Onymos

The SaaS Disruption Report:

SECURITY & DATA

Insights from leaders in application and software development, IT, and security highlight critical priorities and threats amidst the growing adoption of SaaS and cloud services in software development

Key Findings

This report summarizes the security findings from an online survey conducted by ESG and Onymos. The survey polled 300 application and software development, IT, and security leaders to better understand application and software development processes and priorities among midmarket and enterprise organizations in the United States.

The security-focused findings emphasize a need for improved security and data privacy methods in software-as-a-service (SaaS) applications that are relied upon for development.

Top Five Findings

1. **Security (72%) and data privacy (65%)** are the most critical priorities in the app development process.
2. **Nearly all (91%)** believe retaining data within custom-built, internal applications is crucial.
3. **Over three-quarters (78%)** are concerned about security threats in SaaS for application development.
4. **Nearly half (45%)** report experiencing a cybersecurity incident through a third-party SaaS solution in the past year.
5. **Only 36%** run all of their applications on-premise or on private clouds.

Additional Insights in 2H 2024

A second report will be released later this year, highlighting findings around common application and software development processes, priorities, and challenges among U.S.-based midmarket and enterprise organizations.

Check back at Onymos.com.

The Proliferation of SaaS & Cloud Services

Today, SaaS is everywhere and is quickly becoming one of the most profitable areas of technology. McKinsey asserts, "The global SaaS market is worth about $3 trillion, and our estimates indicate it could surge to $10 trillion by 2030."

This predicted profitability underscores how heavily enterprises across countless industries rely on SaaS in their businesses, including:

- Healthcare
- Logistics & Supply Chain
- Manufacturing
- Banking & Financial Services
- Retail
- Education
- Government
- Media
- Telecommunications
- Utilities

It is estimated that the average enterprise uses 130 different SaaS applications. The specific uses for these SaaS applications are widespread. Examples include:

HEALTHCARE

EMRs

Remote Medical Device Connectivity

Record Scanning & Digitization (OCR)

GOVERNMENT

IT Infrastructure

Data Management & Accessibility

Cloud Storage

EDUCATION

Learning Management Systems

Video & Communications

Technology-Assisted Grading

One of the most common enterprise uses for SaaS is in the development of business and customer applications. In this context, SaaS is often used in the form of low-code or no-code tools.

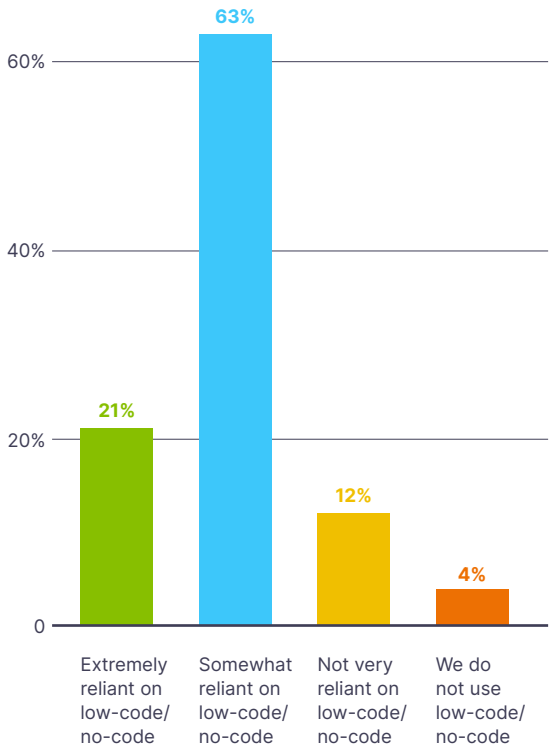
Enterprises are increasingly adopting low-code and no-code SaaS solutions for their application and software development efforts. These solutions are favored for their ability to automate processes, reduce costs, enhance resource efficiency, and accelerate development timelines.

When asked how much their application development teams rely on low-code or no-code capabilities, **84% of leaders reported being reliant**.

In addition to low-code and no-code SaaS solutions gaining popularity, cloud services also offer more options than ever. Leaders were nearly evenly split, with **36% reporting that all their internally-developed applications are on-premise or within private clouds; 32% using public clouds; and 32% opting for distributed environments**.

Private, public, and distributed cloud environments each offer unique benefits. Private clouds allow enterprises to maintain complete control, customize their environment, and implement their own security measures without relying on a third party to handle it for them. Public clouds provide cost savings and scalability, while distributed clouds offer flexibility and resilience.

There Is High Reliance on Low-Code and No-Code SaaS



SaaS and cloud providers often ask enterprises to share their data in exchange for accessing their solutions

The Real Fears and Threats of SaaS in Software Development

While SaaS and cloud solutions offer numerous benefits throughout the development lifecycle, it's crucial to acknowledge and prepare for the associated security threats.

The widespread adoption of SaaS and cloud solutions in software development presents a significant opportunity for data collection. As a result, SaaS and cloud providers often ask enterprises to share their data in exchange for accessing their solutions. This enables providers to leverage customer data for their own benefit, including product development and enhancement. However, it also exposes both the SaaS developers and their customers to greater risks.

The risks associated with SaaS and cloud development solutions can result in accidental and intentional incidents, including those caused by malicious actors, potentially harming all parties involved. For instance, a recent accidental incident occurred with one of the nation's largest healthcare providers, Kaiser Permanente.

An engineering team responsible for managing members' protected health information (PHI) did not fully understand the technology stack, inadvertently allowing SaaS vendors to access PHI through their software's monitoring functions. This data breach exposed the personal information of over 13 million members.

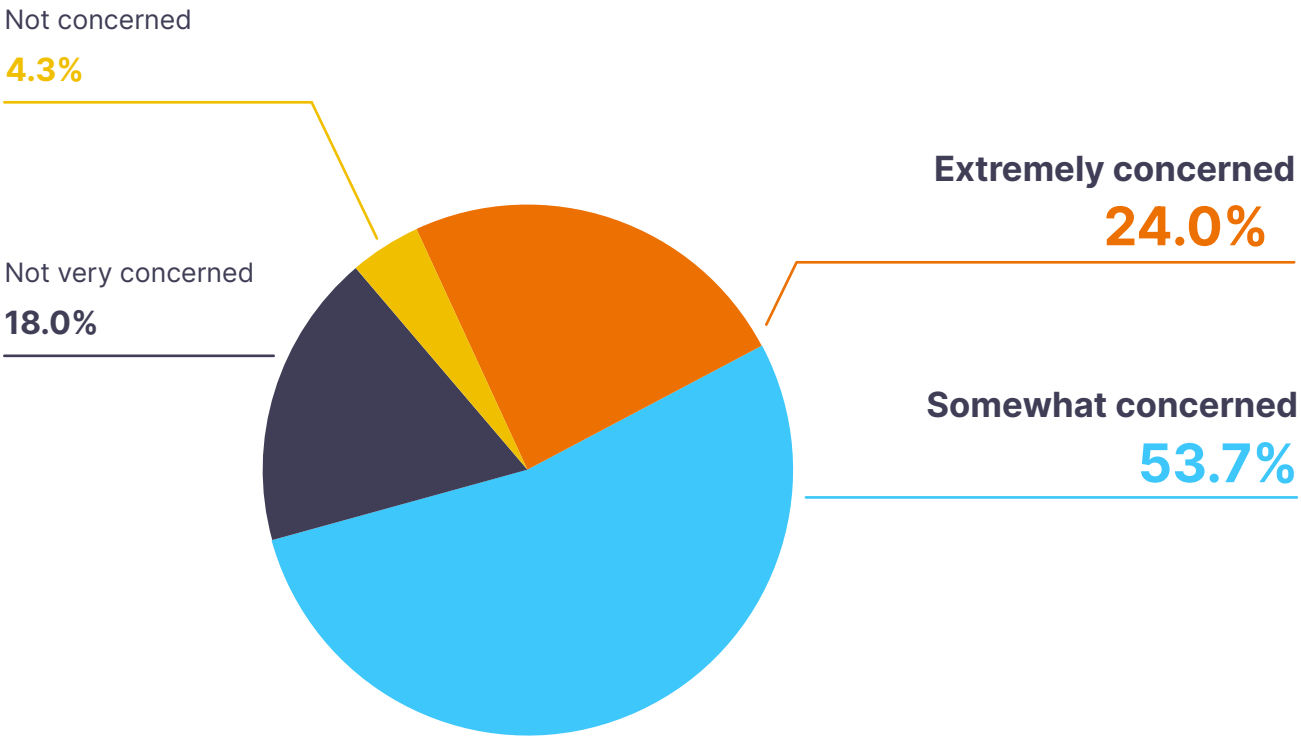
There are also intentional and malicious incidents carried out by cybercriminals. Bad actors have recently targeted SaaS and cloud providers, affecting critical sectors such as healthcare. For example, Welltok suffered a significant data breach due to a vulnerability in Progress Software's MOVEit Transfer server. During the breach, a malicious actor accessed sensitive information, including names, addresses, email addresses, phone numbers, Social Security numbers, health insurance details, and Medicare/Medicaid ID numbers.

Each of these incidents has raised concerns about data privacy and sharing, as reflected in the viewpoints of application and software development, IT, and security leaders.

In the recent Kasier Permanente data breach, an engineering team responsible for managing members' protected health information (PHI) did not fully understand the technology stack, inadvertently allowing SaaS vendors to access PHI through their software's monitoring functions. **This data breach exposed the personal information of over 13 million members**

When asked, in particular, about their level of concern regarding security for the SaaS applications their organization uses in the development process, **more than three-quarters (78%) of leaders expressed concern**.

The Level of SaaS Security Concern Is High



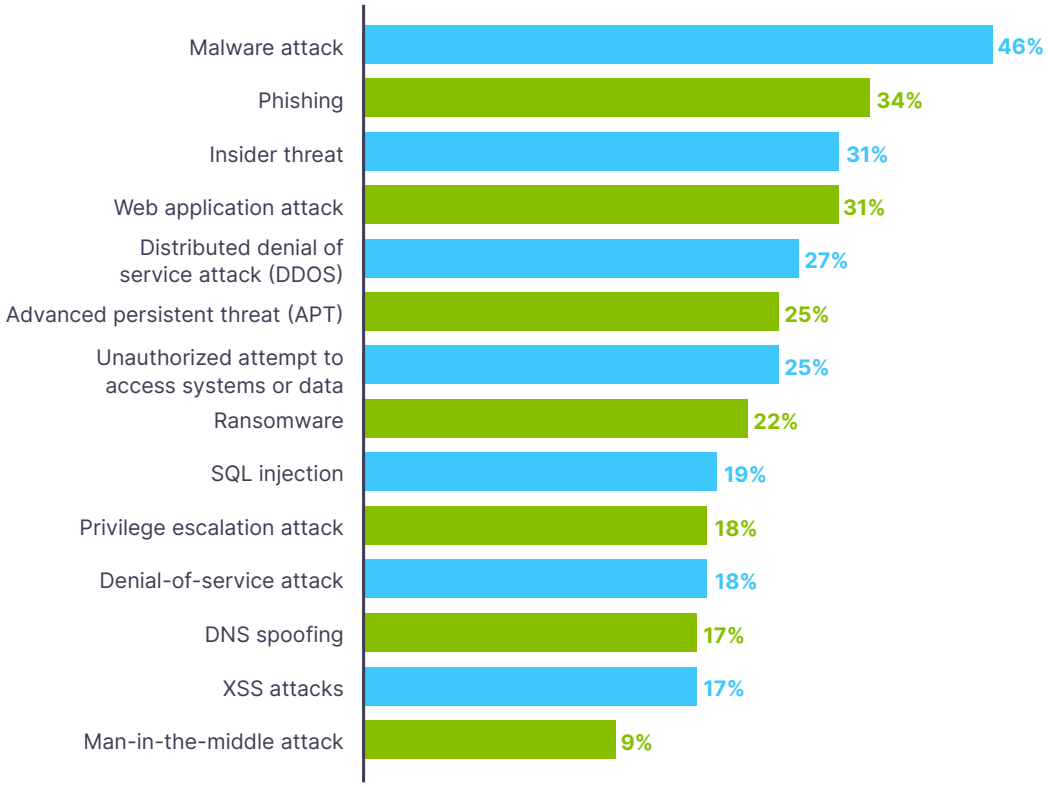
These leaders have a valid reason to be concerned about using SaaS applications. In 2022, Gartner predicted that by "2025, 45% of organizations worldwide will have experienced attacks on their software supply chains, a three-fold increase from 2021."

With less than a year to go until Gartner's estimated timeframe, **45% of all leaders reported in 2024 that their enterprises experienced a cybersecurity incident through a third-party SaaS tool in the last year.**

For those enterprises that experienced a cybersecurity incident through a third-party SaaS solution, **the top five most common incidents were:**

- Malware attack (46%)
- Phishing (34%)
- Insider threat (31%)
- Web application attack (31%)
- DDOS attack (27%)

SaaS Cybersecurity Concerns Come From Multiple Places



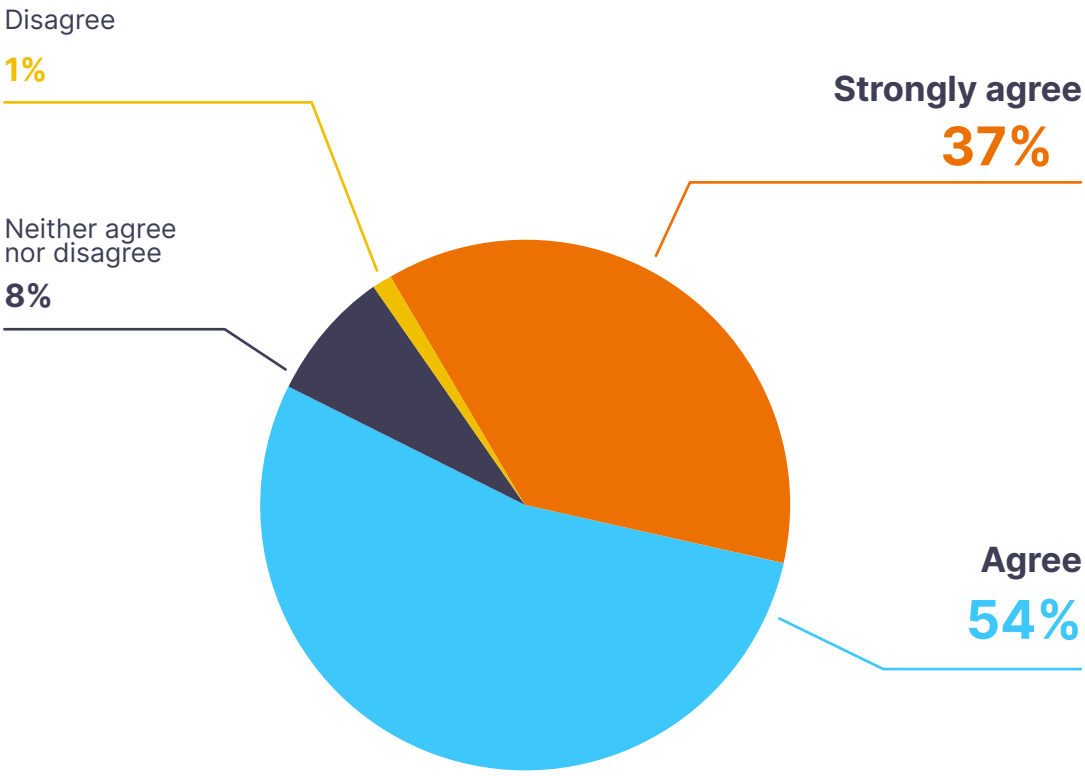
These genuine concerns and threats emphasize the need for enterprises to prioritize robust security measures and continuously refine their strategies to mitigate emerging risks to their applications, software, and overall business operations.

The Prioritization of Security and Data Privacy

For leaders concerned about the security of SaaS software development solutions, many of their key priorities revolve around data privacy and security.

Most leaders (91%) believe that data retention of custom-built, internal applications is crucial. This is evident in their application development priorities. Nearly three-quarters (72%) of leaders highlighted security as a top priority, followed closely by 65% who emphasized data privacy.

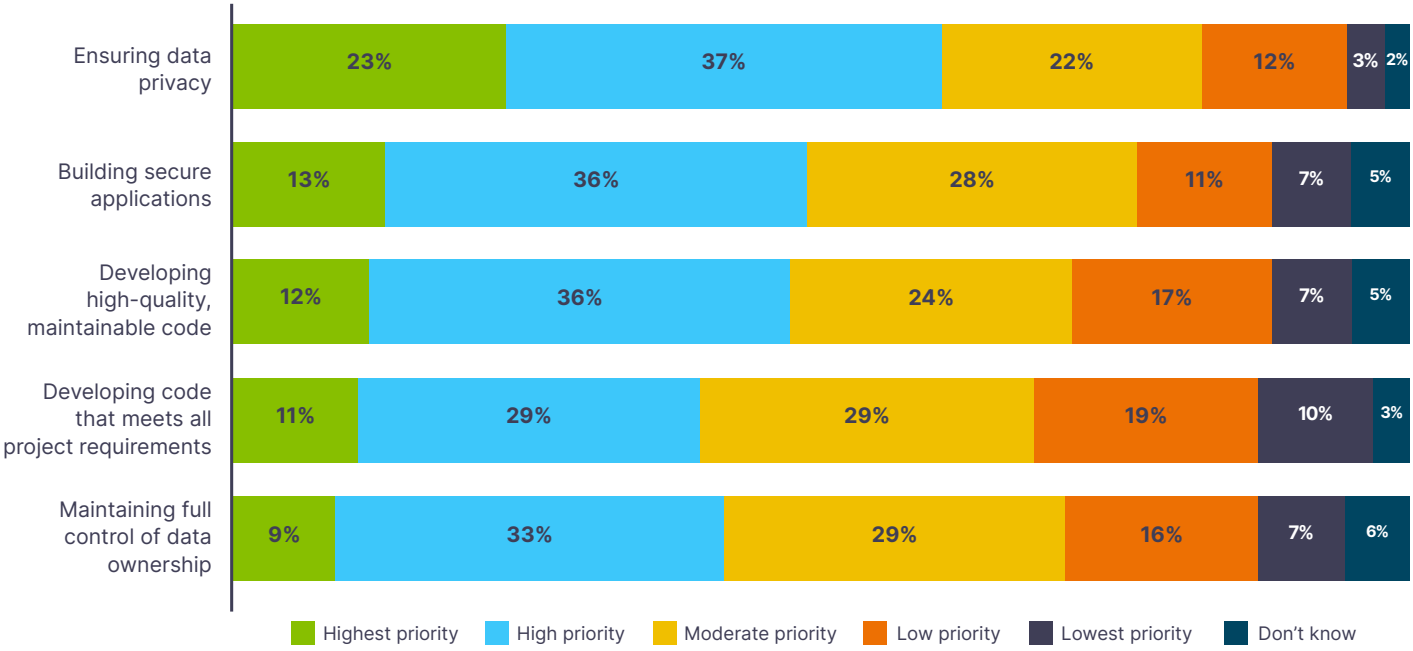
Data Retention for Custom-Built Internal Applications Is Critical



These priorities are also reflected in the specific project assignments, responsibilities, and tasks in their actual application and software development projects. **Three of the top five priorities were:**

- Ensuring data privacy **(60% reported it was a high or highest priority)**
- Building secure applications **(49% reported it was a high or highest priority)**
- Maintaining full control over data ownership **(42% reported it was a high or highest priority**

Data Privacy Is the Top Priority for Application Development

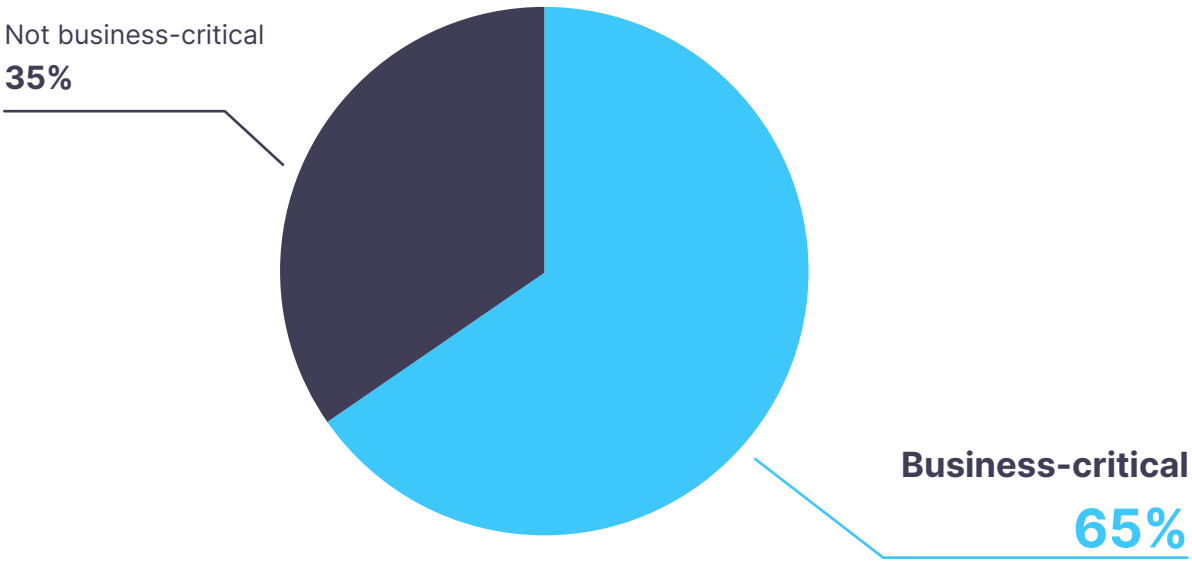


It's Time to Transform Software Development's Approach to SaaS and Cloud Solutions

Despite prioritizing security and privacy, enterprises are still rapidly adopting SaaS and cloud solutions for software development, even when there are strong concerns about their security.

With a **significant number of leaders (65%) reporting that their organizations' internally developed applications are business-critical**, the need to be vigilant about potential threats to sensitive data is critical to maintain customer and user trust.

Internally Developed Applications Are Business-Critical



Given the importance of applications for enterprises, the technology industry needs to reassess its current business model for utilizing SaaS and cloud solutions.

One significant change to the current SaaS and cloud common practices should be **the adoption of "no-data" architecture principles, which prioritize data privacy and security**. This type of architecture allows enterprises to retain full ownership and control over their data, eliminating the need for sharing or granting access to third-party SaaS and cloud vendors and reducing the associated risk.

Enterprises should also be allowed to **own and modify the code associated with the SaaS solutions they use for their application and software development**. This allows enterprise engineering teams the ability to verify and test the code as if they created it themselves. With this approach, organizations can have full confidence in the code's validity, reliability, and security.

Lastly, **rigorous third-party security audits and penetration tests should be prioritized and conducted regularly**. This testing should include understanding how the organization's data flows through different applications and SaaS solutions so that unintended data access and sharing issues can be mitigated.

By re-evaluating and evolving their SaaS and cloud practices, enterprises can ensure a more secure, resilient, and trustworthy future for their businesses and users.

By re-evaluating and evolving their SaaS and cloud practices, enterprises can ensure a more secure, resilient, and trustworthy future for their businesses and users

About Onymos

Onymos is the developer of solutions transforming Software-as-a-Service (SaaS) for software and application development. Its suite of more than 20 foundational software components enables enterprises to build innovative and differentiated web, mobile, and Internet of Things (IoT) applications with unmatched speed, quality, value, and security. Onymos is trusted by top brands, including Albertsons, CVS, Walmart, and Vapotherm. For more information, visit onymos.com, and join the conversation on LinkedIn and X (Twitter).