Software that enables the creation of innovative products finds a secure home in the cloud.

Product Development:

Better and Safer via SaaS

Product development software is key to economic growth. It is essential to the creation of the new equipment, machines, and consumer goods that are woven into the fabric of today's economy. But product development software does not exist in a vacuum: It is subject to larger forces such as the advent of the cloud and the ongoing surge in remote work.

According to the **IDG 2020 Cloud Computing Study**, software-as-a-service (SaaS) utilization is growing, while usage of commercially licensed software is shrinking. Currently, SaaS is 24% of the market; in 18 months, that percentage will rise to 36%, the research found. Meanwhile, remote work, spurred by the recent pandemic, is here to stay. "COVID-19 will create lasting changes in how we work, as organizations develop a more positive view of a work-from-home structure," concluded the **CIO COVID-19 Impact Study of 2020.**

Despite this confluence of forces, the industrial and engineering companies that develop new products must carry on with essential tasks, foremost among which is safeguarding intellectual property (IP). Product creators base their new designs on innovative ideas and trade secrets which, should they fall into the wrong hands, could result in millions and even billions of dollars' worth of damage.

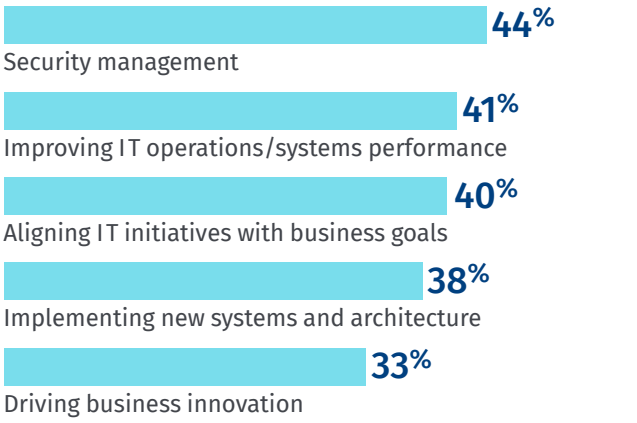
For example, a rogue nation-state could appropriate new product information and produce competing products at lower cost, foreclosing an entire market to the victim company. And should the product under development be intended for the defense industry, national security could be jeopardized.

At the same time, product development processes expose sensitive data to theft. That's because product development requires increasingly intense collaboration across departments, geographies, and companies. As access is extended to more people inside and outside a company, susceptibility to attack increases.

The growing adoption of SaaS, however, brings with it improved cybersecurity and increased IP protection. Compared with on-premises implementations, SaaS applications often deliver higher availability and greater redundancy, as well as more frequent and thorough data backups.

Figure 1

Which activities are CIOs currently focusing on?



THE STATE OF CYBERSECURITY

Concern on the part of IT leaders with regard to cybersecurity, whether on-premises or in the cloud, has risen to the top of CIOs' to-do lists, according to the IDG 2021 State of the CIO Report. Specifically, security management ranks first among priorities for CIOs *(see Figure 1)*.

The concern of these IT decision-makers is fueled by the growing number—and increasing sophistication—of threats. These include:

- **Supply chain attacks.** The recent SolarWinds attack succeeded by corrupting routine software updates, which, when applied by victim companies, compromised IT infrastructure.
- **Dependency confusion attacks.** Also called substitution attacks, this new technique targets the application-building process by planting malware in the libraries developers use to create applications.
- **Industrial espionage.** Because IP is the lifeblood of engineering firms, competitors and nation-states that succeed in stealing it through social engineering or malware can gain a significant strategic advantage.
- **Phishing and its variants.** Still a common attack vector, phishing and spear-phishing emails have become highly sophisticated and often succeed in fooling even wary users as they plant advanced persistent threat (APT) malware.
- **Ransomware.** By encrypting vital data, bad actors hold it hostage while extorting ransom payments. Although savvy companies nullify ransomware by backing up data, others pay the ransom in the hope their data will be released.
- **Distributed Denial-of-Service (DDoS) attacks.** The use of IIoT devices such as security cameras and sensors to launch DDoS attacks has taken down large corporate networks by overwhelming servers with fake requests.

At the same time, IT leaders face many challenges in their quest to protect sensitive data, particularly in their quest to protect data on-premises. For example:

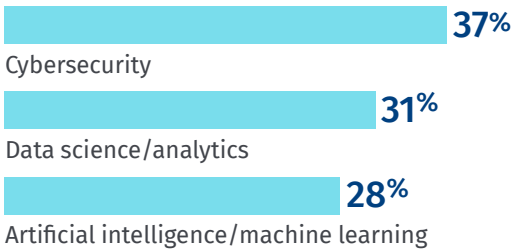
Technology – false positives. Cybersecurity software identifies anomalies and sends alerts for further investigation. But there are frequently too many alerts for in-house staff to evaluate accurately. False positives can overwhelm staff, causing them to ignore real threats. It takes special expertise to sift through reams of alerts to find the events that pose real danger to an organization.

Tools – complexity. Cybersecurity tools are often highly complex, making configuration, maintenance, budgeting, and licensing time-consuming and costly. Cybersecurity tools generally require continuous updates to stay current with newly identified vulnerabilities and exploits, resulting in wasted resources, particularly when an organization deploys point products.

Professional – staffing. Finding, hiring, and retaining cybersecurity specialists with the depth of knowledge to safeguard sensitive corporate data is not easy. Salaries for these rare individuals can be quite high. Should one of them depart, institutional knowledge will be lost and the process of finding, hiring, and retaining a specialist of similar caliber will have to start all over again *(see Figure 2)*.

Financial – high stakes. In taking the measure of their adversaries, IT leaders must evaluate their own willingness to engage in a battle of wits and resources with cybercriminals and rogue nation-states. They must ask themselves whether they are willing to participate in a high-stakes contest in which some bad actors have nearly limitless resources.

Figure 2
Planning to hire in these tech areas

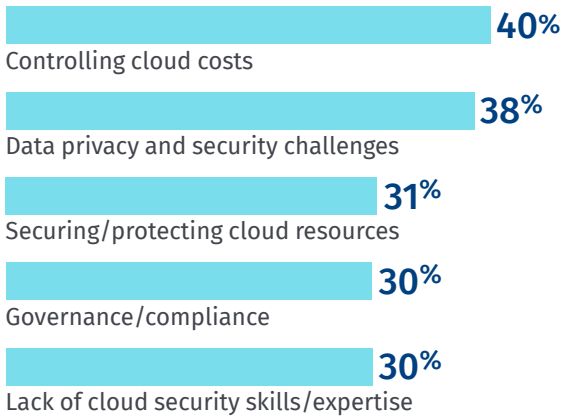


According to the IDG 2021 State of the CIO Survey, cybersecurity specialists are the most sought-after of IT professionals—37% of CIOs currently plan to hire them

CYBERSECURITY IS PERCEIVED AS A PUBLIC CLOUD CHALLENGE

Increasing reliance on SaaS is causing concern among IT leaders. In the IDG 2020 Cloud Computing Study, several security-related issues bubbled up among the top worries, trailing only the need to control the cost of using public cloud services *(see Figure 3)*.

Figure 3
Top 5 challenges to public cloud



Indeed, challenges surrounding data privacy and security (38%) almost matched cost-control as the main concern. Tellingly, the next three issues are all closely linked cybersecurity challenges: the need to defend cloud resources against attack (31%); the need to keep data within regulatory compliance (30%); and the dearth of skilled experts to keep data secure (30%).

SaaS CYBERSECURITY IS BETTER THAN ON-PREM

Although the concerns expressed in the IDG survey are real, the facts demonstrate that these fears are unfounded. Because their business depends on keeping customers' data secure, cloud providers often have broader and deeper cybersecurity knowledge than their customers for several reasons:

1. Managing a number of large data centers generates economies of scale, enabling SaaS providers to invest more in technology, processes, and skilled experts than is possible for most companies.
2. SaaS providers have in-depth knowledge of the applications they are hosting, including high-risk functional areas and specialized secure configurations, that is typically greater than that of commercial customers.
3. The data centers of cloud service providers such as Microsoft Azure and Amazon Web Services (AWS) are routinely audited for ISO and SOC 2 compliance, as are the SaaS providers themselves.
4. Increasingly, SaaS providers are implementing zero-trust cybersecurity principles, in which micro-segmentation is applied to IT resources, access is tightly controlled, and multi-factor authentication (MFA) is enforced.

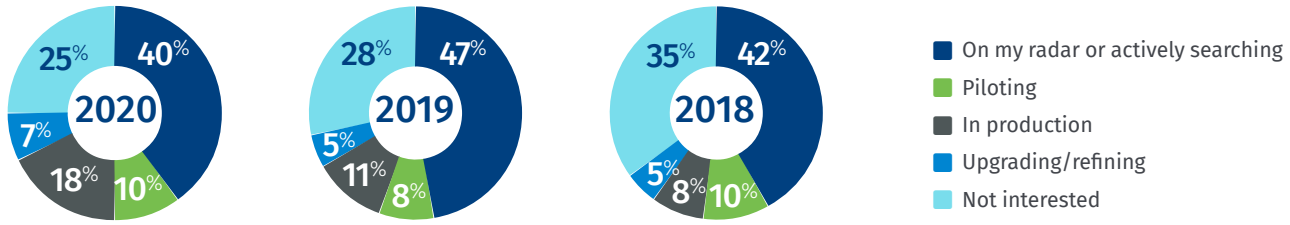
In a significant finding, zero-trust principles are steadily gaining adherents among IT leaders, according to the 2020 IDG Security Priorities Study *(see Figure 4)*. The survey found that production implementations of zero-trust cybersecurity have more than doubled since 2018, rising from 8% to 18%.

THE FUTURE OF ENGINEERING AND INDUSTRIAL SOFTWARE APPLICATIONS

Whether using product lifecycle management (PLM), computer-aided design (CAD), product data management (PDM), or another software application, engineers should utilize a unified development environment that is consistent across multiple worldwide locations. That environment must support secure collaboration for multi-disciplinary, geographically distributed projects. This work could be within one division, across different divisions, or with external partners.

Figure 4

Zero trust continues to gain traction



To protect IP in such an environment, cybersecurity measures should implement defense in depth at the hardware and cloud-provider levels. In addition, tight access control must be implemented for PLM applications in particular.

However, companies that rely on on-premises deployments burden their IT teams with tasks such as maintenance, configuration management, and monitoring that, while important, are non-strategic. By relying on SaaS and cloud-based applications—and SaaS and cloud-based cybersecurity—internal IT teams are left free to focus on their strategic role in bringing about digital transformation at their companies.

REMOTE WORK WILL CONTINUE

Most observers agree with the IDG COVID-19 Impact Study that remote work will continue at a high level following the pandemic. Having learned that productivity need not suffer when employees work from home, many companies will either tolerate or encourage the practice. In turn, countless workers will welcome the opportunity to continue working remotely.

Although IT leaders have striven to make remote work as seamless as possible by providing high-bandwidth connectivity, many believe remote workforce cybersecurity is lacking. Work-from-home vulnerabilities include the use of personal (rather than corporate) devices, USB drives, social media, and non-secure web browsing. An engineer who accesses CAD drawings from a home computer, then saves files to a USB drive on which there might be malware, could introduce malware into the organization when files are later uploaded from the USB drive. IT leaders are concerned about such dangers. IDG's **CSO Pandemic Impact Survey** found that 61% of security leaders expressed greater concern about attacks targeting work-from-home employees than prior to the pandemic.

SaaS DELIVERS FUNCTIONALITY, SECURITY

When the needs of industrial and engineering companies are considered, many signs point to the increased use of SaaS-based applications. SaaS applications can connect and unify an organization by providing users, regardless of their location, the same versions of the same applications. Similarly, SaaS can provide a comprehensive and unified approach to cybersecurity. Rather than a hodge-podge of point products that must be deployed and maintained by hard-pressed staff, SaaS applications can implement the latest cybersecurity software consistently for all applications and users.

A recent report from Aberdeen[1] supports the contention that cloud-based services are generally more secure that on-prem data centers. Because of their intense focus on cybersecurity, SaaS providers as well as the underlying cloud service providers frequently subject their services to rigorous audits by various certification entities. Aberdeen advises that organizations that are on the fence about moving business-critical applications to the cloud should make certifications one of their key criteria for selecting a cloud service provider.

"If your organization is currently evaluating cloud-based implementations for your business-critical applications... the time has come to ask, 'With the right cloud service provider, what are we waiting for?'" writes Aberdeen.[2]

THE PTC DIFFERENCE

SaaS has become prevalent in nearly every category of business software because it lowers total cost of ownership, enables collaboration and mobility, and is continuously updated to provide users with the latest capabilities. Carrying out its commitment to SaaS leadership, PTC has acquired Onshape and Arena Solutions and has created the Atlas SaaS platform to bring the benefits of SaaS to product development.

PTC's suite of SaaS CAD and PLM solutions is well-suited to the new paradigm of remote work and global collaboration. To protect IP at engineering companies, PTC has built in cybersecurity at multiple levels. Each PTC offering has a defined secure software-development life cycle (SDLC), with focused security resources, and PTC's Office of Product Security provides oversight across applications.

Because users access the SaaS applications in the cloud, they do not run any of the application software on their own computers. PTC takes responsibility for securing its SaaS applications and the hardware on which they run, in partnership with cloud service providers such as Microsoft Azure and AWS. As a SaaS provider, PTC is able to hire expert cybersecurity professionals with the advanced skill sets needed to protect its applications in a tightly controlled cloud environment.

In addition, the PTC SaaS solution avoids downloads to USB devices and therefore the possibility of running infected executable files containing supply chain attacks. And as a SaaS service, the PTC suite ensures against data loss due to computer device theft.

PTC SaaS solutions are regularly audited for compliance with a variety of cybersecurity standards and include these cybersecurity features:

- **Access control** over the specific objects to which users have access.
- **Secure workspaces** created within CREO view visualization software.
- **Single sign-on** using SAML authentication and OAuth delegated authorization.
- **Forensic analysis** enabled by security audit and event tracking.
- **Encryption** for data at rest and data in motion.

The PTC SaaS product development suite includes:

PTC Atlas, the integration platform for the PTC SaaS suite.

Onshape, which unites robust CAD with powerful data management, real-time collaboration tools, and business analytics.

Arena Solutions, PLM software that manages highly complex bills of materials, meeting quality standards and providing regulatory compliance.

Windchill, a suite of PLM SaaS applications that provides real-time information sharing, dynamic data visualization, and the ability for multiple geographically dispersed teams to collaborate easily and securely. Windchill's open architecture integrates with other enterprise systems as well as IoT devices.

CONCLUSION

SaaS applications deliver benefits that are essential to the success of modern industrial and engineering companies, even as remote work is increasing to a permanently higher level than pre-pandemic. To assure the protection of IP in the product development process, IT leaders should carefully examine the cybersecurity capabilities of their cloud-based service providers.

With their ability to hire and retain the most skilled cybersecurity professionals, and their focus on advanced cybersecurity methodologies including zero-trust, SaaS providers are uniquely positioned to deliver a higher level of cybersecurity than companies can provide themselves. Organizations that increase their reliance on SaaS- and cloud-based applications will achieve greater productivity, lower costs, tighter security, and higher workforce morale than competitors that remain reliant on on-premises implementations.

To learn how SaaS is transforming product development, visit www.ptc.com/industry-insights/saas

ENDNOTES

1 "Move Your Business-Critical Apps to the Cloud: How Security, Privacy, and Compliance Help Make the Case," by Derek E. Brink, CISSP, vice-president and research fellow, information security and IT GRC, Aberdeen, August 2019.

2 Ibid.