Akamai

THE IT DIGITAL MATURITY HANDBOOK:

A GUIDE TO DELIVERING SECURE, INNOVATIVE CUSTOMER EXPERIENCES AND ENGAGEMENT MODELS THAT PAY OFF

The Digital Experience Imperative

Today's IT leaders are tasked with helping to chart their companies' digital future by building a modern foundation for business. To maintain availability and security, companies need to stay on top of vulnerabilities, evolving attack vectors, zero-day attacks, DDoS-for-hire, and threats from growing IoT-fueled botnets.

In other words, companies must balance seamless digital experiences and fail-safe security to survive in today's economy. Together, these form the foundation of trust and loyalty. They also lead to future business success.

In fact, the most digitally mature companies grow faster than their competitors, more frequently reporting double-digit revenue growth.[1] No wonder "delivering digital services and operations has emerged as a prime mover in reshaping customer experience in almost every sector."[2]

That said, as digital experiences become more sophisticated, security becomes more complex. Failing to achieve the balance can result in less agility, longer time to market, and less of a competitive edge. This brief explores these challenges and what it takes to strike the perfect equilibrium.

> Research by IDC demonstrates that in 2017, the top two priorities for IT executives were "focusing on improving customer experience and creating new engagement models" (64%) and "creating new business models and developing new digital revenue streams" (62%).[3]

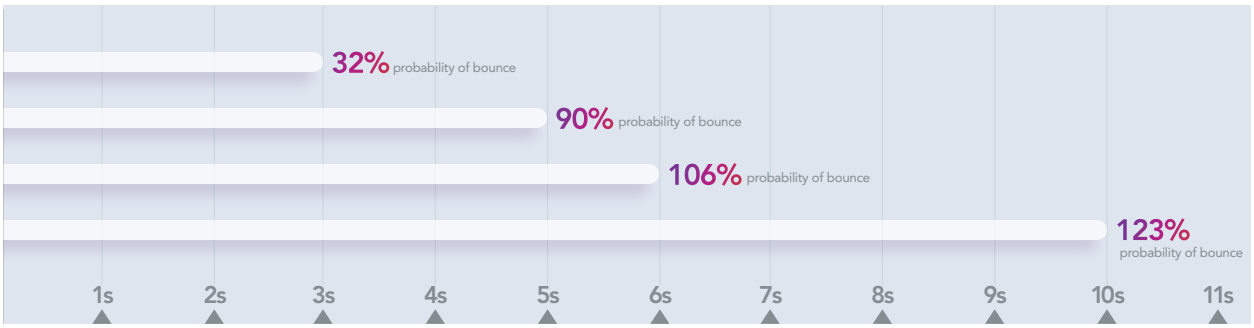
What Defines World-Class Experiences?

While the imperative to deliver sophisticated digital experiences is clear, it's no small feat. Consider the performance element.

How fast your website loads is critical … and that includes page load times on mobile devices. According to Google, the average time it takes to fully load a mobile landing page is 15 seconds. That's far too slow when you consider that 53% of mobile site visitors will leave a page that takes longer than three seconds to load.[4]

Google data shows more than half of overall web traffic comes from mobile[5], and Google will increasingly rank sites based on the performance of their mobile pages and content[6].

1) Forrester Consulting, Drop A Pin At The Intersection Of Digital Experience And Security, November 2017
2) McKinsey, Mastering the digital advantage in transforming customer experience, May 2017
3) FCIO, State of the CIO, Winter 2018
4) Google Inc., Find out how you stack up to new industry benchmarks for mobile page speed, February 2018
5) Google Inc., Find out how you stack up to new industry benchmarks for mobile page speed, February 2018
6) Google Inc., Rolling out mobile-first indexing, March 26, 2018



However, site visitors and application users are spread across the world, using a plethora of devices and screen sizes in regions characterized by varying network connectivity. It's challenging for most organizations to address these variations and optimize for performance on their own. The world outside the company data center is much larger than that within, and is subject to events and conditions beyond an organization's control.

Security is the other extremely important aspect of digital experiences. Yet again, organizations face challenges ensuring world-class security.

The classic, contained enterprise network is a distant memory in a digital world. Digital transformation has led to an explosion of connected environments and devices, rendering perimeter protection insufficient. As attackers and others with malicious intent compromise weak links, they gain deep access to organizations' networks, systems, and data.

The focus of almost every attack is access to the ever-growing and increasingly more valuable data stores dispersed throughout and beyond the corporate environment. This makes it even more alarming that end points are more vulnerable than ever. After all, applications are shifting out of the data center and into the cloud, and employees, partners, and contractors are moving from dedicated offices to remote access in homes, coffeehouses, and everywhere in between.

GDPR: An Opportunity to Build Trust

The General Data Protection Regulation (GDPR) heightens the security issue – while also offering an opportunity to build consumer trust. Under the GDPR, companies are liable for any violation when it comes to how they handle, process, and store data associated with their prospects and customers. With 50% of consumers abandoning their online purchases because the customer journey does not reassure them regarding what will happen to the personal information they provide[7], organizations employing stringent security stand to gain.

Using sophisticated means, attackers can exploit vulnerabilities at rapid-fire pace. Consider the Loapi botnet. Designed to run on mobile devices, this malware was originally used to fuel DDoS attacks. But its creators pushed a modular version, meaning attackers can easily take advantage of Loapi when they find a new vulnerability or a need a new capability.

7) Extens consulting, Take a good look, because behind GDPR compliance hides a host of opportunities! December 4, 2017

In fact, attacks are growing in number, sophistication, and impact. Between Q4 2016 and Q4 2017, Akamai detected a 14% increase in total DDoS attacks, a 14% Increase in infrastructure layer (layers 3 & 4) attacks, and a 4% increase in reflection-based attacks. During the same time period, Akamai saw a 10% increase in both total web application attacks and SQLi attacks, and found that a high percentage (43%) of website login attempts were malicious. Moreover, these attacks continue to focus on industries with high-value data.[8] (For more information, check out the most recent Akamai threat advisories: https://www.akamai.com/us/en/about/our-thinking/threat-advisories.)

The impact of a successful attack on a business can be devastating and immediate. That's because the cost associated with cyberattacks is on the rise, averaging $60 million a year when attackers use stolen credentials to make fraudulent purchases or transactions.[9]

The rise in data breaches and vulnerabilities has led some to suggest that security-less digital transformation leaves organizations at greater risk. Gartner predicted that 60% of digital businesses will suffer major service failures by 2020 due to the inability of security teams to manage digital risk.[10]

The good news is that organizations are responding. Over 70% of businesses surveyed across the United States and Europe have indicated their security budgets are increasing.[11]

What is the real-world impact of taking a proactive, strategic approach to balancing the digital experience and security? Consider these two examples:

One of the world's largest financial asset management companies sees high bot traffic, including credential stuffing and other fraud-related activities. It was experiencing 8,000 account takeovers a month across multiple login endpoints, which led to $100,000 per day in direct fraud-related losses. In response, the firm deployed behavioral-based bot detections in front of every consumer login endpoint. The result? It dramatically reduced account takeovers to just one to three per month and fraud-related losses to $1,000 to $2,000 per day across all login endpoints.

As a growing percentage of retail moves to the mobile channel, an American fashion retailer wanted to respond to that seismic shift in consumer preferences in a scalable way. To provide a seamless customer experience between mobile browsers, desktop browsers, and its new mobile app, it re-architected to a single-page architecture. However, that change exposed the business to new security threats. With the right API protection in place, it was able to execute its shift in business strategy and successfully achieve its growth goals. Within a year, it achieved:

- 66% YoY revenue increase
- 8% of annual target; 24% over projection
- Two $1 million hours, including Cyber Monday
- First $500,000 shopping day for mobile app
- Increased conversions for every channel (9% desktop, 8% tablet, 4% mobile)

The top reason organizations say they secure their web applications is to protect sensitive data and prevent a data breach. The next reason is to prevent revenue loss.[12]

8) Akamai, State of the Internet Security, Q4 2017

9) Ponemon Institute, The Cost of Credential Stuffing, October 2017

10) Gartner, Gartner Says By 2020, 60 Percent of Digital Businesses Will Suffer Major Service Failures Due to the Inability of IT Security Teams to Manage Digital Risk, June 6, 2016

11) CSO, What is security's role in digital transformation? March 14, 2018

12) Ponemon Institute, Trends in the Cost of Web Application & Denial of Service Attacks, September 2017

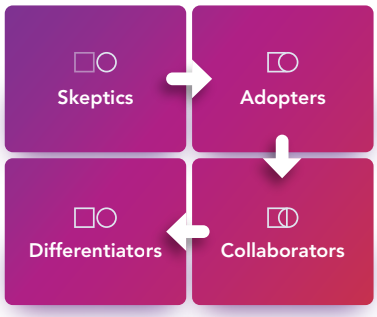
What Makes **Companies Digitally Mature?**

Organizations are at one of four maturity levels when it comes to digital experiences.[13]

- **Skeptics:** Just beginning the digital journey, finding themselves relatively unaware of the evolving expectations of customers.
- **Adopters:** Investing in skills and infrastructure.
- **Collaborators:** Breaking down traditional silos.
- **Differentiators:** Striving to meet evolving customer expectations, backing this with needed budget.

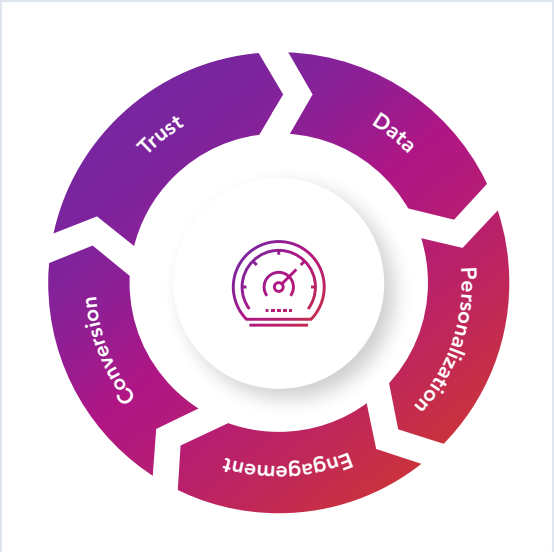
Differentiators balance data-driven digital innovation and security to deliver the experience today's customers expect. As a result, they tend to be the leaders in their industries, enjoying higher growth rates and higher levels of customer trust.

The Maturity Framework segmented respondents into one of four maturity levels



Balance of Data, Experience, And Security

In today's digitally connected world, customer data fuels new experiences. That's why the most digitally mature companies succeed by putting customer data at the center of both experience and security strategies.



"Data security is the top investment priority … often the tip of the spear for digital transformation strategies," says analyst Nicholas McQuire, who leads CCS Insight's enterprise research practice. "What has certainly changed is that today security has become not only a key technical priority but also a business one as well." [14]

The Boston Consulting Group found that "… brands that create personalized experiences by integrating advanced digital technologies and proprietary data for customers are seeing revenue increase by 6% to 10% – two to three times faster than those that don't."[15]

Companies that are able to hyper-personalize drive higher engagement and conversions and gain even more customer trust. It's an enviable, virtuous circle.

But remember: Customer data is under constant threat of attack and loss. And that can easily disrupt the virtuous circle. When trust is lost due to a breach, it puts at risk customer loyalty and the opportunity to drive revenue from customer data insights. According to Forrester, even mere negative suspicion of a company's data use practices can cut revenues by up to 25%.

Because digital experiences and customer data are so tightly intertwined, Forrester says world-class digital experiences are now and forever bound to effective security.

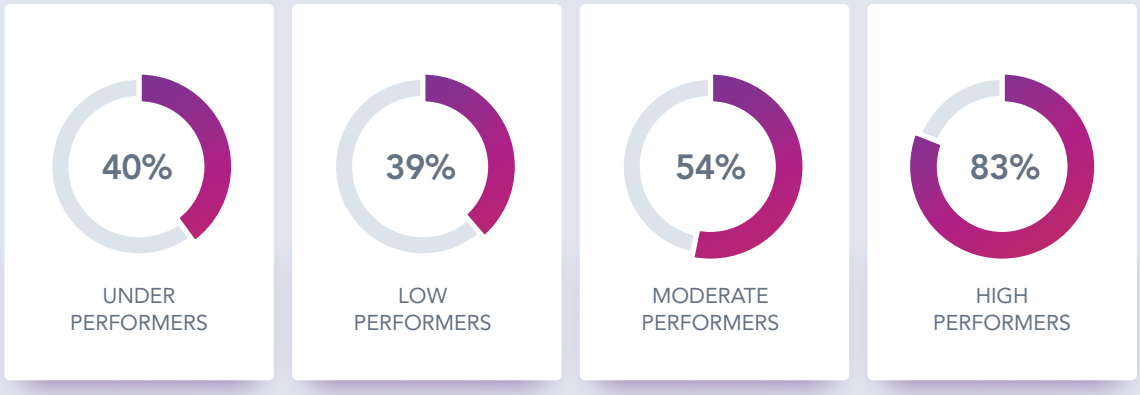
13) Forrester Consulting, Drop A Pin At The Intersection Of Digital Experience And Security, November 2017
14) Ponemon Institute, Trends in the Cost of Web Application & Denial of Service Attacks, September 2017
15) The Boston Consulting Group, Profiting from Personalization, May 8, 2017

> Firms that ensure security is part of the digital transformation effort … right from the beginning … are those that I have seen not only succeed in the long run but also move faster in terms of getting to market in today's climate.[16]
>
> – **Nicholas McQuire**, Vice President, Enterprise Research, CCS Insight

Based on research conducted by Forrester Consulting, digitally mature businesses grasp the importance of a strong security approach and investment.

The highest maturity security behaviours are most often adopted at the highest performing companies.

A security breach of customer data would have a catastrophic impact.



That said, even they must continually reassess their approach to and investment in security. The mandate is for companies to secure customer data without dampening innovation.

Notably, Forrester Consulting underscored the following:

- **Maturity creates complexity surrounding security.** As companies mature their digital capabilities, they should plan to increase investment to sustain the security of customer data.
- **Maturity in security also challenges agility.** While 22% of skeptics struggle to find the balance between security protocols and business agility, more than a third of collaborators and differentiators also share that struggle.
- **Differentiators understand trust depends on investing in security.** Twenty-seven percent of skeptics lack security budget, compared to just 16% of differentiators. Put another way, differentiators understand their revenue depends on investing in security.

16) CSO, What is security's role in digital transformation? March 14, 2018

Essential Elements to **Achieve Digital Maturity**

Companies must balance seamless digital experiences and fail-safe security to accelerate growth and build customer trust in the digital age. In other words, they must ensure the highest levels of web performance and security.

Web Performance

Online success starts with a performance baseline fueled by real user experience that serves as the foundation for insights that are turned into meaningful actions.

To strike the right balance between rich and responsive online experiences, organizations must understand user behavior by geography, network, and device access as well as how those factors impact the way their applications are used. With a continuous approach to digital performance management, companies can monitor, optimize, and validate user experiences to maximize online revenue.

The only way to truly see the actual experiences of users is with digital performance management that incorporates real user measurement (RUM). RUM tracks session paths, bounce rates, user think time, user location, device type, network type, third-party resources, and peak analysis – all critical pieces in understanding and predicting how users will behave. It also allows companies to map user data to business objectives with key performance indicator (KPI) metrics such as bounce rate, conversion, session length, and revenue. With this understanding, organizations can then employ the best-suited solutions to optimize performance.

The key is to use digital performance management tools that align with the organization's business strategy and IT execution without introducing additional complexity.

Understand Two Common Approaches to Monitoring

Synthetic monitoring is a simulated health check of a site or application that can help find code defects, benchmark against the competition, and compare current and previous versions of site pages. Real user measurement (RUM) provides insight into the actual experiences of site visitors and application users.

Web Security

At the same time, organizations need to stay two steps ahead of cyberthreats that are intensifying in magnitude and sophistication every day.

APIs and third-party integrations are both popular ways to increase agility and personalize user experiences. Securing endpoints is critical to ensuring that a company's differentiation isn't turned against it. That's why it's essential to safeguard applications and user data while being ready to mitigate the threat of DDoS attacks. The keys are to:

- Protect mobile apps and APIs from emerging threats like credential stuffing
- Stay ahead of the doubling of DDoS attack sizes
- Migrate toward a zero trust security architecture using a security service in the cloud

> Modern security technologies will help firms establish security architectures which are fit for purpose for the mobile and cloud era in computing and a new age in data compliance …. [17]
>
> – **Nicholas McQuire**, Vice President, Enterprise Research, CCS Insight

Embrace The Power of Zero Trust

A zero trust security architecture operates on the principle of "never trust, always verify" – introduced by Forrester Research – with the goal of addressing the shortcomings of traditional perimeter-based security in a hyperconnected world.

Akamai's cloud delivery platform, the world's largest and most trusted, is designed to empower organizations to deliver superior and secure digital experiences. It provides numerous performance and security solutions that are seamlessly integrated into the platform. This means businesses can continue to leverage the platform at every stage of their digital maturity. These solutions also support the trends above to help accelerate digital strategies.

17) CSO, What is security's role in digital transformation? March 14, 2018

Conclusion

Site and application availability isn't enough in today's digital economy – an alternative is just a few clicks away when experiences fall short. Today's prospective and existing customers expect fast, secure, personalized digital experiences.

For a company to thrive, it must innovate in delivering customer experiences while keeping those interactions secure. Given the potential damage of a major breach, it's understandable that most companies prioritize digital security over digital experience. But by failing to strike the right balance, they miss major business opportunities.

Companies must find the balance between digital experience and cybersecurity. Companies that do this well create a virtuous circle of interaction with customers.

By taking advantage of solutions such as Akamai's cloud delivery platform, IT leaders position their companies to maintain that essential balance – and drive ever-higher levels of trust and revenue.

Visit this resource page to learn more about how your organization can achieve the right balance of digital experience and security. To find out where your organization stands when it comes to digital maturity, **take the self-assessment**. You'll get customized results and recommendations that provide insights into your organization's readiness for digital business success. To raise your digital maturity, you can take advantage of Akamai's cloud delivery platform to quickly, reliably, and securely deliver the digital experiences your customers value, enjoy, and trust.