27001, PCI, and SOC 2.

Security Scanning and Testing

Finally, contracts with the vendors you select should include terms regarding regular testing of their security practices and systems.

This testing comes in two forms: one focused on the actual security measures in place and the other assessing the effectiveness of these measures.

These are very common and your vendors should be doing them regularly (at least monthly for vulnerability scanning and once or twice a year for penetration testing). These should provide you with the confidence that your data and organizational interests will be protected by a particular vendor.

Modern Marketing and Security

“It’s time organizations of all sizes roll up their sleeves, coordinate with the IT team, and establish best practices for protecting data. Data is a significant asset. Marketers have to keep gathering it, but they can also be the first line of defense to ensure that it’s protected.”

Becca Chambers, VP of Global Corporate Communications, Corel, in Forbes

Acquia and Security

Acquia is deeply committed to the security of all our customers' digital properties. We strictly and enthusiastically adhere to a comprehensive security and compliance portfolio that validates the safety of our platform. This portfolio includes a variety of industry-specific audits and certifications performed by independent third parties. Our platform is compliant with all major regulatory frameworks and policies.

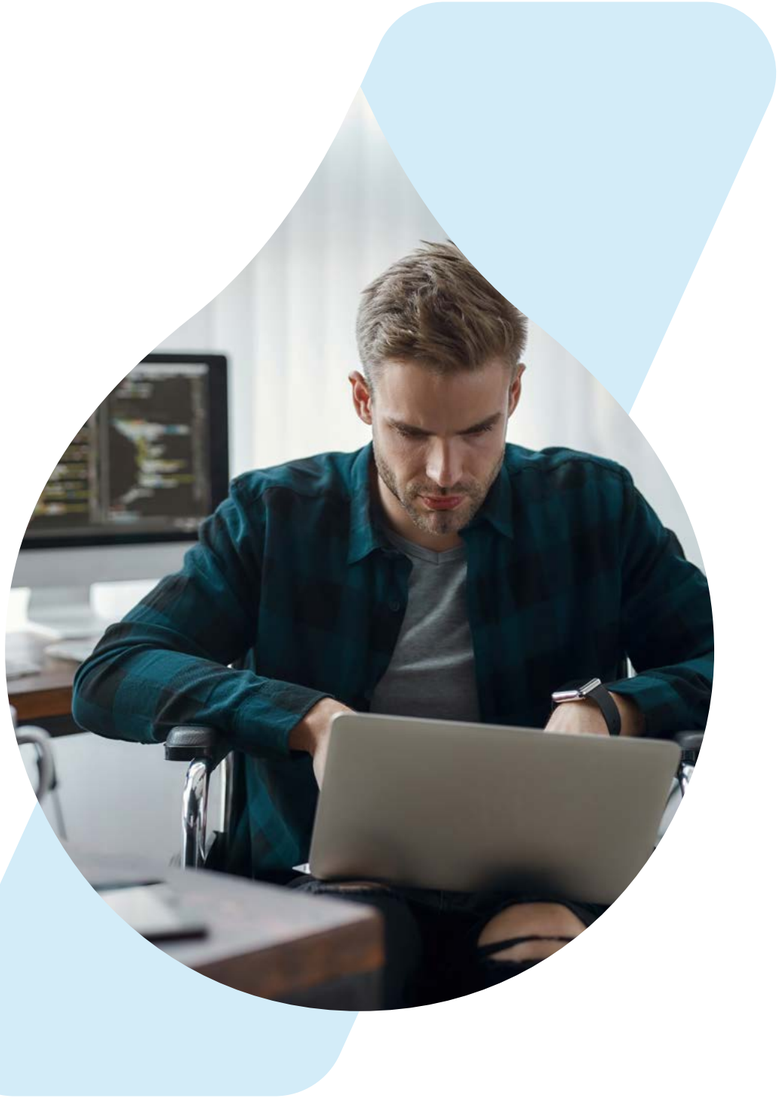
To further protect you from becoming the next online threat victim, Acquia provides a preemptive mitigation solution called Acquia Edge Security.

Through Edge, customers get a web application firewall (WAF) and DDoS mitigation solution that delivers hands-off security monitoring and real-time attack mitigation. The features include preemptive identification and mitigation in under 10 seconds of any risk or impacts on customer site and application responsiveness tied to unpredictable, catastrophic security threats.

We are also committed to anticipating your needs as a valued customer. We recognize that this is critical in an era of ever-evolving technologies, increased focus on privacy, and emerging cyberthreats. We don't just hand off the technology and wish you luck. Instead, we are an engaged partner that helps every step of the way and are always available when you need us.

As one example, Acquia recently renewed its support of the Drupal Steward Program, which adds another strong layer of protection across the portfolio of products optimized for Drupal.

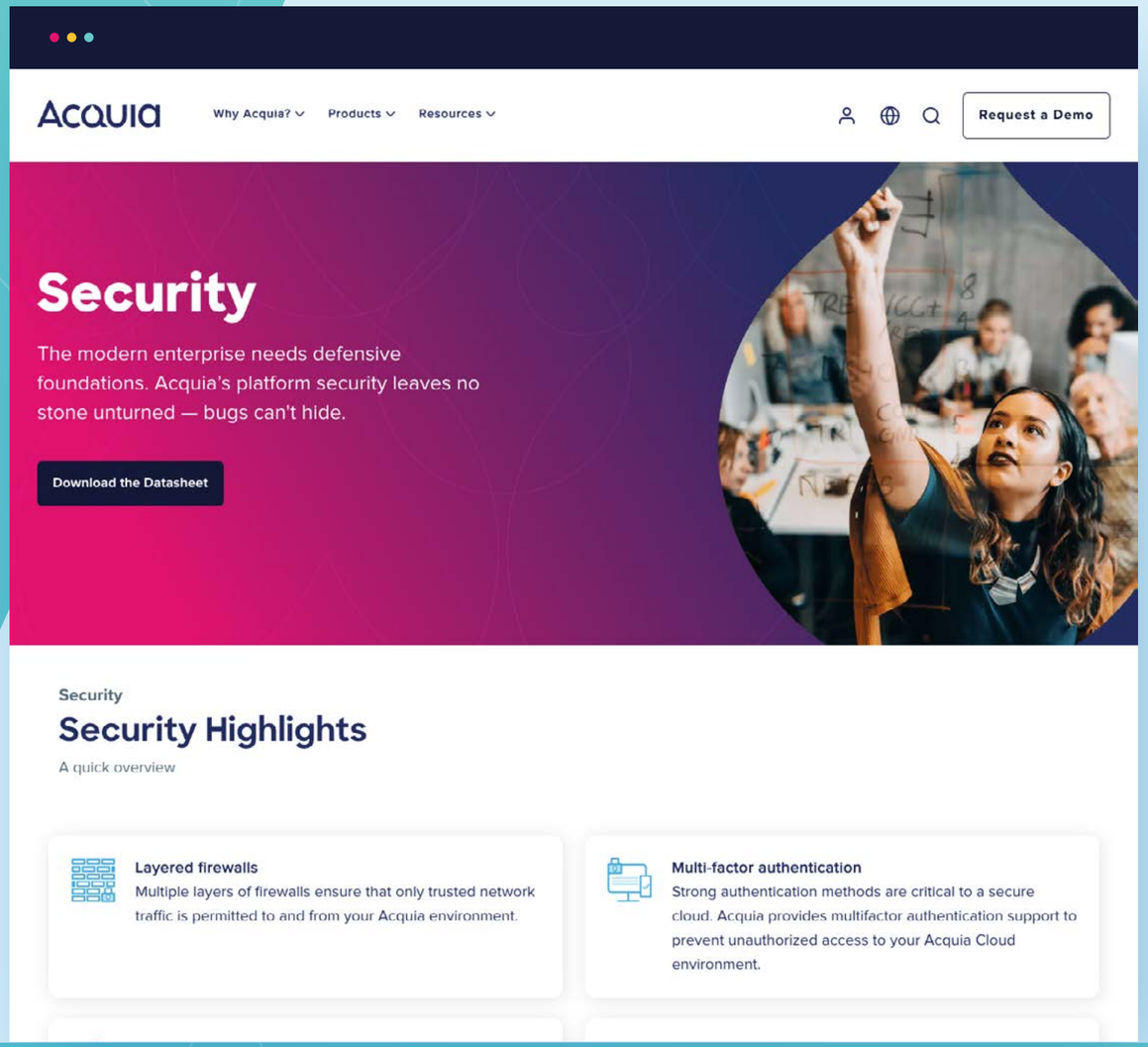
Whether your company requires a general framework compliant with your industry's regulatory structures or a sophisticated solution tailored specifically to your needs, Acquia offers a comprehensive suite of platforms and services.



Secure By Design

At Acquia, we build security into the digital experience.

Learn More



ACQUIA.COM

About Acquia

Acquia empowers the world's most ambitious brands to create digital customer experiences that matter. With open source Drupal at its core, the Acquia Digital Experience Platform (DXP) enables marketers, developers, and IT operations teams at thousands of global organizations to rapidly compose and deploy digital products and services that engage customers, enhance conversions, and help businesses stand out.