McKinsey & Company

Risk Practice

Securing software as a service

Here is how SaaS providers can meet the security needs of their enterprise customers.

by Rich Cracknell, James M. Kaplan, Wolf Richter, Lucy Shenton, and Celina Stewart

September 2019

Companies are rapidly adopting software as a service (SaaS) in place of purchasing commercial off-the-shelf software (COTS). Companies using SaaS rely on SaaS vendors to host their applications in the cloud instead of running them in their own data centers. Industry analysts estimate that the SaaS market will grow by more than 20 percent annually, reaching nearly $200 billion by 2024, a level that would represent nearly one-third of the overall enterprise-software market. With enterprise values for SaaS businesses reaching approximately seven times forward revenue, software companies are racing to convert from on-premises to SaaS-based delivery models.[1]

Most companies, therefore, will eventually confront the cybersecurity risks inherent in the SaaS approach. These are different risks from those posed by on-premises COTS. In building COTS, the vendor takes responsibility for removing security vulnerabilities from the application code. The customer, however, installs the software, configures it, and takes responsibility for running it in a secure infrastructure. For SaaS offerings, the vendor takes on many of the security responsibilities previously assumed by the customer.

Companies do not always feel comfortable with the indirect relationship to cybersecurity risk that SaaS presents, mediated as it is through vendor-based protections. More important, SaaS vendors have not always ensured that their products meet their customers' security requirements. That is the story that emerged from our survey of cyber professionals from companies seeking to adopt SaaS solutions.[2] Their responses also provide insights into how enterprises should think about security in an SaaS world and important clues for SaaS vendors on how to earn the confidence of their enterprise customers.

The security challenges of software as a service for adopting companies

Our survey polled chief information-security officers (CISOs) and other cybersecurity professionals from more than 60 companies of varying size in a range of industries. We wanted to understand how companies experienced SaaS offerings and how they responded to security challenges. Almost universally, respondents confirmed what we had suspected: they have increased their focus on security for SaaS offerings, emphasizing capabilities at the intersection of the vendor's and their own security environments. They expressed a fair amount of frustration with shortcomings in vendors' cybersecurity capabilities, which often caused delays in contracting and implementation. In their view, SaaS vendors need to take a much more customer-centric approach to security, making it easier to understand their products' security capabilities, easier to integrate them with the rest of the enterprise-security environment, and easier to configure them in a secure and compliant way.

All the companies we spoke with had already begun to make the transition to SaaS offerings. About half had used products from 20 or fewer SaaS vendors, about a quarter from more than 80. Almost all companies surveyed were deploying SaaS offerings in at least one major area, especially office automation, IT-service management, and niche business applications (Exhibit 1).

Many security executives said that their organizations were not ready to use SaaS in some critical domains, however, because of the potential risks. These include enterprise-resource-planning applications, where downtime can prevent the entire business from functioning. Similar concerns were raised for engineering- or manufacturer-related applications. For health-

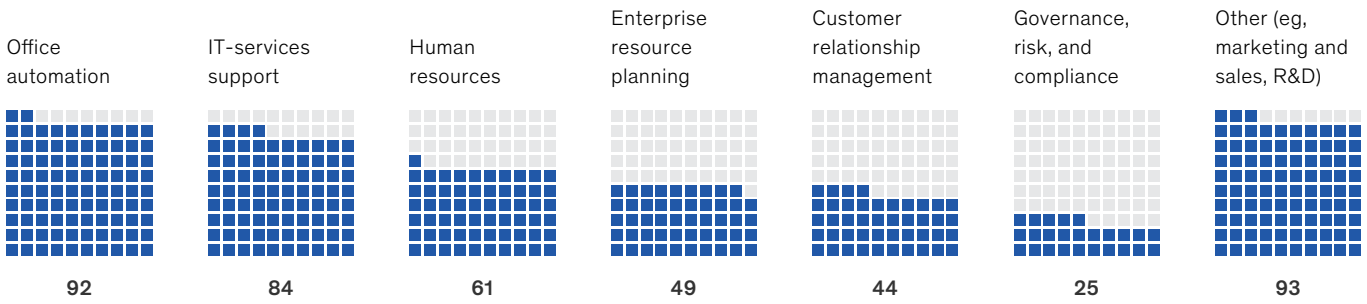
[1] KBV research cited in "Software as a service (SaaS) market to reach a market size of $185.8 billion by 2024: KBV Research," PR Newswire, December 19, 2018, prnewswire.com; *Enterprise software market research report—global forecast 2023*, Market Research Future, May 2019, marketresearchfuture.com; "Just where are SaaS companies priced after the 2018 correction?," Tomasz Tunguz, December 26, 2018, tomtunguz.com.

[2] 2019 McKinsey Customer Perspectives on SaaS Survey of chief information-security officers (and managers responsible for cloud security or vendor security) from more than 60 organizations. More than half of the participants were from companies in financial services, insurance, pharma, and health services, with the rest spread across the government, industrial, and tech sectors. Each third (approximately) of the responding companies had respective annual IT budgets of $500 million and above, $50 million to $500 million, and less than $50 million. Most respondents were from companies based in the United States. Differences in size, geography, and sector apart, however, the companies largely expressed similar concerns.

Exhibit 1

Surveyed enterprises most commonly used software as a service for office automation, IT-services support, and niche business applications.

Level of SaaS[1] adoption by usage type, % of respondents (n = 61)



[1] Software as a service.
Source: McKinsey Customer Perspectives on SaaS survey

related applications and applications that may contain M&A information, the biggest barriers to SaaS adoption concern data confidentiality.

Priorities in attempting to secure software as a service

In their relationships with SaaS vendors, most respondents use questionnaires to gauge security capabilities but criticize the approach as imprecise, incomplete, and overly time consuming. Security executives tend to focus on four key issues when confronting SaaS capabilities: encryption and key management, identity and access management (IAM), security monitoring, and incident response (Exhibit 2). Notable is that each of these issues has more to do with the interface between the customer and the SaaS provider than with the providers' intrinsic technical protections, such as code security and endpoint protection.

Encryption and key management

Applications running in the cloud and data stored there are not protected by a traditional corporate-security perimeter of firewalls and the like. As a result, security becomes essentially reliant on encryption and management of the keys that provide access to encrypted data. Our interviews revealed that most companies, especially large ones, do not entrust SaaS providers to host and manage their security keys. The majority prefer to hold their keys on premises through a hardware security module, retain management control of cloud-hosted keys, or use a combination of methods (Exhibit 3). These approaches allow companies to control access to sensitive information. It also ensures that government agencies cannot gain access to and unencrypt their data without contacting them first.

The survey further revealed that companies want a degree of sophistication in key management so that they can grant access to data for a certain period of time or revoke access quickly. This preference again emphasizes that most respondents want to exercise full control over their sensitive information.

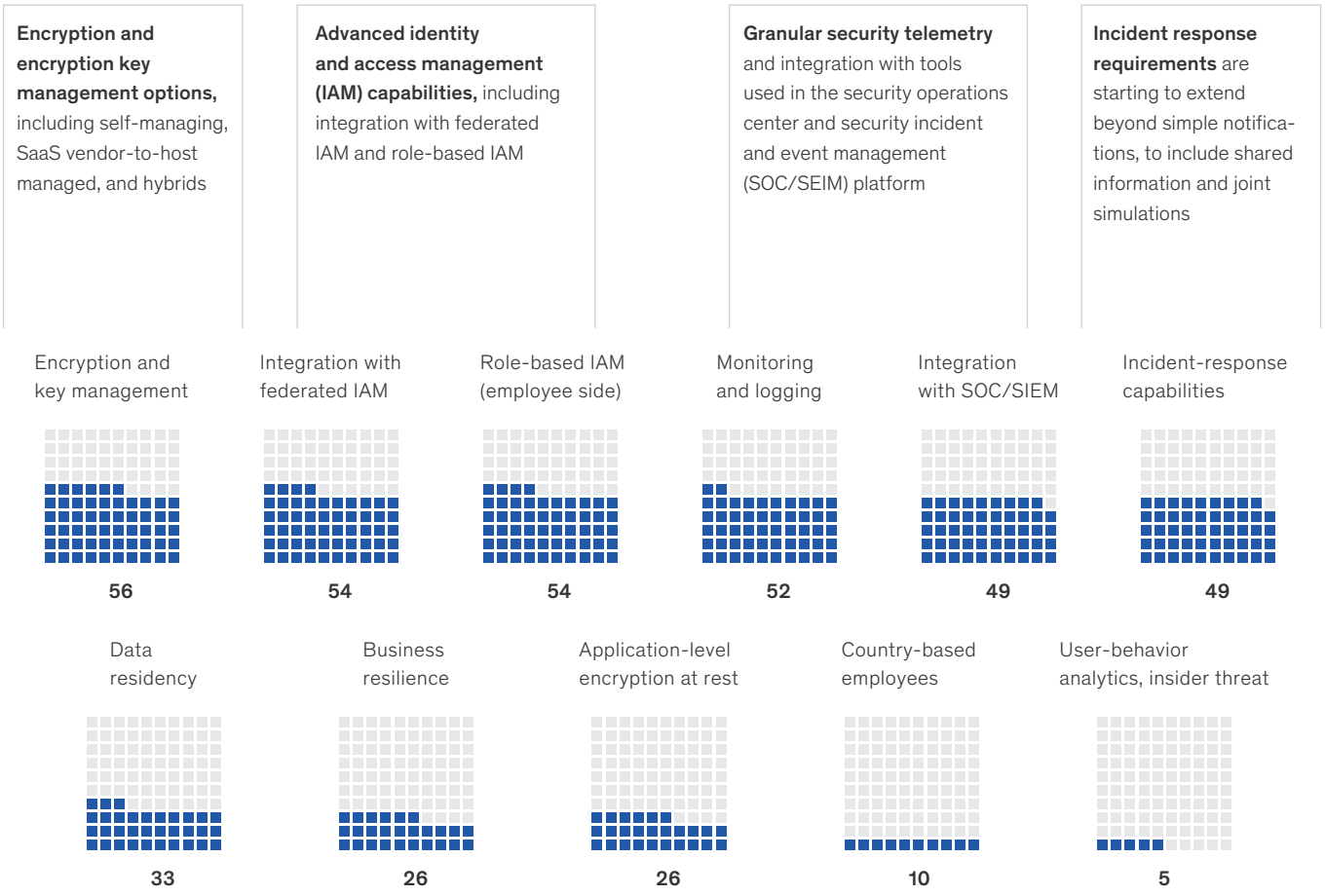
Identity and access management

Identity management is the act of confirming that each user is the person he or she purports to be. Access management is the determination that a user does or does not have legitimate rights to retrieve data or use an application. As important as both identity and access management are on company premises, they are even more important for cloud-based applications.

Exhibit 2

Enterprise customers focus on the interface between software-as-a-service providers and their own security environments.

Capabilities that respondents would like to see from SaaS[1] vendors, % of respondents (n = 61)



[1] Software as a service.
Source: McKinsey Customer Perspectives on SaaS survey and interviews with more than 60 industry leaders

Security executives emphasized that two IAM capabilities are especially important to them. First, they want tight, easily implementable integration between SaaS applications and widely adopted enterprise IAM tools. Companies deploy hundreds or thousands of applications, dozens of which are SaaS applications. They cannot expect users to memorize yet another password for each new SaaS offering that is adopted. They want to allow users to sign into SaaS applications via enterprise-wide IAM platforms, which will provide additional features like two-factor authentication. Second, they need sophisticated, role-based access management, including the ability to provide selected people with the authority to access certain data or undertake certain transactions within an application.

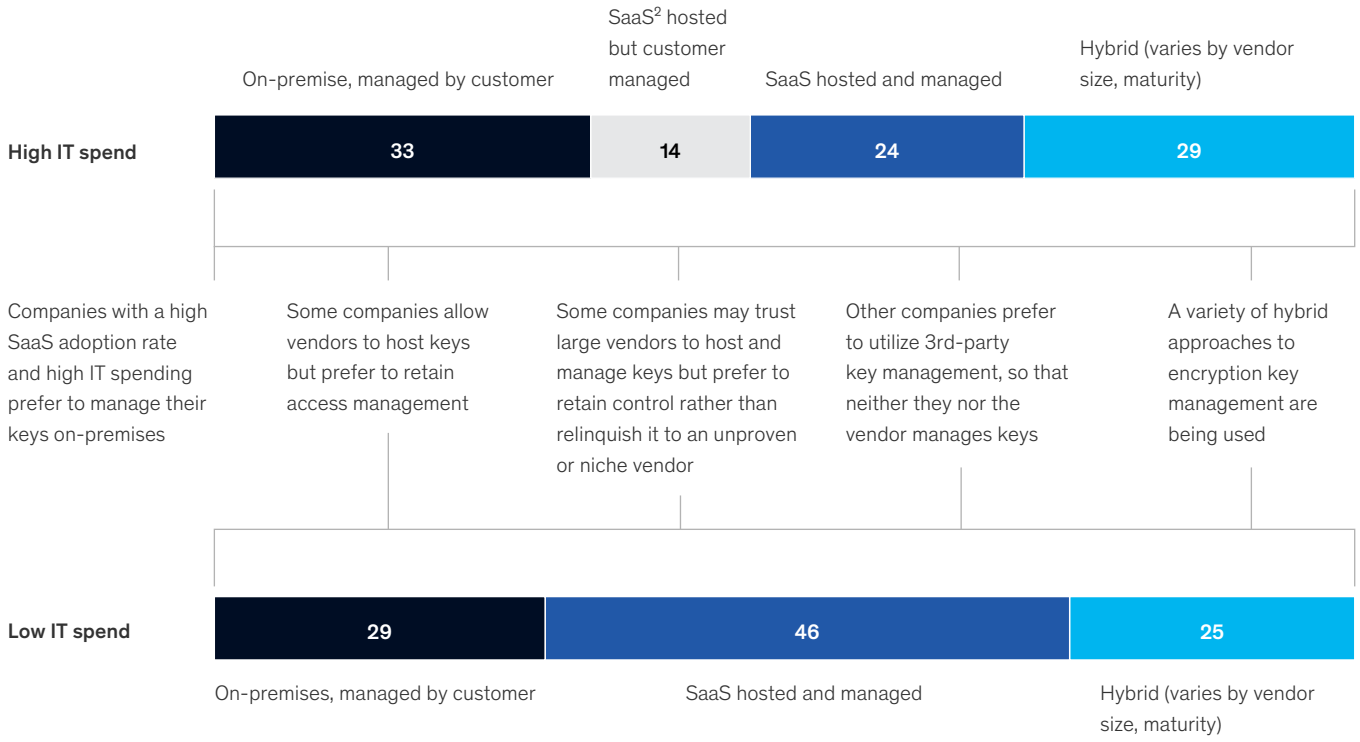
Security telemetry and monitoring

Increasingly, CISOs acknowledge that they cannot prevent every instance in which security is compromised. They therefore want the necessary transparency to identify and assess emerging security risks quickly and thoroughly. As companies adopt SaaS offerings, data from SaaS providers about usage patterns become critical to this analysis.

Exhibit 3

Most enterprises do not fully entrust software-as-a-service providers with hosting and managing encryption keys and so use different control methods.

Preferences for hosting and managing encryption keys, by level of estimated IT spending,[1] % of respondents (n = 44)



[1] All IT-spending estimates rely on information from "IT key metrics data 2019: Executive summary," Gartner, December 17, 2018, gartner.com.
[2] Software as a service.
Source: McKinsey Customer Perspectives on SaaS survey and interviews with more than 60 industry leaders

Security reporting is the baseline capability CISOs demand. They want a clear view—usually consolidated in a dashboard—of the users that have been accessing their data and what they have done with it. Without this kind of transparency, implementing even the best security concepts can be a "nightmare," as one security executive remarked.

Many security teams seek to integrate data on SaaS usage with external-threat intelligence and information from the rest of their technology environment to determine the actions they must take to protect their company. To accomplish this, the security teams need SaaS providers to offer application programming interfaces (APIs), which will allow them to pull data into their security-operations centers (SOCs) and security- incident and event-management platforms (SIEMs). As a health-services CISO explained, "On-premises security controls are getting extended into the cloud. Only a few SaaS providers allow us to pull logs to go into our SIEM." A banking CISO said, "I want to integrate with SOC/SIEM. I want something flexible enough to work with hardened SIEM tools, and something capable of integrating as well." In other words, CISOs want their vendors to make it easier to use APIs for integration. They also want timely service provision as well as accurate security information from their SaaS providers included in service-level agreements (SLAs).

Incident response

Every company can be breached. Therefore, security teams must implement tools and practices

for managing, mitigating, and resolving incidents. Naturally, security monitoring plays a significant role in this, as greater transparency enables better incident response.

Most organizations focus on SOC and SIEM integration. The more sophisticated security organizations we spoke with have dramatically broadened their incident-response requirements to include joint simulations, joint forensic activity, and intelligence sharing. One company even secured the right from one provider to send personnel to the provider's SOC in the event of a major breach.

Broader security concerns and pain points

CISOs also stated broader concerns with SaaS vendors' security capabilities. These include a lack of readiness of many SaaS offerings for integration with the company's larger security environment as well insufficient transparency on whether SaaS products meet local data-privacy requirements. A further concern surrounds the experience of SaaS sales forces, which CISOs say can be ill informed and sometimes even outwardly deceptive about security-related issues.

Integration is challenging

Nearly two-thirds of companies express frustration with the process of integrating SaaS products with the rest of their security environments. The trouble spots cited are as follows:

- lack of preexisting connectors to commonly used IAM and SIEM platforms
- insufficient functionality of APIs for obtaining the information required, especially log visibility at the platform level
- poor API documentation, confusing API-usage semantics, and a shortage of relevant code samples
- differently designed APIs for products from the same vendor
- lack of trained vendor personnel to assist in using APIs

CISOs complained of APIs that are not delivered, integration that is not achieved, even when the road map is followed, missing documentation, a lack of active support, and no vendor response when a problem develops. A biotech CISO emphasized "the lack of security monitoring: [SaaS vendors] forget about the confidentiality and integrity aspects of the monitoring."

Limited focus on data privacy

As major data breaches proliferate and regulatory attention mounts, data privacy is becoming an issue in the decision-making process for SaaS contracting and implementation. Security teams, meanwhile, find vendors scrambling to provide adequate clarity on the data-privacy protections in their offerings. One medical-products CISO pointed out that SaaS providers struggled to fulfill data-residency requirements—identifying the countries where the data are stored. Companies need to know the residency to meet local data regulations.

CISOs often cannot tell whether SaaS products properly meet new data-privacy mandates, including the European Union's General Data Protection Regulation (GDPR), Brazil's General Data Protection Law, and the California Consumer Privacy Act. Companies need to know this information to configure critical features, like encryption, data purging, and data logging, as they ensure compliance.

Respondents say that the claims SaaS providers make about product compliance are often overstated, so they don't necessarily trust them. A technology company's CISO said, "For things like GDPR, everyone is trying to figure it out; if anyone claims that they are mature in their process around

GDPR, I would question this. I would prefer a sense of openness [and] honesty around what SaaS providers are doing and why they believe they are compliant."

Uninformative sales interactions

Security executives assert that their interactions with SaaS-provider teams on security issues are difficult and frustrating. They say that sales reps make security claims that don't appear to be backed up by fact, and that vendors don't have security experts they can talk to. Such experts, who would know the technical specifications of the offerings, are needed to help companies decide how to configure SaaS offerings in a secure way. More than 70 percent of respondents said that uninformed or misleading claims about security capabilities were a cause of dissatisfaction. Reportedly, some sales representatives even misrepresent certifications or customer references. One manufacturing company's CISO said, "I am sick of receiving glossy marketing materials, which are essentially snake oil when it comes to security features . . . many, many vendors will claim their security features are better than [what] a very simple assessment will reveal." Another pointed out examples where simply checking a reference proved that the referenced company had not used security features in the way the sales team had described.

Implications on software as a service purchasing and contracting

SaaS vendors' shortcomings in security capabilities are shaping the ways enterprise customers contract for and use SaaS products. Negotiations about security terms and conditions (T&C) can add weeks or months to contracting processes. Survey respondents said the most challenging issues debated included financial liability for breach events, required cyber-insurance policies, and preferred location for legal proceedings.

Security issues often disqualify providers from consideration. For those that are considered, security remains a major concern; a few of our respondents told us that they had reverted to a provider's on-premises solution because they could not become comfortable with the security provisions of the SaaS offering. When deploying SaaS offerings, security executives cited the cost and complexity of the compensating controls they had to put in place to manage the accompanying risk. Many decide to invest in specialized third-party tools to manage encryption keys, ensure compliance with corporate policies, analyze vulnerabilities, enhance encryption, or track data usage for SaaS offerings. CISOs also say that they must expend scarce talent and resources in configuring and managing security offerings to meet their standards.

In a few reported cases, large companies called off planned migrations from an on-premises platform to an SaaS offering for security reasons. In one case, the vendor failed to meet commitments to make the APIs mature for IAM and SIEM integration. After the company had devoted significant resources to use the required APIs, it gave up and reverted to

Security issues often disqualify providers from consideration.

the existing version of the application in order to ensure required performance. In another example, new charges for security-related features were significant enough to sour the business case for adoption of a SaaS offering, causing the company to continue using the on-premises version.

Actions software-as-a-service providers can take to meet the security requirements of their enterprise customers

For all the value that SaaS promises, security concerns limit enterprise customers seeking to make the transition from on-premises solutions to SaaS-based ones. Fortunately, providers can take the following steps to remove barriers to SaaS adoption.

1. Adopt a multilevel model for addressing security-related customer inquiries

When asked about the characteristics of best-in-class SaaS vendors on security, 70 percent of cyber professionals cited transparency on security capabilities. They said that in selling, vendors can distinguish themselves by giving informed, straightforward responses regarding security capabilities and aftersales onboarding. They also said that vendors should provide transparency regarding updates and expected implications for customer systems. Software vendors can meet these expectations with a multilevel model for addressing security-related customer inquiries.

Level 1. Partner with third-party security-assessment vendors to make data about security capabilities easily available at a low cost. Some third-party platforms capture more than 1,200 data points about each vendor's security capabilities. SaaS providers have no reason to refrain from sharing this information with potential customers.

Level 2. Train the sales force in the basic security features of the offerings and ensure that they respond to security inquiries accurately and intelligently. In addition, vendors need to provide incentives to sales people that encourage them to ask for expert help rather than provide incorrect or incomplete information.

Level 3. Create a specialized team to respond to sales-force inquiries, supported by a robust knowledge base to help answer more complicated questions. Given the importance of API-based integration, this group should act as a developer-support function in many respects. It should also invest in developing code samples and other artifacts that will make it easier for the customer's security teams to implement the vendor's products.

Level 4. Provide a clear escalation path to security engineers who can answer the most complicated questions about IAM, telemetry, key management, and other issues.

Level 5. Prepare for customer T&C requests. Customers will ask about the assumption of liability, preferred legal venues, and other issues. Vendors need to develop protocols for the circumstances under which they will accept requests, such as which requests will be accepted and from whom. Just as enterprise customers seek to assign prices to security risk, vendors may want to assign costs to special T&C requests. Even if they cannot pass that cost along to the customer, this type of accounting tool can provide an indication of whether a deal is worth making.

2. Aggressively facilitate integrations

The day of the stand-alone, monolithic application ended years ago, for security features as well as for the enterprise-technology environment. SaaS vendors should thus make it easier to integrate their offerings with the rest of their customers' security environments. This requires several actions.

Build a comprehensive set of connectors to relevant security tools. Major SaaS providers need to have pre-wired integration capabilities for every major enterprise IAM platform, cloud IAM platform, privileged-access-management platform (PAM),

and SIEM platform. So equipped, providers will enable customers to implement their products more quickly, less expensively, and with greater confidence that they are not introducing new security vulnerabilities.

Invest in building better APIs. Too often, SaaS vendors pay little attention to security APIs. Instead, they should create a consistent security-API model across the products they offer. They should work with customers' security teams to provide the granular capabilities required in the areas of encryption, key management, and telemetry. They should deploy simple, easy-to-understand API semantics backed up by documentation.

Enhance security-related customer-success teams. Nearly two-thirds of security executives said that leading vendors were distinguished by the superior technical expertise of their support organizations. This means that vendors should enhance the security skills of the teams that help customers implement their products. In addition to improving customer outcomes, enhanced customer support could lead to more sales.

3. Help customers address data privacy

With expanding market and regulatory demands for data privacy, CISOs believe that SaaS vendors have not demonstrated sufficient leadership in this area. They need these vendors to research thoroughly the regulatory expectations in the markets they participate in and identify the specific actions required to comply. They need vendors to invest in the encryption, key-management, logging, data-tracking, and data-purging capabilities necessary for compliance. They should also guide CISOs on how to implement their products to minimize regulatory risk.

Over time, SaaS will largely replace traditional on-premises COTS applications, with enterprises benefiting from faster innovation, reduced complexity, lower operating costs, and massively reduced management spending on obsolete technologies. However, SaaS disrupts the traditional relationship between vendors and customers on security. With the vendor taking on much more security responsibility than before, the security team is put right in the middle of SaaS-adoption decisions. Moreover, companies cannot accept SaaS products as security "black boxes." As we have emphasized, they must be able to determine how to integrate them into the rest of their security environments.

Our survey indicates that many SaaS vendors have yet to understand this new reality. They do not communicate well with customers on security; their products are hard to integrate with the rest of the customers' security environments; and they have not taken the lead in helping customers comply with data-privacy expectations. Security issues are causing companies to eliminate certain vendors from consideration, extending procurement processes by weeks and months, and adding significant cost and complexity to SaaS deployments. By actively addressing these issues, providers will speed the ongoing migration from traditional on-premises applications to SaaS.

Rich Cracknell is a manager of solution delivery in McKinsey's Silicon Valley office; **James M. Kaplan** is a partner in the New York office, where **Celina Stewart** is a cyber solutions senior analyst; and **Wolf Richter** is a partner in the Berlin office, where **Lucy Shenton** is a cyber solutions specialist.

Designed by Global Editorial Services