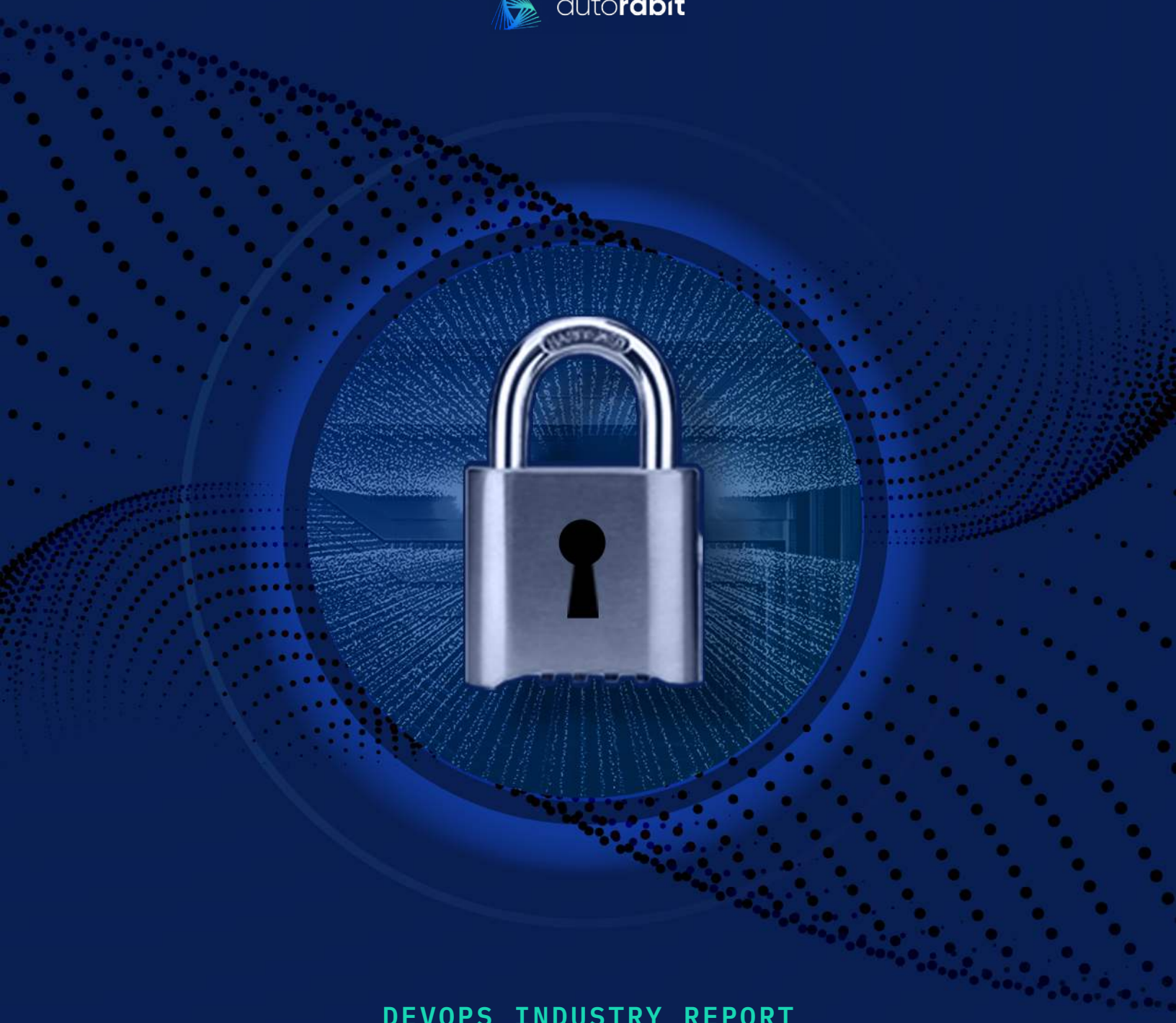
autorabit



DEVOPS INDUSTRY REPORT

Salesforce Data Security in an Evolving Landscape

Current DevOps Data Security + Compliance Trends Throughout a Variety of Industries

The Current State of DevOps Security

The DevOps industry is always changing. New technology, new methods, and new concerns are constantly being adapted to and addressed. Staying on top of these changes helps keep your company at the forefront of your industry.

Optimizing DevOps processes helps put you ahead of your competition.

We're starting out 2021 by analyzing how companies that utilize DevOps are addressing their data security needs.
It's estimated that a ransomware attack will occur every 11 seconds in 2021.

Are you prepared to guard against this or restore your system should the worst-case scenario occur?

This report analyzes where companies across a variety of industries currently stand in their fight against criminals, and what habits position them to have a successful and secure 2021.

Our Contributors

We reached out to thousands of professionals that represent a wide variety of industries. Their responses provide a macro view of the current state of DevOps and how Salesforce data security exists within it.

We sought feedback from development teams most concerned with security and compliance concerns in DevOps.

Over 1/3 of our respondents operate in highly regulated industries like finance and healthcare.

Many viewpoints are represented—from individual contributors up to VPs and higher. This means the information provided comes from those who are most qualified to provide it.

We want to thank everyone that took the time to offer their responses on the security and compliance of their Salesforce DevOps processes. Their efforts provide an illuminating viewpoint on the current state of the DevOps industry.

Summary

Security and compliance are major concerns throughout a variety of industries. The main idea behind these concerns is to ensure the proper handling of sensitive information. Every business that handles customer data has a responsibility to treat it accordingly.

The responses to our survey indicate that while many companies take this responsibility seriously, there is still more that can be done to keep this information secure.

Only 18% of respondents are confident in their current Salesforce data security protocols.

Data security and compliance remain priorities for most companies utilizing DevOps processes. However, these processes are constantly changing and need continued attention.

Adjustment of security and compliance practices is necessary to properly protect information deemed sensitive either by regulations or by the company themselves.

Breaches, accidental deletions, and data leaks are major concerns for representatives from every industry represented by our respondents.

The issues of security and compliance for a company's Salesforce platform will never be completely solved. Consistent effort and attention need to be applied to address evolving concerns as they emerge to properly protect sensitive information.

2020 presented a series of new challenges to these efforts. 2021 will continue this trend.

01

Data Security Practices

DevOps is as essential practice for unifying the development and operations teams to efficiently produce higher quality products. Salesforce is a powerful platform that can facilitate a useful DevOps strategy. But since Salesforce was designed as a CRM and not a development platform, third-party systems can be utilized to get the full potential of the platform.

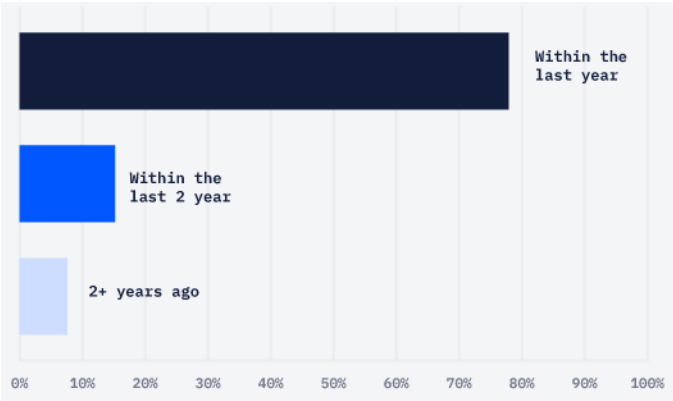
41.85% of respondents aren't using third-party DevOps systems to manage their Salesforce development processes.

This means almost half of our respondents can make great strides in efficiency and quality by simply optimizing their Salesforce platform with a third-party service. Both data quality and data security will benefit from this.

31.6% of respondents are not confident in the security practices utilized in their organization's Salesforce development process.

Consistently updating your data security measures is the best way to keep up with the evolving technological landscape. Consider the previous year—How many changes did you make to your operations through the help of new or updated technological tools? Each change creates new potential vulnerabilities, and your data security plan needs to account for this.

When was the last time our respondents updated their data security measures?



Salesforce recommends "someone in your organization should do regular audits to detect potential abuse." However, our survey showed that ***only 18.65% perform audits on their Salesforce data security measures monthly, and 20.21% don't do it at all.***

2020 forced almost every industry to adapt their functions in one way or another. 2021 will continue this trend and your data security measures need to keep up with these changes to remain reliable.

02

Data Security Threats

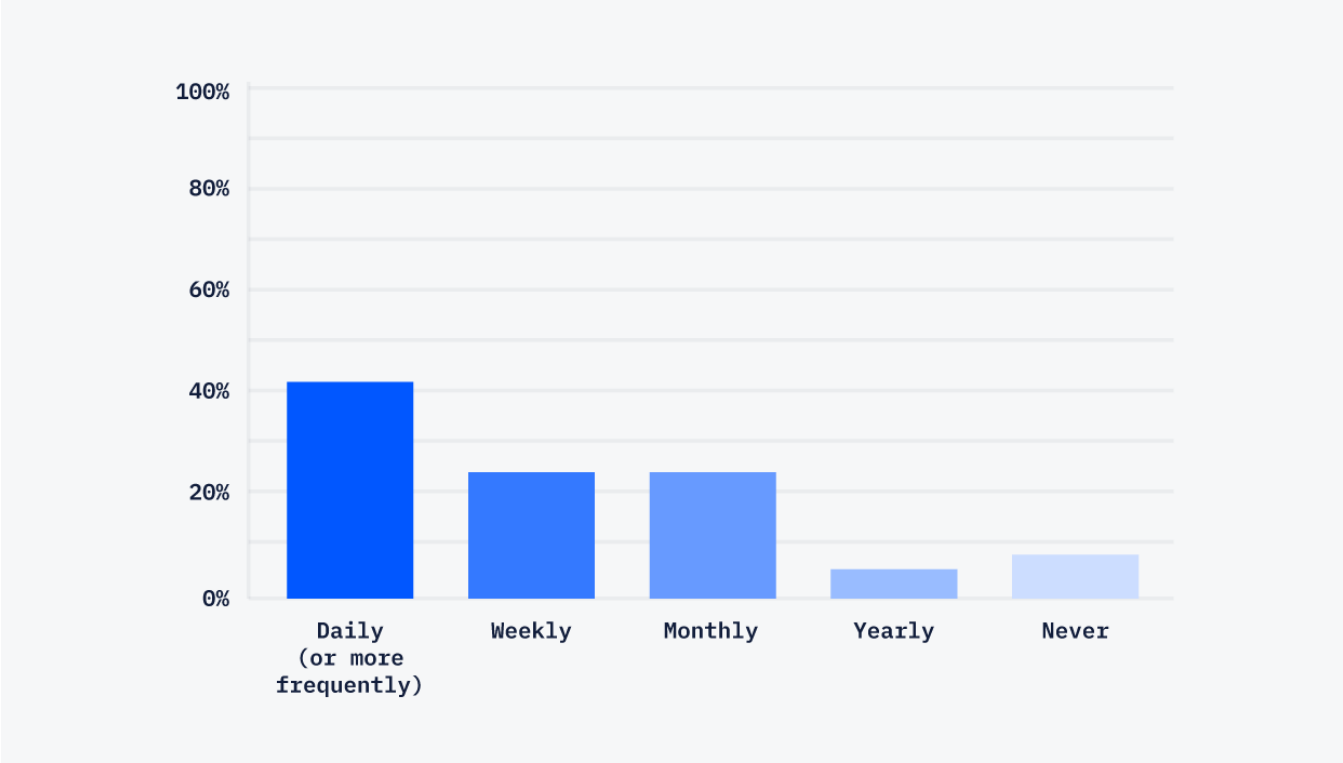
Cyberthreats are a constant concern of every business. High profile breaches of huge companies like Home Depot and Equifax show that nobody is immune to cybercriminals. The increased reliance of internet services over the last year have increased the potential for breaches and hacks.

20.2% of respondents report experiencing a data security incident in the past 5 years. And of these cases, 38% took three or more days to return to normal operations.

Backups are an essential tool to getting your system back online after a data security incident. And of these backups, contemporary repositories of data and metadata are the most useful.

It's recommended to back up your Salesforce data at least once per week.

But how often do companies actually backup their data?

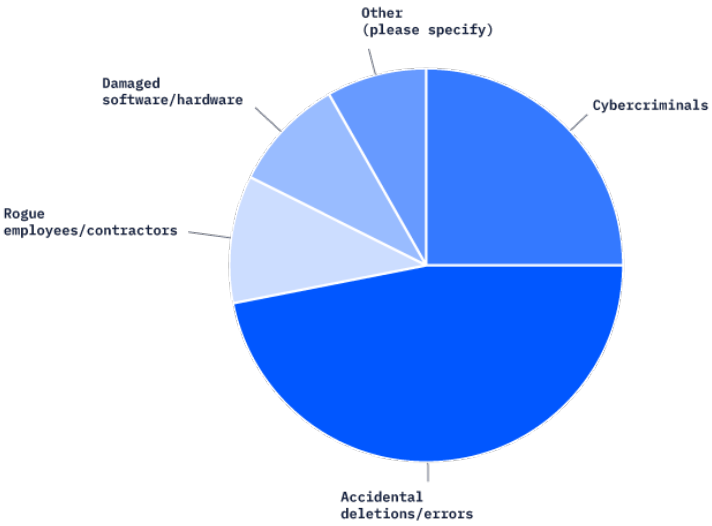


03

Data Security Considerations

Data security threats might seem like they would vary widely between industries, but that is not the case.

What's the biggest threat to data security in the Salesforce development process?



Compare that with a word cloud that shows the data security issues our respondents actually experienced:

Data loss, data breach, and accidental employee deletion are frequent data security concerns for businesses in all industries.

With these threats in mind, how do companies feel about their current data security systems?

82% of respondents said there is room for improvement in their company's data security systems.

The threats that face each company are varied and evolving. Constant attention and clear communication with your team is the best way to fight against potential vulnerabilities.

These concerns can have drastic ramifications if not properly addressed, which is why stipulations are written into law with government regulations.

04

Regulatory Data Security Concerns

Government regulations are incredibly important. They aim to ensure proper handling of sensitive consumer information. Various industries have regulations they are legally obligated to meet. These regulations often involve the security of Personally Identifiable Information (PII), financial information, and more.

Healthcare and financial institutions are among the most regulated bodies regarding data security.

However, only 71.88% of respondents form the banking and healthcare industries reported regulatory compliance to be a driving factor behind their Salesforce data security practices.

Every business in these highly regulated industries need to put compliance at the forefront of their data security strategy.

Data security should be an important consideration for every company, regardless of industry regulations.

72.54% of respondents say they've stressed the importance of data security to their team, but again, all businesses need to make this a priority.

Lapses in data security put your customers—and company-wide systems—in danger of corrupted files, compromised information, and data loss. All these potential outcomes result in money lost for the company, and longstanding issues for the consumer.

ABOUT

autorabit

AutoRABIT is an industry leader in Backup + Recovery solutions and Automated Release Management for SaaS platforms. We automate and accelerate the entire application development and release process. This enables continuous integration and delivery by providing fast, simple, and secure end-to-end automation across all Salesforce implementations. We help enterprises achieve higher release velocity and faster time-to-market.

AutoRABIT provides automated Metadata Deployment, Version Controlling, Advanced Data Loading, Orgs and Sandbox management, Test Automation, and Reporting. Our services complement and extend Salesforce DX. AutoRABIT Vault—our backup and recovery solution—streamlines Salesforce data, simplifies data backup challenges, offers disaster recovery and endpoint data protection on Cloud.

VISIT US TODAY TO LEARN MORE

www.autorabit.com