Securing SaaS Applications: Extending Identity to Secure Data Across a Multitude of SaaS Applications

Publication Date
January 2023

IDC Analyst Brief
Sponsored by DoControl

IDC ANALYST BRIEF
Sponsored by: DoControl

The growth of SaaS applications, the increasing demand to integrate SaaS applications for unified security and control, and the issue of APIs have created demand in the market for a single service offering that integrates and manages disparate SaaS applications.

Securing SaaS Applications: Extending Identity to Secure Data Across a Multitude of SaaS Applications

January 2023

Written by: Frank Dickson, Group Vice President, Security and Trust

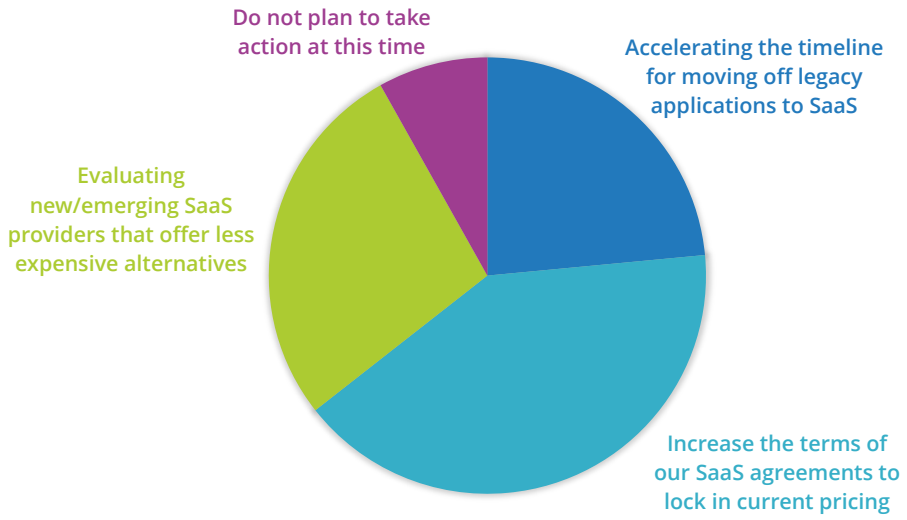
Introduction

The promise of digital transformation is being realized by many. IDC forecasts spending on digital technologies will reach $2 trillion in 2023, driven by cloud, artificial intelligence (AI), and the Internet of Things (IoT). SaaS applications have been a major component of digital transformation. Even as fears of inflation persist, accelerating the movement to SaaS applications is viewed as a strategic weapon to combat looming economic malaise (see Figure 1).

FIGURE 1: ***Worries of Inflation Increase the Move to SaaS***

For those expecting inflation to have the greatest impact on pricing for software application costs, only 8% intend to take no action.

Q ***You indicated that you expect inflation to have the greatest impact on pricing for software application costs. Which of the following statements best describes how you think SaaS options will affect your approach to minimizing impact?***

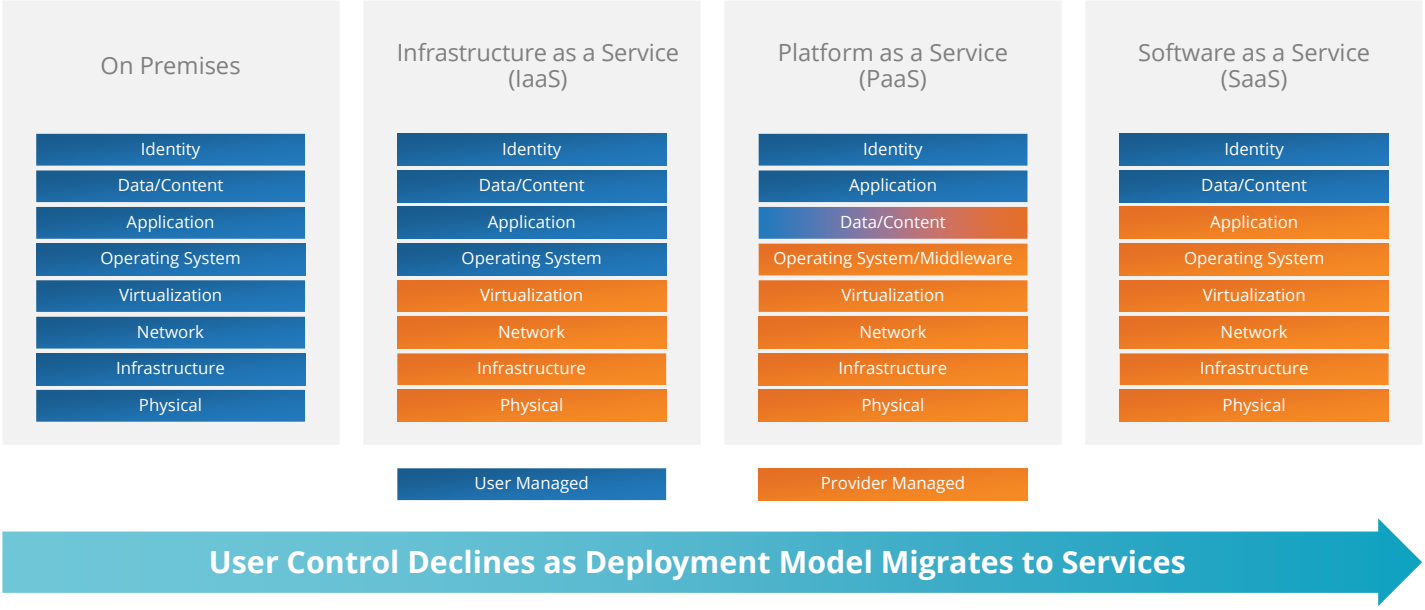


n = 285

Source: IDC's Future Enterprise Resiliency and Spending Survey, Wave 3, April 2022

The promise of moving to SaaS is compelling. As organizations offload and simplify the building, operation, and ongoing maintenance of applications, most of the shared infrastructure model is managed by the SaaS provider; the customer retains control of only identity and data (see Figure 2).

FIGURE 2: ***Shared Infrastructure Model***



Source: IDC, 2023

It is important to note that as a component of identity, SaaS introduces/emphasizes a new responsibility for integrating identity functions. Rarely does a SaaS service operate in a silo, and it is the user's responsibility to manage the security of the authorized integrations created by the users of the service. In the past, identity meant authorization/authentication; in today's digitally transformed world, the scope of identity has expanded to self-service, invite by peers, and OAuth integrations.

However, protecting SaaS application data (within applications such as G Suite, Office 365, Salesforce, Slack, Box, and Dropbox) is still the responsibility of the customer, and the relationships between data in these SaaS applications and who or what has access to it are increasingly complex. The significance of the complexity and value of the data increases as security professionals start to realize that their source code (e.g., GitHub, Bitbucket), production operations (e.g., Snowflake, DNS - Google Domains), and finance (e.g., QuickBooks, NetSuite) are also impacted.

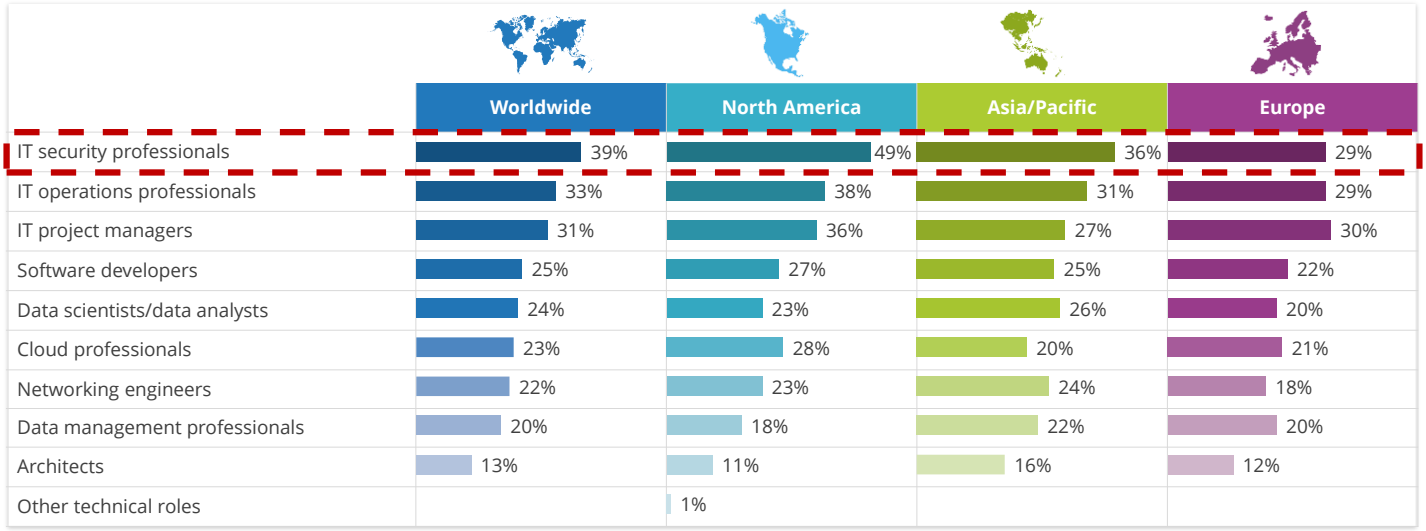
This protection scope is no longer just for collaboration and document management. SaaS applications are driving prolific collaboration between end users and giving more control to end users directly. Users now have more flexibility and administrator control over data sharing settings within traditional SaaS applications such as documents, spreadsheets, slides, email groups, chat messages, no-code/low-code integrations (e.g., Zapier, IFTTT), and OAuth connections. New categories of SaaS such as customer databases, corporate IP, and production access are all part of this concern now. Whether a customer list is stolen from a production database or from a rogue SaaS marketing app, the same reporting obligations and brand damage apply.

These "ease of use" drivers open more opportunities for end users to easily create mistakes with SaaS configuration settings. Best practices are centered around automating the management, monitoring, and necessary remediation of application data as manual efforts would be undertaken by IT and security teams (that are already stretched thin) and/or would add more cost (to hire professionals to do the work for which they do not have time). SaaS security can thus scale with SaaS utilization and prevent known high-risk activities such as a departing employee exfiltrating data by sending it to their private email account or a former contractor who still has access to a customer list on the G: drive.

The acute shortage of security professionals cannot be overemphasized. As organizations complete their digital transformation initiatives to become digital first, the lack of security professionals is a top concern. IT security professionals are in the highest demand for technology initiatives globally (see Figure 3).

FIGURE 3: ***IT Security Professionals Are in the Highest Demand for Technology Initiatives Globally***

Q ***What technology roles are in highest demand for the most important technology initiatives?***



Worldwide n = 816; North America n = 256; Asia/Pacific n = 369; Europe n = 191

Source: IDC's Future Enterprise Resiliency and Spending Survey, Wave 6, July 2022

SaaS application data, configurations, and settings increasingly need to be integrated, governed, and managed using APIs to do the following:

- View and administer the settings and configurations across SaaS applications in one place
- Automate onboarding and offboarding user life-cycle management
- Examine user activity across SaaS applications in real time using native application activity
- Have granular control beyond what native SaaS admin tools provide since most SaaS admin controls are only exposed via APIs

- Gain visibility into publicly shared files, third-party connected apps, and content discovery for data loss prevention
- Detect and prevent insider threats for emails, data, and files based on examining SaaS usage activities
- Restrict super admin and access roles to limit privileged account sprawl and excessive privileges
- Discover inactive users to reduce license expense, demonstrating a hard ROI
- Perform maintenance such as cleaning up empty public Slack channels or empty public Google or Dropbox groups

The reality is that if managing and maintaining one SaaS application takes effort, then doing the same for two integrated SaaS applications takes that effort to the exponent of two. Three integrated SaaS applications takes that effort to the exponent of three. Additionally, different groups with organizations use different SaaS apps with different data sensitivity, making it even harder for security teams to keep up with malicious activity, misconfigurations, and data exfiltration.

Benefits

The growth of SaaS applications, the increasing demand to integrate SaaS applications for unified security and control, and the issue of APIs have created demand in the market for a single service offering that integrates and manages disparate SaaS applications. This requires a platform-based approach that uses SaaS APIs to address the following needs:

- Assist in the discovery of SaaS applications
- Expose the business context of all user behaviors and interactions (both internal and external identities)
- Assist in the proper configuration of SaaS applications
- Assist in the integration of applications
- Assist in maintaining the application integrations against version upgrades and API deprecations
- Provide pan-application visibility and reports, especially for a compliance use case
- Make the establishment, implementation, maintenance, and enforcement of policies easy and automated

These needs can be satisfied with professional services through custom scripts and point tools, but with two drawbacks:

- Professional services are reactionary, often requiring API drift to break an integration before acting.
- Professional services can be pricey.

Conclusion

Life on the cloud is far from static, and there is a risk that an organization might underestimate the effort needed to stay on top of the continuous changes that SaaS and cloud-based software introduces into the organization. Similarly, there is also a risk that organizations won't identify and exploit the new features and functionality coming from the software provider on a fairly continuous basis.

It's important for SaaS and cloud software users to maintain a proactive and business-oriented approach to "life on the cloud."

Change is the constant, and if you learn to go with it, you will only improve your organization's use of cloud services and get more from your SaaS and cloud-enabled software.

About the Analyst

Frank Dickson, *Group Vice President, Security and Trust*

Frank Dickson is the Group Vice President for IDC's Security and Trust research practice. In this role, he leads the team that delivers compelling research in the areas of Security Services; Information and Data Security; Endpoint Security; Trust; Governance, Risk, and Compliance; Identity and Digital Trust; IoT Security; Network Security; Privacy and Legal Tech; Security Analytics; Video Surveillance; and Application Security and Fraud.

MESSAGE FROM THE SPONSOR

About DoControl

DoControl is an agentless, event-driven SaaS Security Platform that secures sensitive data and files within business-critical SaaS applications. DoControl helps you understand how much data is exposed, remediate it quickly, and automatically remediate over time through granular, no-code workflows. DoControl uncovers all SaaS users, 3rd party collaborators, assets/metadata, OAuth apps, groups, and activity events. DoControl helps reduce risk, prevent data breaches, and mitigate insider risk without slowing down business enablement. To learn more about DoControl, visit www.docontrol.io, read the DoControl blogs, or follow us on Twitter and LinkedIn.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com