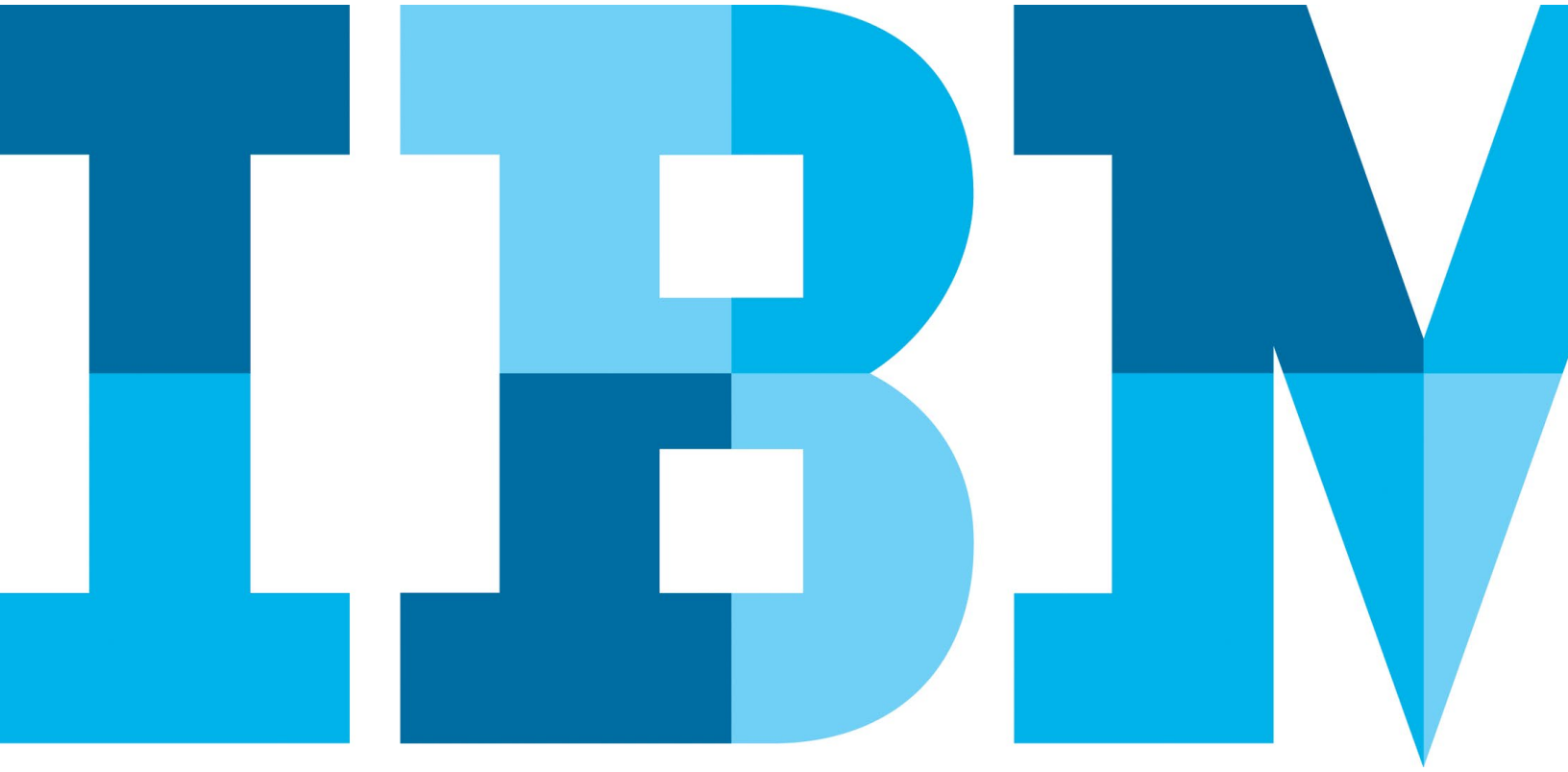
August 2016

Secure your data to build your digital business

Speed your time to market, improve your customer experience and reduce risk with a multi-channel solution from IBM



IBM

Introduction

In the era of digital business, the ways in which companies and their customers seek and consume information, make purchase decisions, and buy and sell goods and services has undergone rapid change. To remain competitive, organizations must now focus more intensely on the quality of their interactions with customers and business partners, and innovate across more channels than ever—via web and mobile platforms, in the cloud, and through applications and services made possible by application programming interfaces (APIs). As an enabling technology, APIs are rapidly making this new digital economy and the accompanying opportunities for growth not only increasingly possible but more pervasive every day.

Yet along with new opportunities, these innovations also bring new risks. How can your organization be open to change, yet remain secure? How can you protect your business workloads, data and application infrastructure? How can you add the capability to support new services for customers and integrate the necessary technologies with your existing infrastructure?

Success in the digital economy requires organizations to transform their client and business-to-business interactions by delivering a secure experience across a diverse ecosystem. This white paper explores how organizations can meet the security challenges of the digital economy—and how a secure, multichannel gateway that supports participation in that economy through five key scenarios can help securely meet rapidly changing business needs at every interaction.

The brave new world of a digital economy raises new security concerns

Businesses of all sizes now offer API-based applications and services through mobile, web and cloud channels to drive new sources of revenue, build more efficient and effective business-to-business partnerships, and acquire and serve customers. Nearly 70 percent of US organizations, in fact, report using APIs to attract customers. What's more, almost 60 percent of organizations say they are using APIs to improve time to market. Almost 50 percent report using APIs to drive innovation and generate revenue.[1]

But as APIs are increasingly interwoven with mobile and cloud platforms to deliver application services, security becomes an increasing concern. That's because as the digital economy grows, enterprise security must grow and adapt with it. The explosive growth in data, ubiquitous use of mobile devices and emergence of the Internet of Things (IoT) make security a constant and ever-changing concern. And the all-encompassing, multichannel nature of today's digital economy—including mobile computing, the cloud, APIs, business-to-business interactions and web services—requires both close attention and powerful tools to ensure secure operations.

APIs: Meeting the need for security amid business transformation

Rapid changes in technology and commerce are driving the digital economy, in which businesses provide services when and where customers want them. To remain competitive and create new routes to market, organizations are delivering unique experiences by using APIs to unlock the value of existing assets, historical information and business processes, as well as to harness customer context found in social media, mobile applications and the IoT.

The shift to a digital economy, however, opens up new risks and raises questions about how to speed innovation, reduce time to market and drive competitive advantage while ensuring the security of data, transactions and business processes. As APIs expose

back-end systems and data to users who can range from a handful of trusted business partners to a loosely organized community of developers to thousands or millions of unknown customers, the need to keep business resources secure and highly available becomes more critical than ever before.

Mobile: Ensuring security for users and the enterprise alike

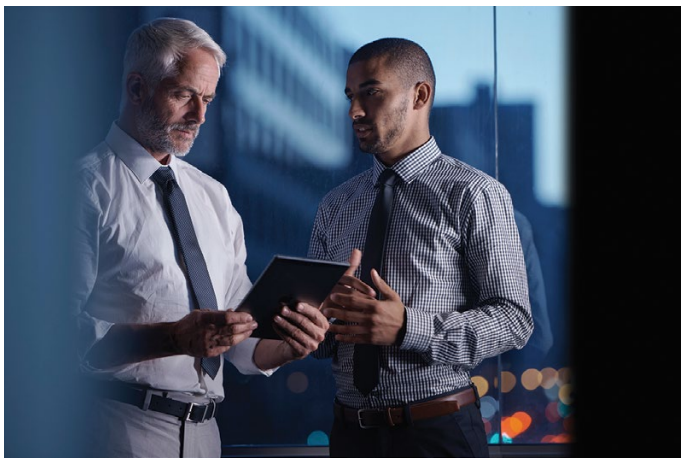
By now, mobility is a key element in the revenue growth strategy of many organizations. Business partners and customers alike expect their mobile experience to be as rich as their web experience. Many employees expect bring-your-own-device (BYOD) policies that allow them greater flexibility, connectivity and ease of use on the job. But the user experience requires security for sensitive data such as credit card information. And it requires that the enterprise protect its resources with capabilities such as multi-factor authentication.

What's more, since mobile transactions flow through many individual server instances before reaching their ultimate destination, the mobile application that originated the request cannot guarantee the confidentiality and integrity of the message unless it is digitally encrypted and signed at the message level. In order to be successful in an increasingly mobile world, organizations are looking to secure sensitive data in mobile transactions, including the ability to decrypt, encrypt, sign and verify processing actions.

Cloud: Securing and optimizing applications to grow business

The end user neither knows nor cares whether a connection to a business service runs through the cloud or an on-premises enterprise data center. But to the enterprise, the path a connection takes to reach its resources and data is a critical concern. When done correctly, utilizing a cloud deployment can help speed digital innovation and transformation, helping the enterprise create new markets more quickly at a lower cost by securely unlocking digital assets to drive more customer value and business growth.

However, government and industry regulations and data privacy concerns remain a hurdle in an enterprise's move to public cloud technologies. As a result, hybrid cloud integration is becoming a common way to provide secure access to sensitive data hosted within enterprise data centers. The hybrid approach can enable an organization to gain the elasticity and cost benefits of running workloads in the cloud, while still protecting access to sensitive data.



Business-to-business: Reaching new partners and new markets

Electronic interaction between business partners is nothing new. For example, a company can set up supply chain automation that allows them to exchange orders with their suppliers and allows the suppliers to send them invoices in response. This is a proven scenario that demands rapid transmission, effective management, smooth operations and strong security—the final factor being extremely important, as transactions typically involve sensitive information such as financial data and intellectual property.

The classic business-to-business interaction begins to shift, however, in the digital economy. And as interactions leverage APIs, mobile and cloud technologies, two concerns emerge. In an environment where back-end systems are more open and business information is more readily shared, the longstanding need to connect organizations securely with the necessary authentication, authorization and security management is amplified. At the same time, a newer concern emerges—the need to communicate across the diverse protocols and standards that these business environments employ. Organizations need solutions that will ensure that the necessary communications occur—or they'll be limited in their quest to gain new partners and grow business. And they need solutions that can keep communications safe—companies that open their resources for the use of APIs may also open themselves and their partners to risks such as malware or cyber attacks if strong security is not in place.

Web services: Confidently delivering a secure user experience

Organizations are reliant on web services for a vast amount of their contact with customers and partners. The web now provides a highly interactive experience, so security must have multiple layers. The business must be confident, as a result, that it knows who the message is from, can ensure the integrity of the message during transactions, and can make sure communication is safe from digital eavesdropping in transit.

With the delivery of services from back-end systems of record to front-end systems of customer engagement, organizations can provide more personalized customer experiences. As a result of these rapid changes, many organizations have found themselves with disparate security silos that prevent the free flow of information—adding cost and complexity, and slowing organizational responsiveness.

Amplify and simplify security with a multi-channel security gateway

While firewalls provide lower-level protection, the demands of the new digital economy require a more specialized solution capable of handling today's wide range of application workloads. Acting as a policy enforcement point, this type of solution provides consistent, end-to-end security for transactional workloads, regardless of the business channel they are coming through.

Such a solution can reduce infrastructure complexity and lower operating costs—while improving the user experience and helping scale the back-end IT infrastructure. An effective multi-channel gateway can secure, control, integrate and optimize across the API, mobile, cloud, business-to-business and web services scenarios. Such a gateway provides:

- *Security:* Encryption and decryption, message filtering, validation and digital signatures are critical when APIs expose applications, data and services for new channels of engagement.
- *Control*: Policy-based management helps enforce consistent governance, security and controls across all channels and workloads.
- *Integration*: The ability to securely transmit data over a variety of protocols and standards provides important integration with end users and partners that is critical for success in the digital economy.
- *Optimization*: Decoupling the enforcement of security and other policies from the underlying application, offloading repeatable tasks and ensuring intelligent load distribution enables systems to scale and helps prevent bottlenecks and failures.

A multi-channel gateway from IBM supports the digital economy—securely

Offering multiple deployment options to fit a wide array of business needs, IBM® DataPower® Gateway is a multi-channel solution that provides an integrated set of capabilities designed to help organizations thrive in the digital economy. Whether in an IBM or heterogeneous back-end environment, DataPower Gateway provides the same robust security, integration, control and optimized access for a full range of mobile, cloud and web workloads—in a single, purpose-built network device. With this solution, organizations can eliminate unwieldy point-to-point connectivity and streamline the flow of secure data into and out of its infrastructure.

IBM DataPower Gateway uses policy-based security that makes it easier for IT to ensure consistency across all channels and radically reduce risk. As the first point of entry and egress for data moving in and out of the enterprise, DataPower Gateway makes it easier to gather essential information to feed data and analytics systems. What's more, by consolidating security across channels, the solution makes it possible to simplify the network, reduce development costs and speed delivery of new services.

Conclusion

In the digital economy, organizations of all sizes are working to provide more personalized interactions with their partners and customers than ever before—regardless of the access point. The extreme speed with which this has occurred has resulted in new risks to systems and sensitive data.

These key priorities—keeping systems, processes and data secure while enabling the organization to be nimble and responsive—don't have to be incompatible. With a robust gateway solution such as DataPower Gateway, the enterprise can secure, control, integrate and optimize transactions across API, mobile, cloud, business-to-business and other channels.

For more information

To learn more about IBM DataPower Gateway, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/software/products/en/datapower-gateway

Additionally, IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit: **ibm.com**/financing

IBM Cloud
Route 100
Somers, NY 10589

Produced in the United States of America
August 2016

[1] Amy Konary, "The Mobile Application Ecosystem in a Post-API Economy World," *IDC*, March 2015.

Please Recycle

IGW12349-USEN-00