Sponsored by

infor

How Cloud-based ERP Can Help Businesses Balance Innovation Goals and Security Requirements

June 2019

Authored by

SMB Group
Actionable Market Insight

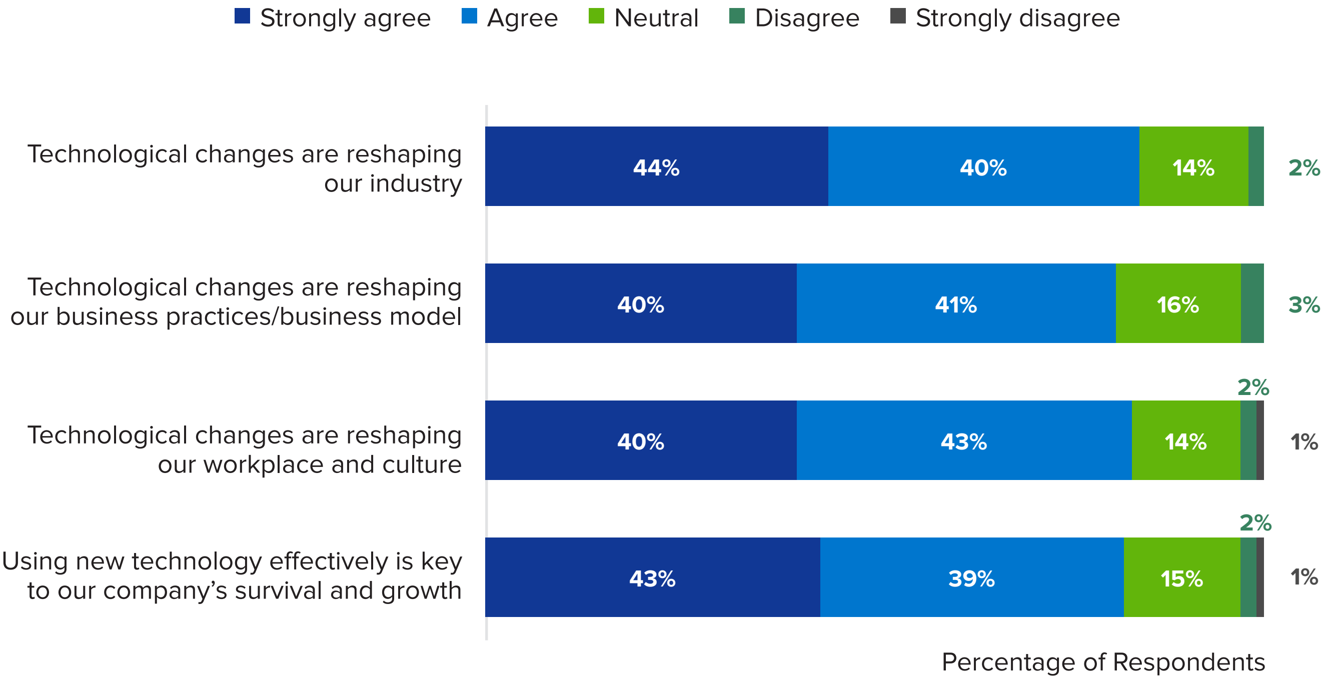
INTRODUCTION

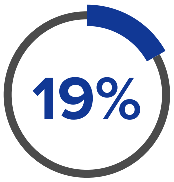
Digital data has become the most valuable resource in our modern world. But unlike natural resources, the quantity of this virtual reserve is expanding at a mind-boggling rate. Amid this data explosion, the ability to harness data for operational, market, and competitive advantage increasingly defines a business's success or failure.

Conceptually, small and medium businesses (SMBs) understand this. More than three-quarters of them agree that using new technology effectively is key to business growth and survival. However, fewer than one-quarter of SMBs strongly agree that they have a well-defined digital strategy to help them to achieve their goals in this area.[1]

[1] SMB Group 2019 SMB Digital Transformation Study

SMB CHANGES ARE COMING, BUT MANY COMPANIES ARE NOT WELL PREPARED





of SMBs strongly agree that their company has a well-defined digital business strategy

As SMBs become more dependent on technology, the risk of cybersecurity breaches increases. Technology makes it easy to transmit data across wired and wireless networks; consequently, sensitive data is distributed beyond corporate firewalls to many devices and clouds. Businesses must not only protect more and more data but also secure and protect it in more places to give workers the anytime, anywhere access they need to get their jobs done.

This requirement makes it difficult to balance the need to innovate with the need to protect and secure company, employee, and customer data. Even large corporations with dedicated security operations centers struggle to counter the metastasizing cyber threat. For SMBs—which often lack security expertise and resources—these challenges can seem overwhelming. In fact, SMB Group research shows that SMBs rank protecting company information from security threats as their top technology challenge.[2]

TOP TECHNOLOGY CHALLENGES

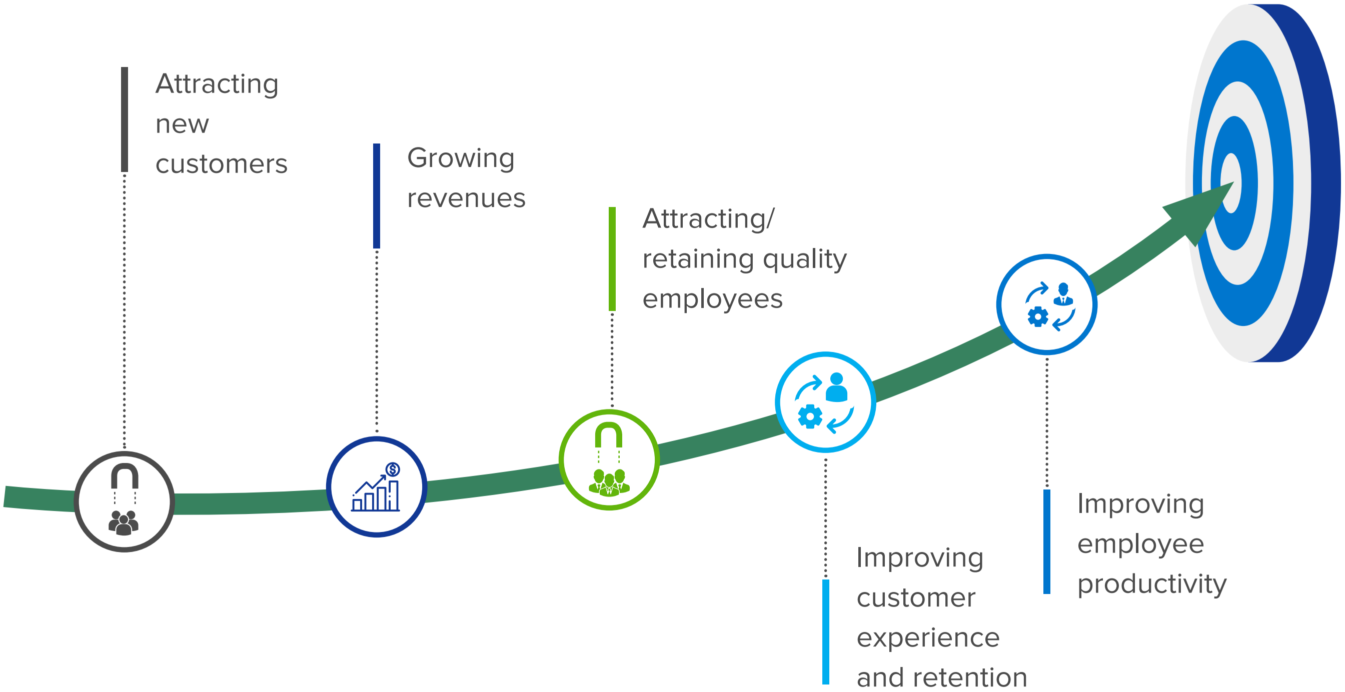
While there is no easy solution to this dilemma, cloud-based ERP solutions can help SMBs balance the dual requirements for innovation and security. IT and business decision makers may worry about placing company applications and data in the cloud, but the truth is that leading cloud service providers can often deliver security capabilities and expertise far beyond those that most SMBs can achieve with their limited in-house resources.

USING ERP TO LEVEL THE PLAYING FIELD

SMBs recognize that the rules of business success are changing fast—and that they need modern, flexible technology solutions to attract customers and grow revenues, recruit and retain talent, improve the customer experience and more.[3]

[2] SMB Group 2019 SMB Digital Transformation Study
[3] SMB Group SMB 360: Connecting the Dots Between Business and Technology Study

TOP SMB BUSINESS GOALS

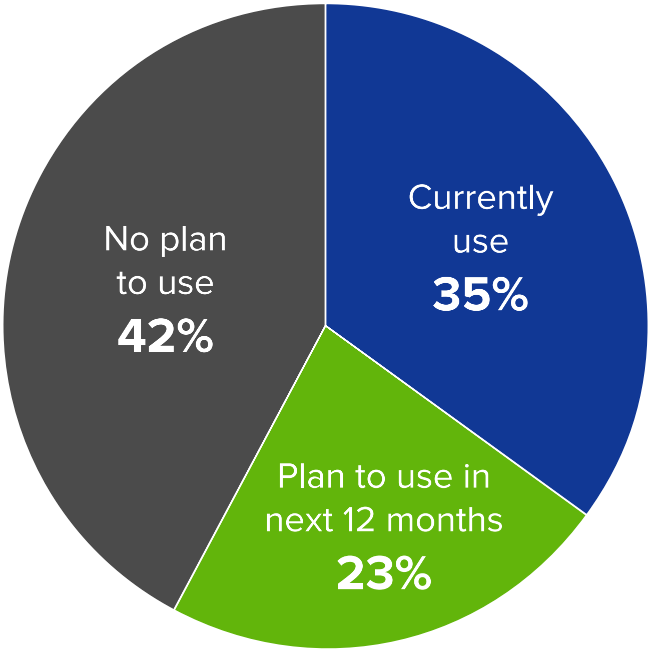

Attracting new customers
Growing revenues
Attracting/ retaining quality employees
Improving customer experience and retention
Improving employee productivity

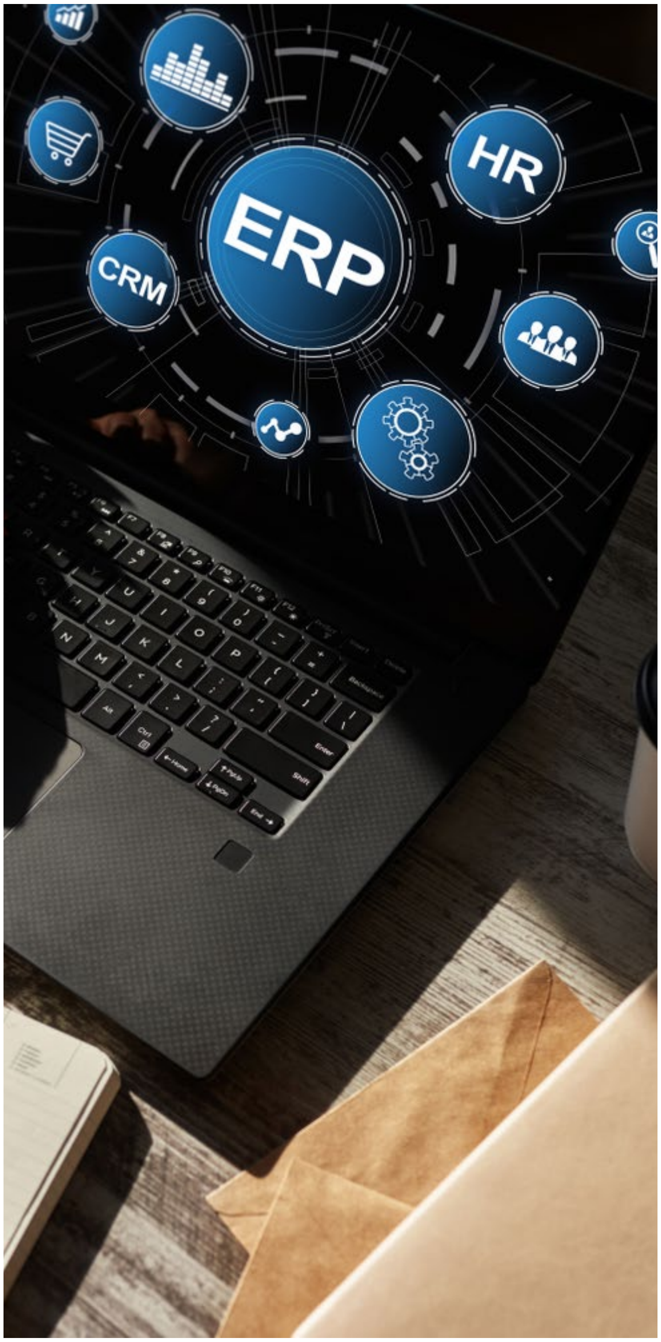
The right technology foundation can help businesses automate and streamline workflows; provide insights to improve customer, supplier, partner and employee interactions and processes; and efficiently and flexibly scale operations.

While using multiple disconnected point solutions (e.g., financials, human resources, supply chain and analytics) may work when a business is very small, this approach can't support or fuel business agility and growth. Enterprise resource planning (ERP) solution suites help companies integrate workflows across the business—streamlining operations and providing the visibility that businesses need to make better decisions—and help to level the playing field against both large, established corporations and disruptive startups.

Consequently, 23% of SMBs that don't currently use ERP are planning to deploy a new ERP solution.[4]

SMB USE OF AND PLANS FOR ERP SOLUTIONS





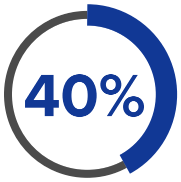
Furthermore, 40% of SMBs that already use ERP are planning to replace their existing solution. Top reasons for considering replacement include the need for easier-to-use and less costly solutions; the need for better intelligence and reporting; the desire to move to the cloud; the need for a more innovative solution; and requirements for better integration with other solutions.[5]

[4] SMB Group SMB 360: Connecting the Dots Between Business and Technology Study

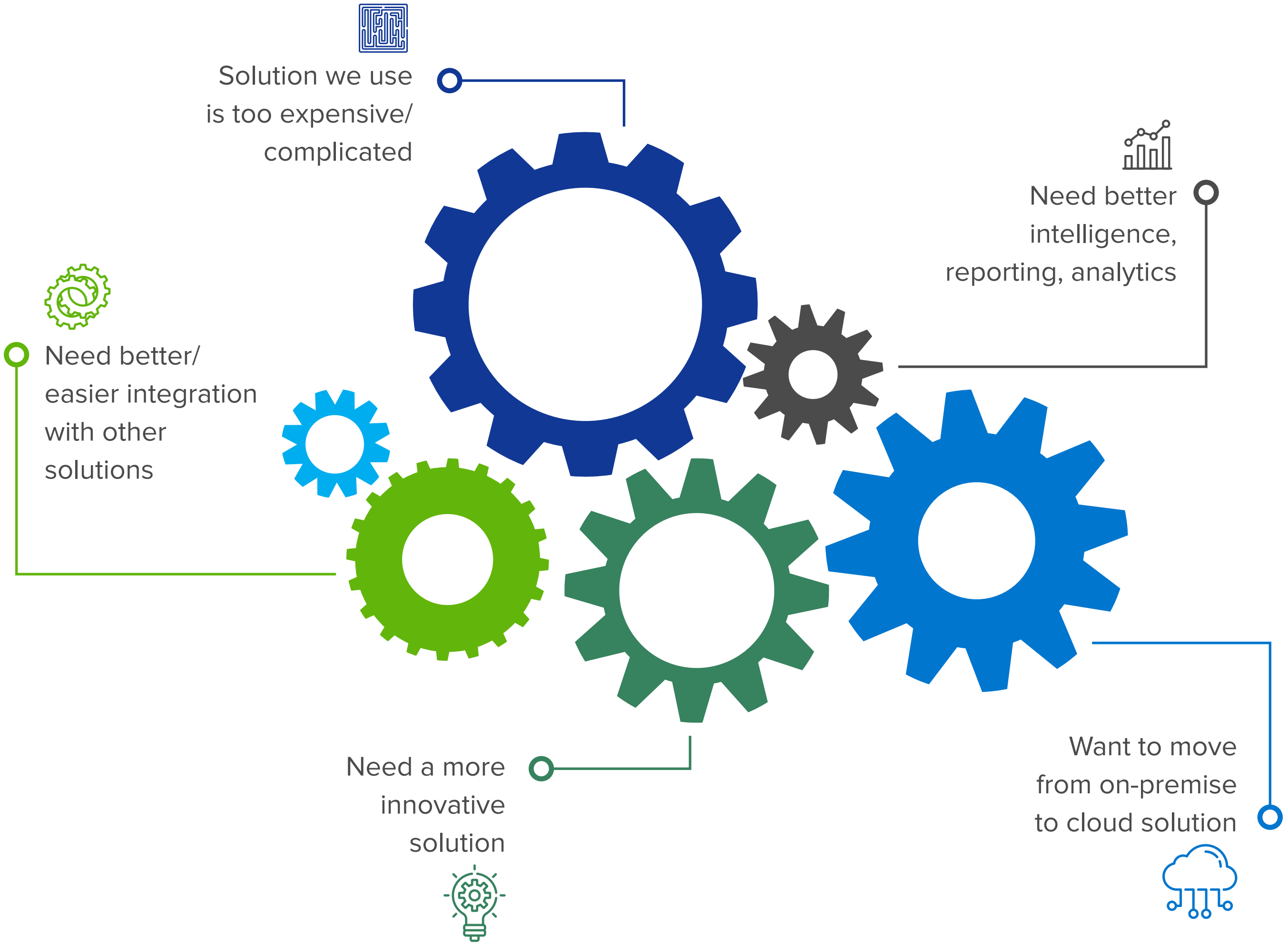
[5] SMB Group SMB 360: Connecting the Dots Between Business and Technology Study

SMB PLANS FOR AND DRIVERS TO REPLACE ERP

Top Reason SMBs are Considering Replacing Their Current ERP Solution



of SMBs currently using ERP are considering replacing the application they use for this in the next 18 months



Solution we use is too expensive/ complicated

Need better intelligence, reporting, analytics

Need better/ easier integration with other solutions

Need a more innovative solution

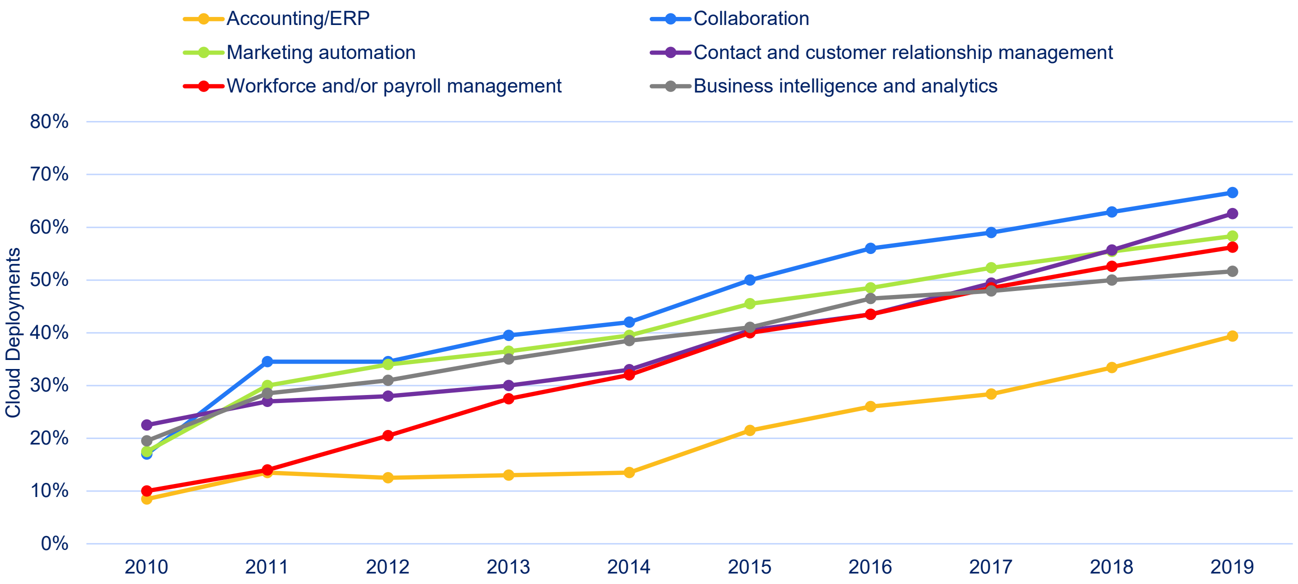
Want to move from on-premise to cloud solution

CLOUD ERP ADOPTION IS RISING

It's not surprising that many SMBs are considering replacing their existing ERP system with a cloud-based ERP alternative. SMBs are increasingly finding that cloud-based solutions offer an easier, faster and less resource-intensive way to deploy and manage business solutions. While ERP has lagged other functional areas in terms of cloud adoption, it is starting to catch up as businesses get more comfortable with the cloud model.[6]

[6] SMB Group Survey Studies, 2010-2019

CLOUD ADOPTION CONTINUES TO RISE



Cloud-based ERP suites integrate core business functions to create a "single source of truth" database with real-time, consistent, and accurate data. They also offer a common, web-based interface across functions, which helps to speed training and boost productivity.

In addition, cloud ERP vendors are building new technologies—such as artificial intelligence (AI), machine learning (ML), natural language processing (NLP) and the Internet of Things (IoT)—into their solutions. Such initiatives are providing SMBs with a natural on-ramp to take advantage of these new technologies within the ERP interface they already know and use.

NAVIGATING THE CYBERSECURITY LANDSCAPE

No company, large or small, wants to see its name in the news as the latest victim of a cyber breach. In the best-case scenario, such a breach merely tarnishes a company's reputation. More dire consequences include everything from stolen customer data to intellectual property theft to regulatory and legal consequences.

But understanding the negative impacts of cyber attacks is one thing. Defending against them is another thing altogether. Cyber criminals increasingly exploit the same digital technologies being created for legitimate business purposes to diversify, expand, and increase their avenues of attack. For instance, while legitimate organizations use AI and analytics as powerful business tools, cyber criminals can use them to supercharge the scope and effectiveness of digital assaults.

This expands the potential for threats well beyond viruses and simple malware exploits. For example, consider the following:

- Distributed denial of service (DDoS) attackers can build massive traffic-spewing bots that can commandeer tens of thousands of poorly secured IoT devices.
- Phishing attacks use sophisticated social engineering ploys to trick email recipients into opening destructive attachments or linking to malevolent websites, and a “vishing” voice fraud variant is on the rise, with callers using similar techniques to elicit sensitive information via phone calls.
- Ransomware criminals encrypt critical data, which may or may not be “freed” if the victim pays the attacker a ransom in crypto currency.

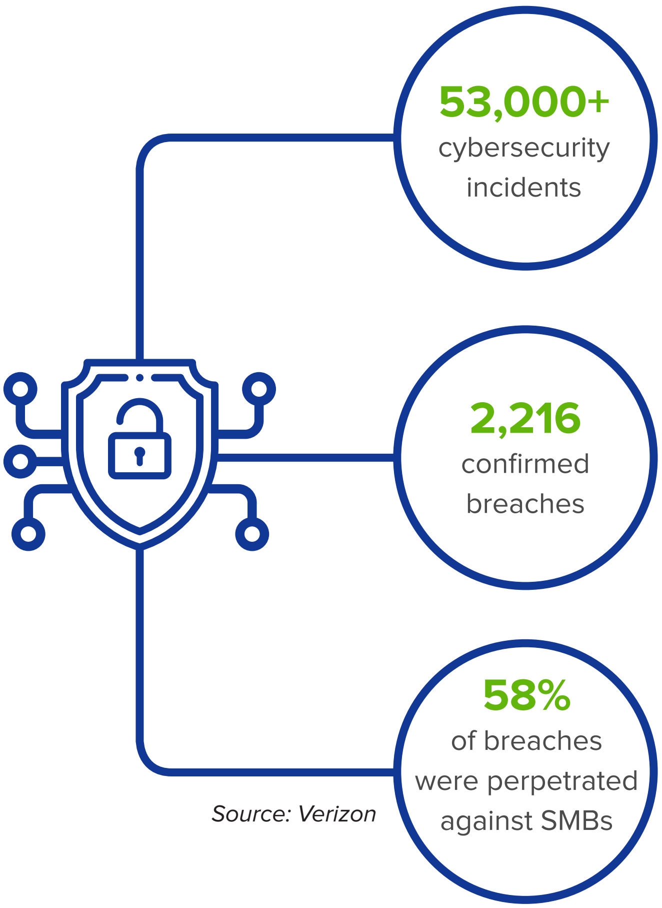
Many SMBs think that they’re too small to attract the attention of these and other cyber attackers. However, *Verizon’s 2018 Data Breach Investigations Report* categorized more than 53,000 cybersecurity incidents and 2,216 confirmed breaches and found that small businesses were the victims of 58% of the breaches. According to the study, breaches hit every business sector, from financial services to healthcare to manufacturing and distribution.

Sadly, SMBs that want to mitigate these threats by hiring cybersecurity experts are likely to be disappointed. Demand for security professionals has outpaced supply for years, and the prospects of reducing this talent gap are dim. *Cybersecurity Ventures* predicts there will be 3.5 million unfilled cybersecurity positions by 2021.

SECURITY—A SILVER LINING IN THE ERP CLOUD

Security concerns have hindered cloud adoption in the past. However, leading cloud business solution providers can equip their solutions with sophisticated security safeguards that most SMBs would be hard-pressed to match in an on-premises deployment. Because they are developing, running and managing applications for thousands or even tens of thousands of customers, cloud ERP vendors must make their systems insusceptible. And, because they can amortize costs over a large customer base, they can afford to hire security specialists that most SMBs would never be able to bring on board. This means they can design security into their development and release processes and develop capabilities to constantly monitor, scan, and mitigate common vulnerabilities and potential intrusions.

2018 Cybersecurity Statistics



Source: Verizon

While SMBs may not have great visibility into behind-the-scenes development processes, they can gain some insight by examining the security characteristics of the solutions themselves. For instance, does the application prevent you from typing bad information into its fields? If so, that’s one indication that security was top of mind during the application’s development and testing phases. Likewise, an application that runs multi-factor authentication as its default setting indicates that the software developers were trying to code in some best security practices.

Of course, "security" encompasses more than just defenses against cyber attacks; it also means that the vendor can guarantee uptime levels to ensure that the services and data you need are available.

Another security-related concern—and one of growing importance—is compliance with all pertinent regional government and industry regulations. These and other factors should be part of a comprehensive security assessment when SMBs evaluate cloud-based ERP solutions.

NOT ALL CLOUDS ARE CREATED EQUAL

When evaluating the cybersecurity capabilities of cloud-based solutions, it's important to first understand that the "cloud" encompasses a wide range of deployment models and services. There are many differences—including the scope of security coverage—among infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS) and software-as-a-service (SaaS) offerings, for example. The security features and capabilities delivered by these and other "as-a-service" providers and models vary considerably. For that matter, so does the balance of security responsibilities shared between cloud service providers and their customers.

Customers that are simply "renting" cloud-based infrastructure from an IaaS provider will continue to shoulder the bulk of the security burden. For instance, the customer will need to implement an identity and access management system, install security patches as soon as they become available and perform all other security functions associated directly with the application itself.

By comparison, the SaaS model can provide a more comprehensive security solution—at least if it's well architected and managed. SaaS providers often provide built-in solutions for everything from data encryption to user authentication and access. In addition, SaaS providers will often upgrade their security infrastructure with the newest generation of security controls more quickly than many individual companies can justify, and they are also likely to do a better job of immediately installing patches and performing other day-to-day security hygiene tasks.

Significant variations exist within the SaaS community of solutions, of course. Some SaaS providers own and operate their own infrastructure on which the SaaS applications run, while others deploy their solutions on third-party cloud infrastructure, such as that provided by Amazon Web Services (AWS) and others.

CLOUD ERP IS JUST ONE PART OF THE SECURITY PUZZLE

While cloud ERP solutions can lighten the security burden, they can't eliminate it.

SMBs should start by understanding the security features their ERP cloud service provides and ensuring they take advantage of the solution's controls and safeguards. For instance, many SaaS solutions support multi-factor authentication and full data encryption—both at rest and in transit—but these features will only work if they are turned on.

Next, if there is more than one provider delivering different layers of the cloud solution, the customer must understand how the partnership works. In addition, the customer must ensure that security roles and responsibilities are clearly delineated and defined among providers. Without such clarification, it's easy for critical functions to fall through the cracks, resulting in hidden vulnerabilities. Any reputable SaaS provider should be able to precisely describe its own cybersecurity capabilities and areas of coverage, those provided by any of its cloud partners and the security responsibilities that belong to the customer.

Relative to that last point, the SaaS provider should also be able to help customers understand and implement any additional security controls for the ERP application and data beyond what the provider typically can offer. Even the best technical defenses can be undermined—and often are—by careless user actions such as opening malicious attachments and clicking on dangerous links in phishing emails. SMBs must train employees to follow good cybersecurity practices.

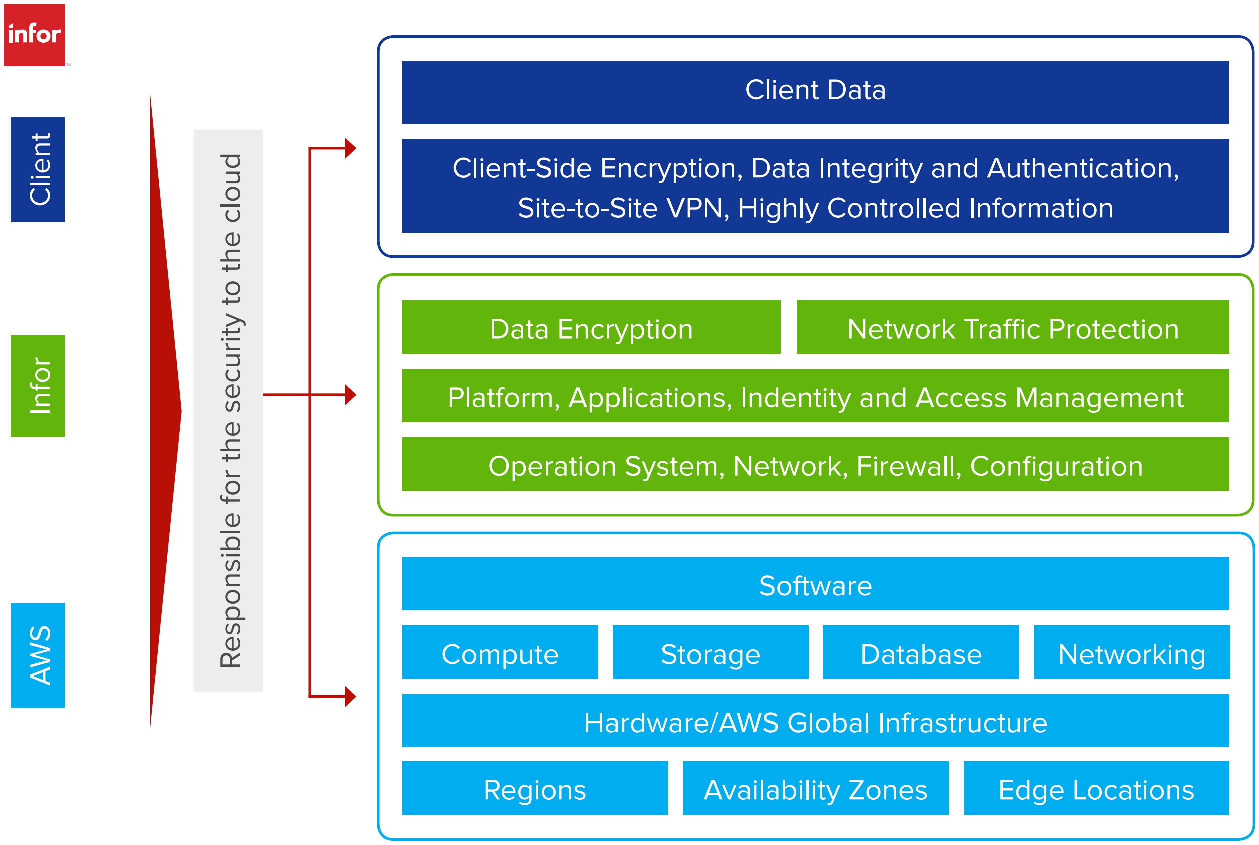
Finally, SMBs should engage in a corporate-wide security audit—beyond the ERP application itself—to identify the biggest gaps in their overall security strategy. Although it is impossible to ward off every conceivable breach, SMBs should deploy data center and endpoint solutions to protect their most valuable digital assets.

INFOR CLOUDSUITE DELIVERS "DEFENSE IN DEPTH"

Infor, a leading provider of cloud ERP for manufacturing, distribution, healthcare and hospitality industries, adheres to a "*defense in depth*" strategy throughout the design, deployment, maintenance, and updating of its CloudSuite ERP offering. The company's dedicated Infor Cloud security staff work 24x7 to monitor the cloud environment, respond to any cyber threats that emerge and contribute a significant portion of the comprehensive security defenses it shares with its partners and customers.[7]

[7] Infor

SHARED SECURITY RESPONSIBILITY IN A CLOUD-BASED DEPLOYMENT MODEL


infor
Client
Infor
AWS
Responsible for the security to the cloud
Client Data
Client-Side Encryption, Data Integrity and Authentication, Site-to-Site VPN, Highly Controlled Information
Data Encryption
Network Traffic Protection
Platform, Applications, Indentity and Access Management
Operation System, Network, Firewall, Configuration
Software
Compute
Storage
Database
Networking
Hardware/AWS Global Infrastructure
Regions
Availability Zones
Edge Locations

Source: Infor

Part of Infor's multi-layered security commitment involves working closely with its cloud infrastructure partner, AWS. In addition to its own application's security functions, Infor leverages *AWS security capabilities*. Infor's and AWS's security experts are in continual contact and team up when necessary to jointly counter any security threats.

Infor's CloudSuite complies with the SSAE 18 Service Organization Control standards and also supports a large number of regulatory compliance standards. These include broad standards such as the European Union's General Data Protection Regulation (GDPR) and industry-focused standards such as the Health Insurance Portability and Accountability Act (HIPAA).

The bottom line is that a security-focused cloud ERP provider such as Infor can help SMBs harness the technologies they need to grow their businesses and to do so in a more secure manner.

PERSPECTIVE

Balancing the need for business innovation with the need for digital security has never been easy—and it's only becoming more difficult in a world where business results are increasingly entwined with technology. SMBs must streamline critical business processes and harness the growing volumes of data they produce and access to stay ahead of the market and their competitors—all while keeping that data safe.

Cloud ERP has always offered SMBs a faster, easier route to deploy and reap value from sophisticated business solutions; on-demand scalability to facilitate business growth; and the financial benefits of a subscription model. Now, SMBs increasingly recognize that cloud ERP can also help them run their business applications more securely—enabling them to focus more time, energy, and resources on driving the innovation required to increase competitiveness and profitability.

ABOUT INFOR

Infor is a global leader in business cloud software specialized by industry. With 17,300 employees and over 68,000 customers in more than 170 countries, Infor software is designed for progress. To learn more, please visit www.infor.com/products/erp.

ABOUT SMB GROUP

SMB Group is an industry research, analysis and consulting firm focused on technology adoption and trends in the small and medium business (SMB) market. Founded in 2009, SMB Group helps clients to understand and segment the SMB market, identify and act on trends and opportunities, develop more compelling messaging, and more effectively serve SMB customers.