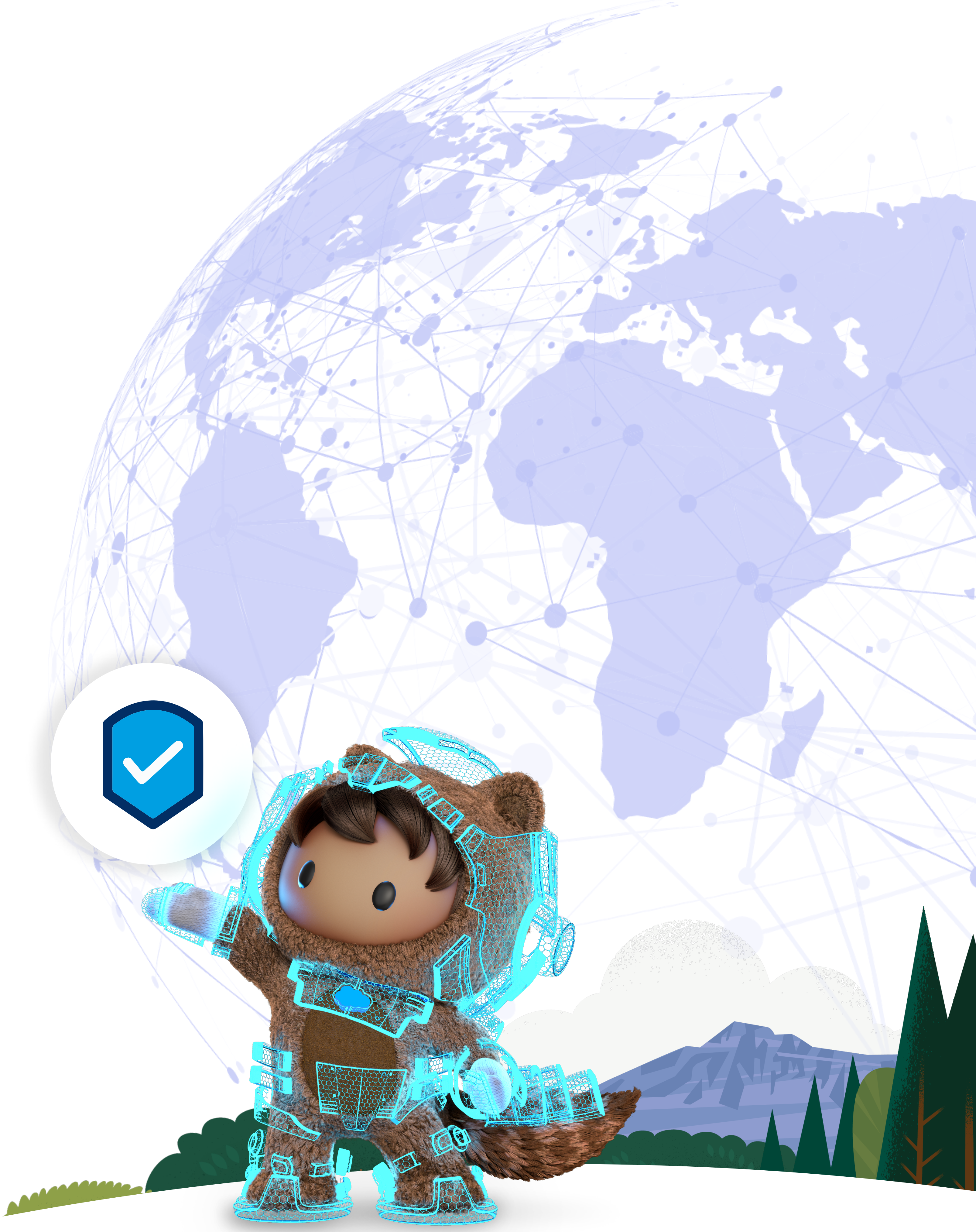
salesforce

Global Data Security Trends

300+ IT leaders detail must-have tools for their data security toolkit.



Contents

Executive Summary

Digital Urgency

As organizations look for ways to do more with less in the face of a possible economic downturn, digital transformation offers an essential lifeline. Digital-forward organizations can: automate without using code; build and use intelligent apps at scale; and secure and activate data in real time. However, these capabilities require rock-solid IT governance and the highest levels of security and compliance.

So, how are IT leaders juggling these demands on a global stage? Gartner Peer Insights and Salesforce surveyed 300 InfoSec and IT executives to find out. Get the key findings and data security best practices in this summary and the pages that follow.

Chapter 1

Security Enables Global Business

Eighty-one percent of surveyed IT leaders say their organization operates in multiple countries. However, even while acknowledging global vendor management and data security challenges inherent in a global business environment, the majority also report achieving high levels of international data compliance.

Chapter 2

Three Security Threats to Get Ahead of Right Now

Ongoing threats continue to make data security an unpredictable, and often treacherous, terrain to navigate. IT leaders are most concerned about **phishing, ransomware, and DOS/DDOS attacks**.

Chapter 3

Three Must-Have Tools for Your Data Security Toolkit

IT leaders frequently empower employees to be the first line of defense against attacks. In addition to employee vigilance, 80% report multi-factor authentication (MFA) as a top defense tactic, and identity and access management and data encryption are virtually tied as the next most effective tactics. Surprisingly, there's **one glaring gap in the IT leaders' security arsenal: backup and restore solutions**. Only 39% say it's a core component of their security strategy.

Chapter 4

Look Ahead: Top Data Security Tactics

IT leaders will remain on high alert for increased ransomware, phishing, and DOS and DDOS attacks. Expect the financial, banking, and insurance industries to be at the highest risk for cyberattacks.

Chapter 1

Security Enables Global Business

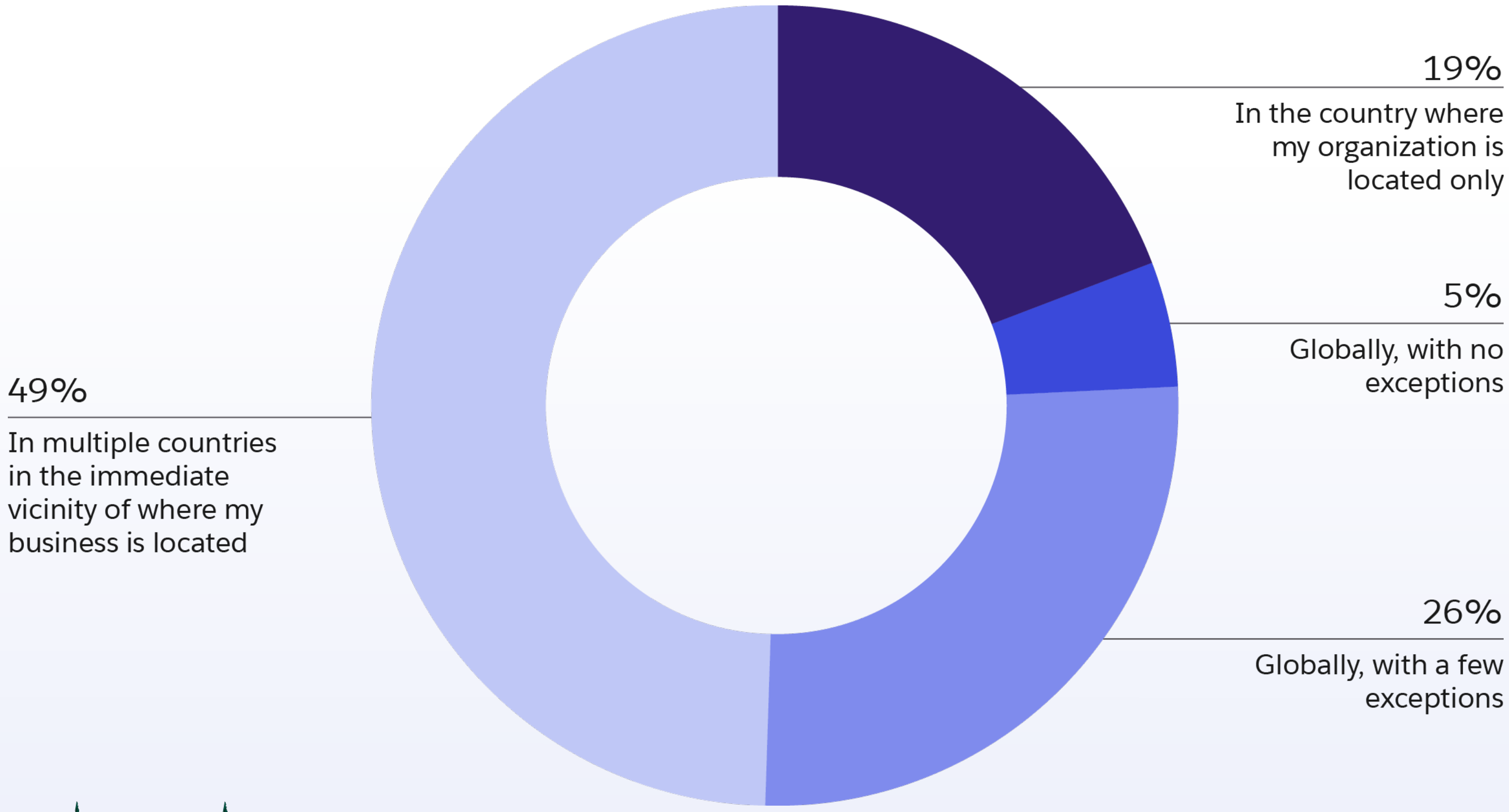
Digital transformation has enabled more businesses than ever before to operate without geographic borders. Eighty-one percent of respondents say their organization does business in multiple countries.

But the increasingly “borderless” landscape introduces additional business challenges. At the top of the list are data security and compliance.

Regional Insight

Ninety-two percent of respondents in EMEA say their business operates internationally. With 82% of APAC and 67% of AMER respondents reporting the same, the ripple effects from global data security threats make compliance a matter of critical urgency.

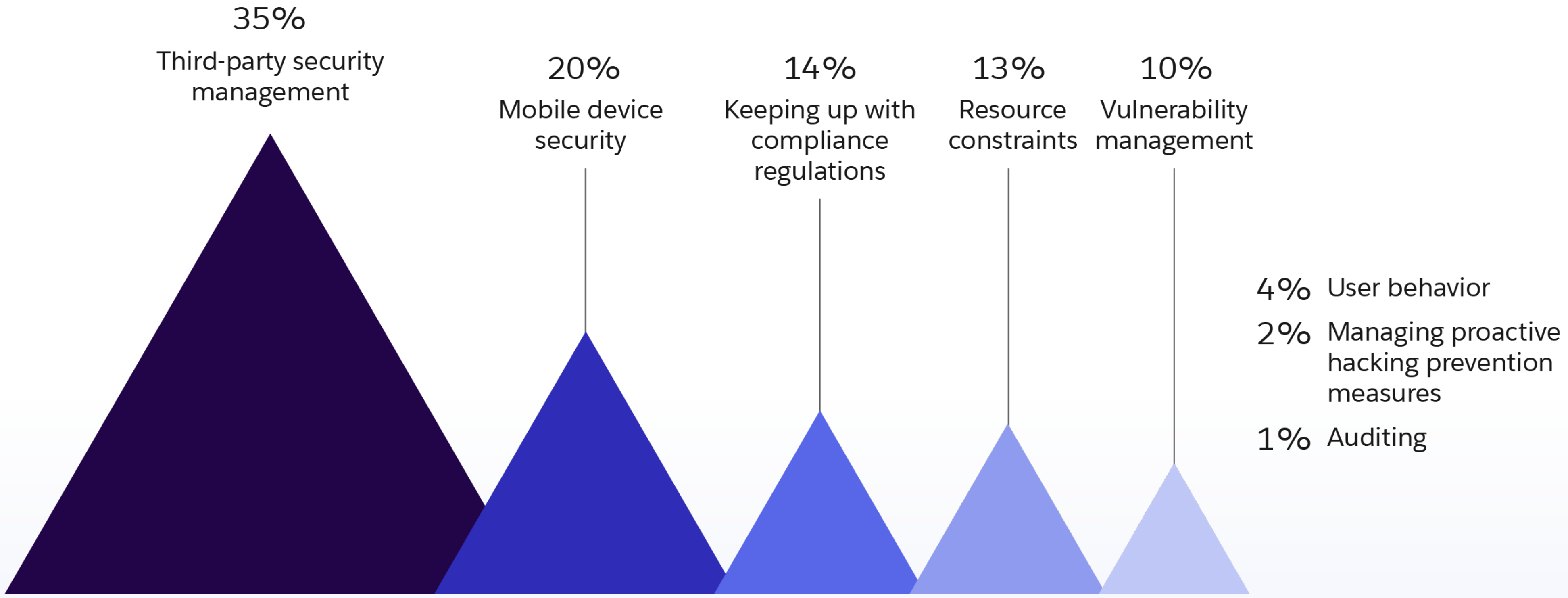
Where does your organization do business?



> “With more data protection laws being put into place … the compliance landscape for data security and privacy becomes much more difficult to navigate.”

VP, North America

In the last 18 months, what have been your top three pain points in managing data security?



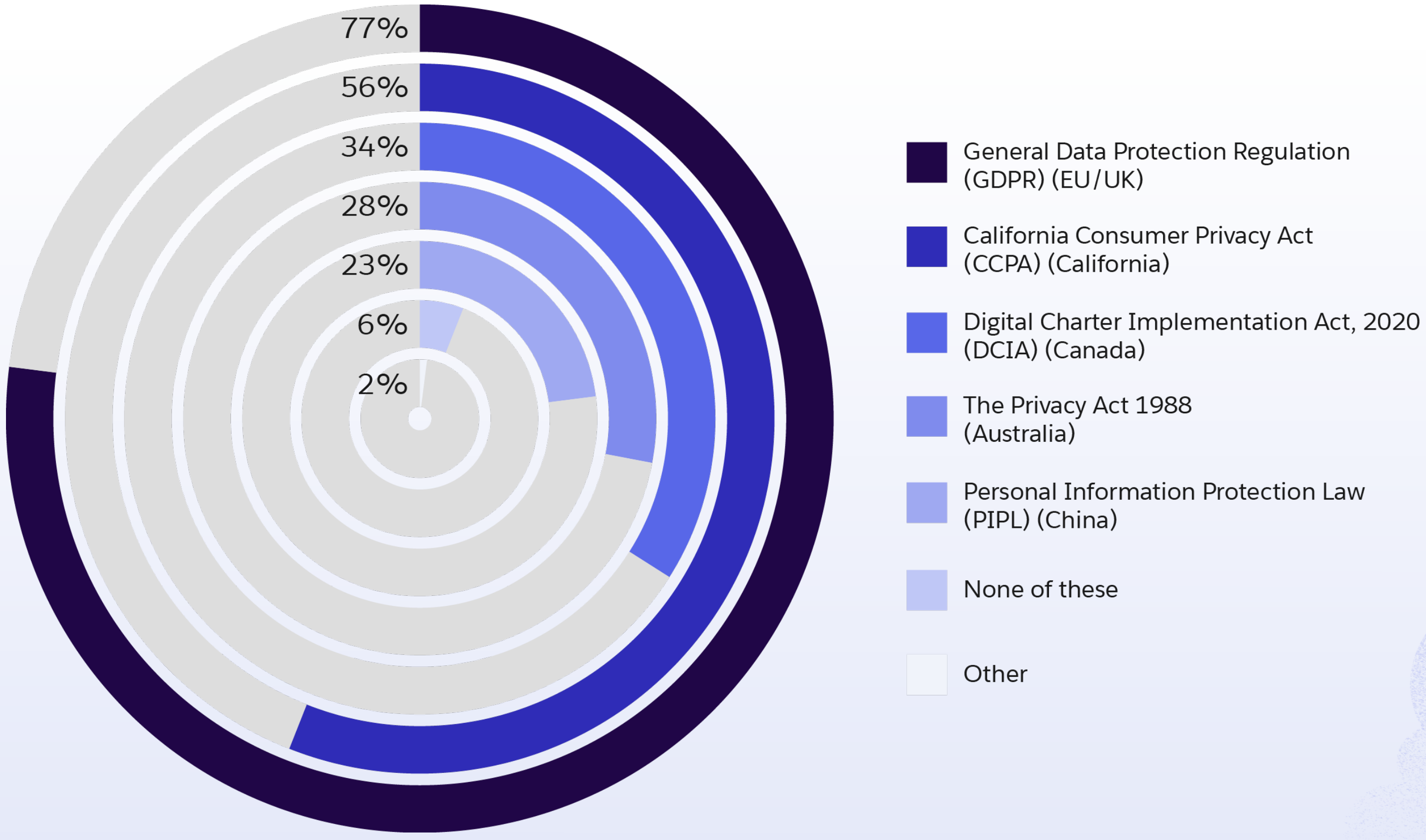
Data Security Capabilities Keep Pace with Compliance

Despite acknowledging compliance-management challenges, most global IT leaders say they have achieved high levels of international data compliance. However, additional technology investments to streamline compliance management could help ease the challenges of keeping up with and adhering to international regulations.

Regional Insight

Seventy-five percent of APAC respondents and 64% of North American respondents said they are GDPR compliant, which speaks to the significance of conducting business in Europe.

Which of the following international privacy laws is your organization compliant with?



> Most countries create their own privacy regulations, making compliance for business organizations increasingly difficult. There's a need for a governing framework which may form the basis of privacy laws worldwide.

VP, North America

Chapter 2

Three Security Threats to Get Ahead of Right Now

Due to global businesses' reliance on digital data, bad actors now have more targets and more opportunities to attack than ever before. According to a recent Ponemon Institute survey, 52% of organizations reported an increase in cyberattacks in 2022.

Within this persistent threat landscape, IT leaders in our survey identified phishing, **DOS/DDOS attacks, and insider breaches** as their top security concerns.

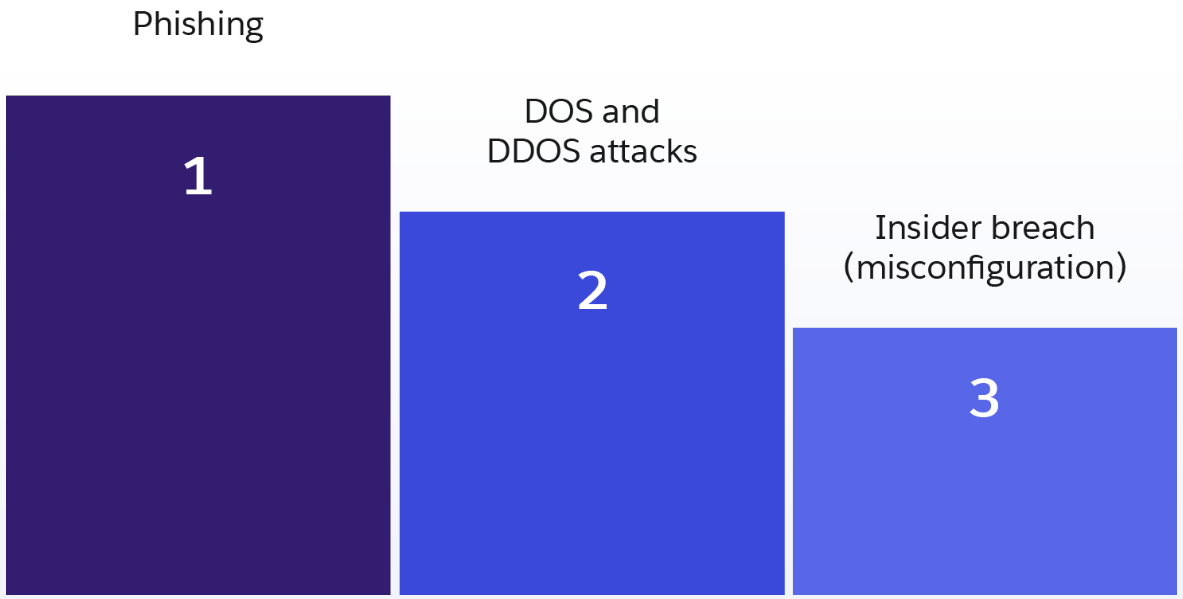
Regional Insight

Respondents in North America cited ransomware over insider breach as one of their top three security concerns.

> "The burdens upon companies to store and protect more data, and quickly leverage new systems and methodologies … often yields blindspots for organizations."
>
> VP, North America

What are your top three IT security concerns?

(top = highest level of concern, bottom = lower level of concern)



The Three Cyberattack Outcomes that Concern IT Leaders Most

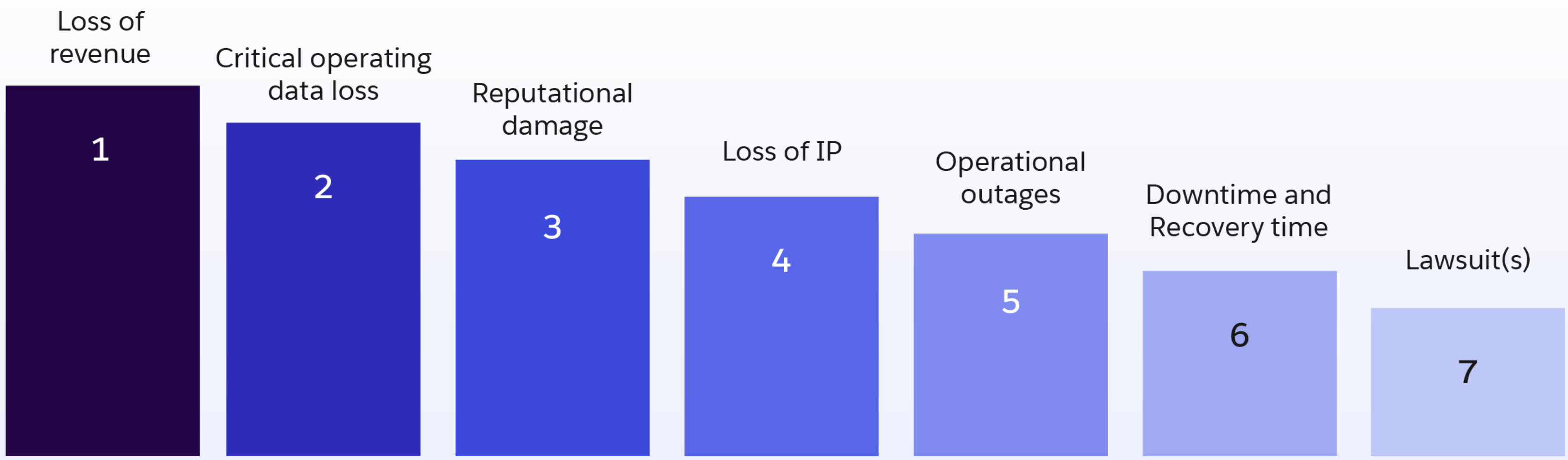
The average cost of a data breach stands at a staggering $4.35 million.[2] Unsurprisingly, **loss of revenue** is the cyberattack outcome weighing most heavily on IT leaders in the current economic climate. **Losing critical operating data and suffering reputational damage** are reported as their next greatest concerns.

Regional Insight

For leaders in APAC, the possibility of reputational damage replaces critical operating data loss as the number two concern when it comes to cyberattacks.

What potential cyberattack outcomes are you most concerned about?

(top = highest level of concern, bottom = lower level of concern):



> “Along with the continued movement into the cloud, there'll be an increase in malicious activity — in my experience, this happens whenever there's an economic downturn.”
>
> VP, North America

Chapter 3

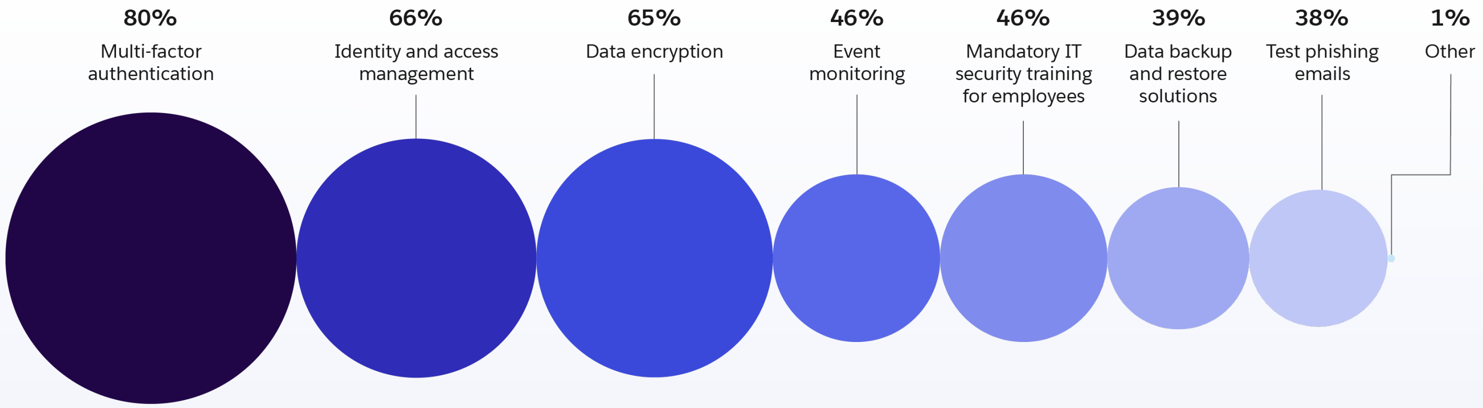
Three Must-Have Tools for Your Data Security Toolkit

What are the most powerful protections against cyberattacks? According to our findings, they're **data encryption, identity and access management (IAM), and multifactor authentication**. But there are some regional nuances.

Regional Insights

- **Multifactor authentication has the highest rate of adoption and success in APAC** – 84% of respondents said it's been effective in defending their organization against security attacks.
- **Seventy-one percent of North American respondents and 62% of respondents** in both EMEA and APAC included **data encryption as an effective security strategy**.
- **Sixty-nine percent of North American respondents, 67% of APAC respondents, and 61% of EMEA respondents said IAM is an effective** part of their security strategy.

What strategies have been most effective in defending your organization against security attacks? (Overall)



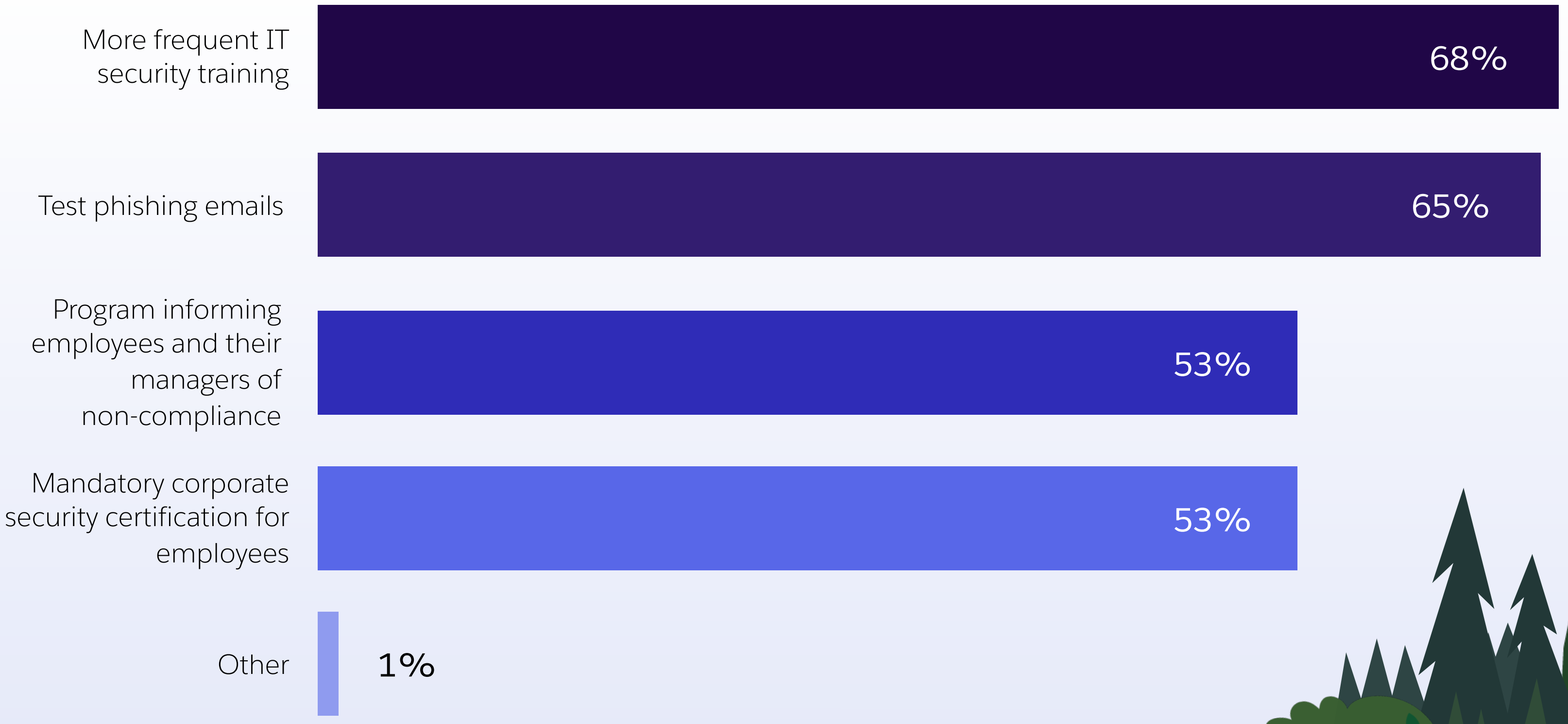
Employee Vigilance Is Key

Employees are a huge part of the data-security solution. And that's why the majority of leaders are empowering employees to be a first line of defense against cyberattacks. **Sixty-eight percent of leaders say that they are more frequently training employees on IT security tactics** to drive adoption of security measures.

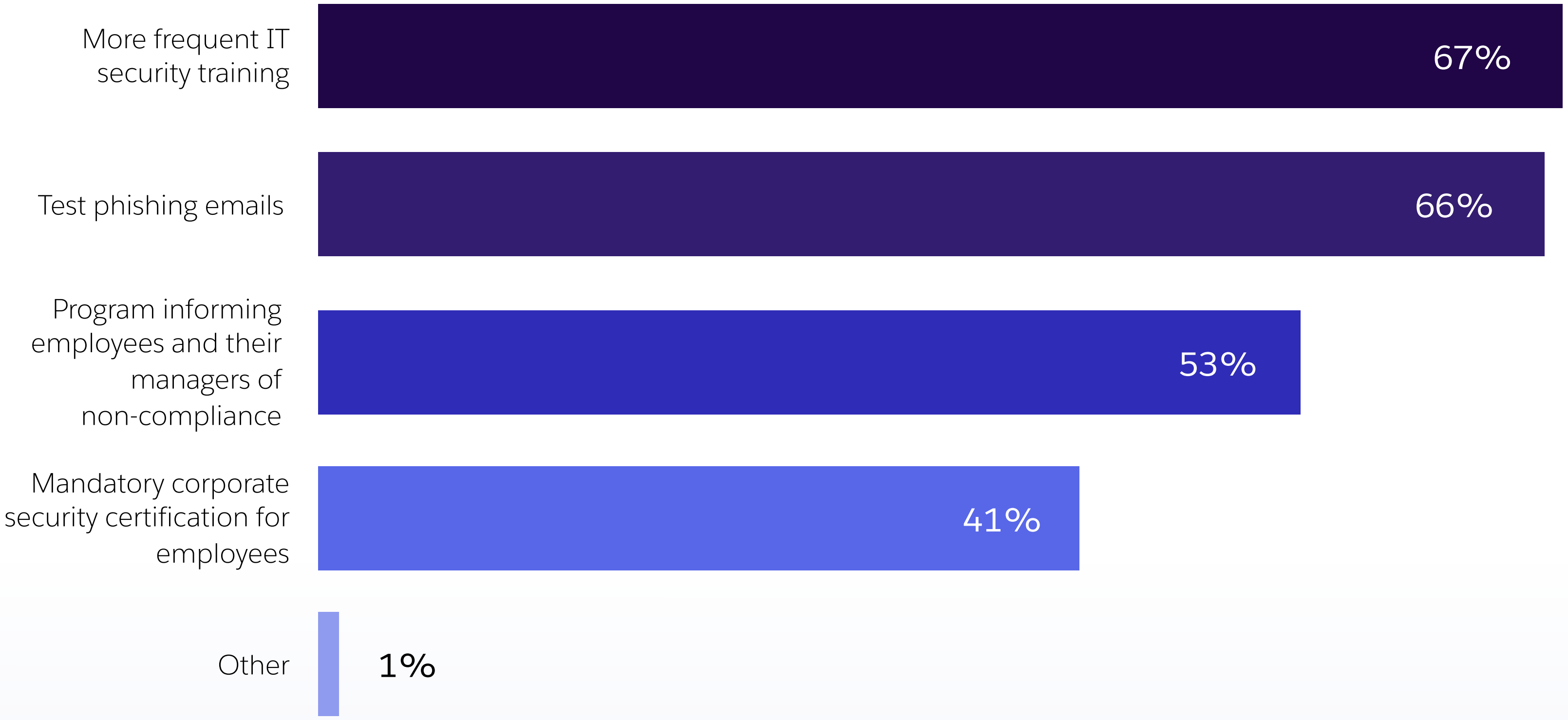
Regional Insight

While respondents in EMEA cite high levels of compliance with global privacy standards, they are far less likely to require mandatory corporate security certifications for employees. Just 41% of respondents from the region indicate that it is a part of their employee security strategy.

What are you doing to encourage employee adoption of IT security measures?



What are you doing to encourage employee adoption of IT security measures? (EMEA, n=101)



> One important element of our security posture is our people. We keep them trained for their roles, current risks, and new trends."
>
> C-Suite, North America

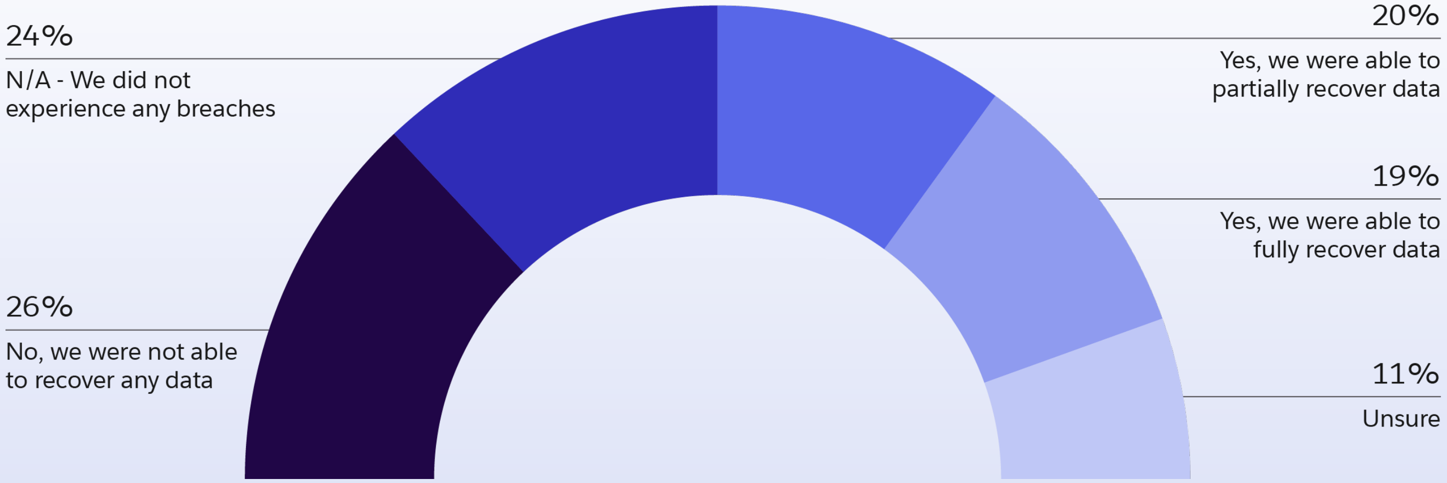
Cyberattacks Expose a Security Gap: Data Recovery

Nearly two-thirds (65%) of leaders reported experiencing a security breach between June 2021 and June 2022 – despite their best efforts. Among those who experienced a breach (n=227), 35% were not able to recover any data, highlighting the need for robust data recovery solutions. Of those who **did not** experience a breach (n=73), most (71%) used both an identity and access management solution **and** multi-factor authentication.

Regional Insight

- In EMEA, 40% of respondents who experienced a breach were unable to recover any data.
- **31% of respondents in APAC said they did not experience a breach between June 2021 and June 2022**. Among APAC respondents who did not experience a breach (n=31), 84% were using MFA.

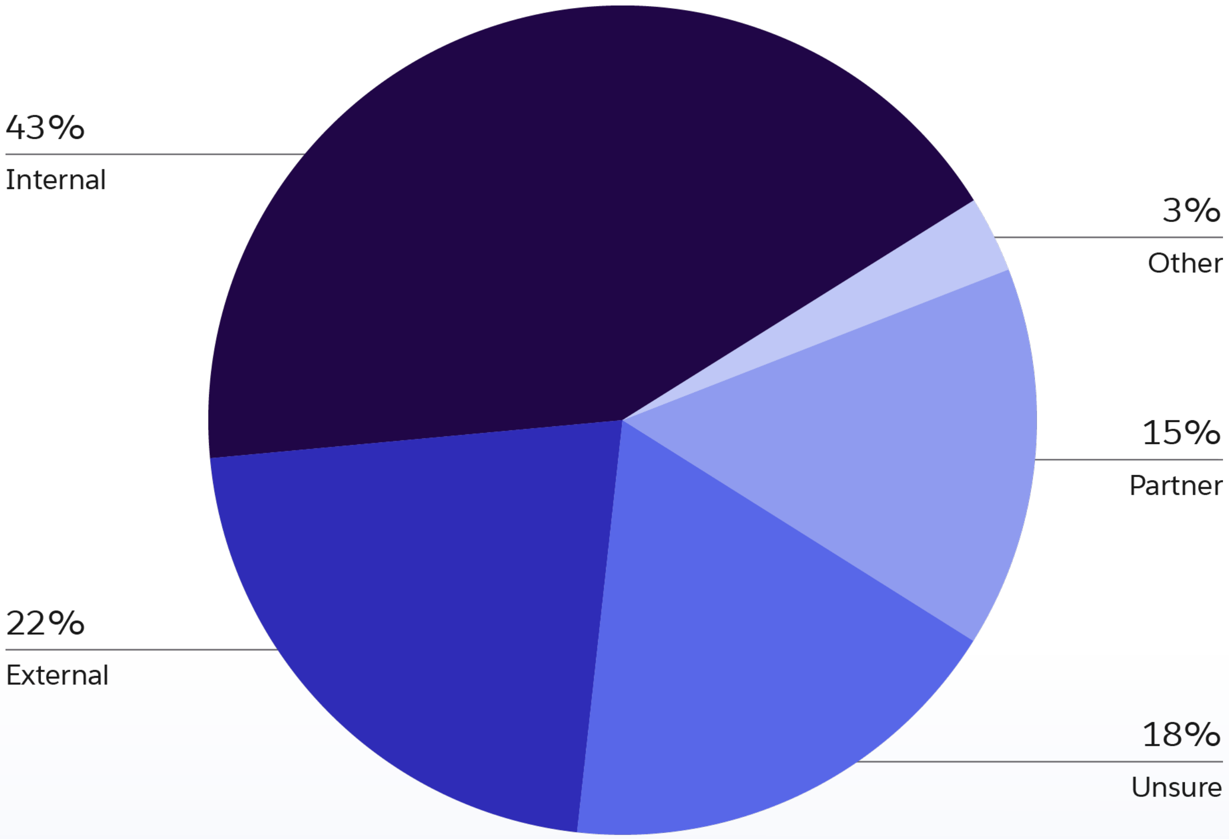
If you experienced a security breach between June 2021 and June 2022, were you able to recover data lost or corrupted during the breach?



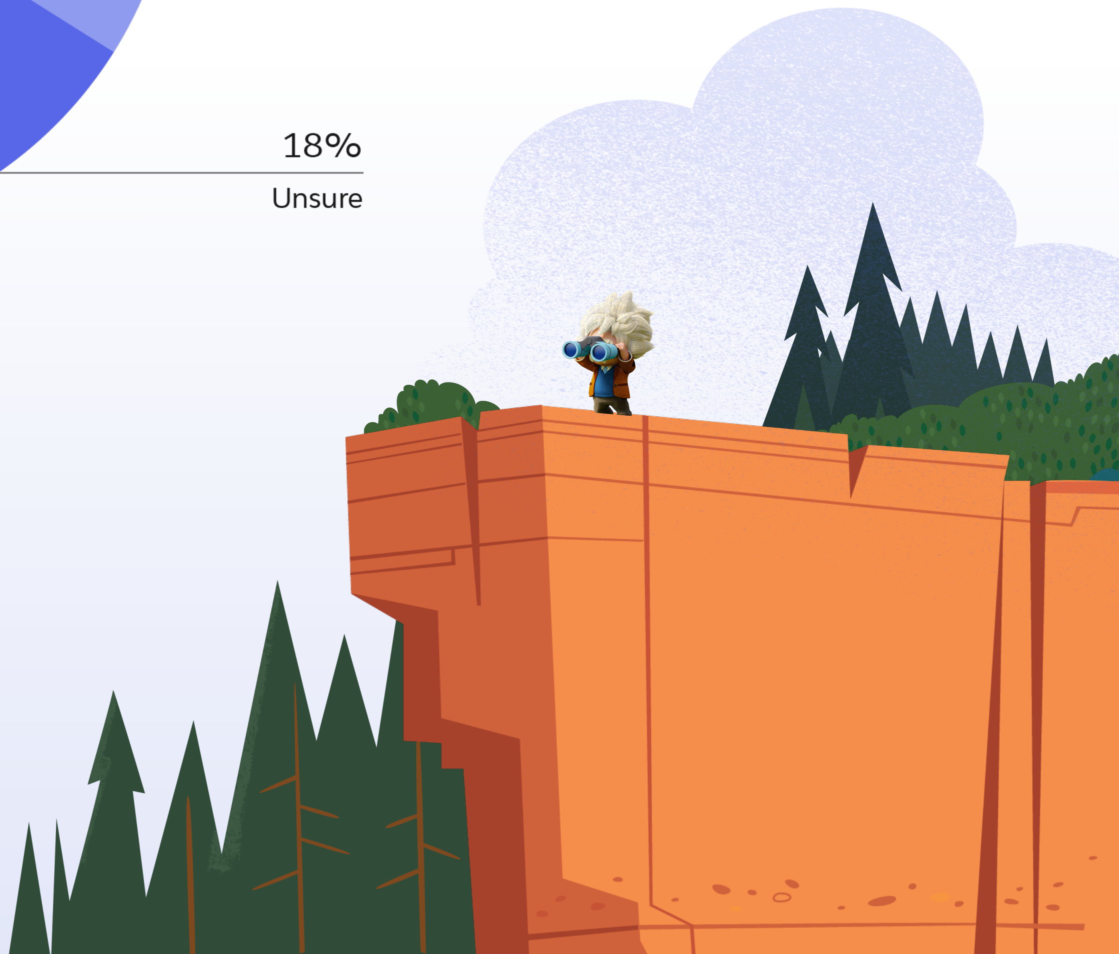
Quick Tip

Identity and access management is worth the investment. Forty-three percent of respondents who experienced a breach said the source of the breach was internal.

If you experienced a security data breach between June '21 - June '22, what was the source of the breach? (n=227)



> Enterprises will need … further encryption and more/better authentication and double down on internal cyber security awareness training and simulation."
>
> C-Suite, North America



Look Ahead: The Top Data Security Tactics

IT leaders will still remain on high alert for increased ransomware, phishing, and DOS and DDOS attacks. And they expect the financial, banking, and insurance industries to be at the highest risk.

Here are three ways to fortify your security strategy this year and beyond, according to our survey findings:

- **Ensure you have the right toolkit**: Data encryption, identity and access management, and multifactor authentication are the top countermeasures IT leaders are taking to guard their data.
- **Keep employees vigilant**: The more employees know about data security, the less likely they are to let bad actors into your enterprise.
- **Back up your data**: Data loss could be catastrophic to your business. So, protect your data with robust data backup and recovery solutions. And prioritize this as a core part of your security strategy.

Rank the top 5 industries you think are at the highest risk of experiencing a cybersecurity attack within the next 12 months

(top = highest risk, bottom = lower risk)

1 Finance, banking & insurance

2 Government

3 Educational services

4 Construction

5 Oil, gas & mining

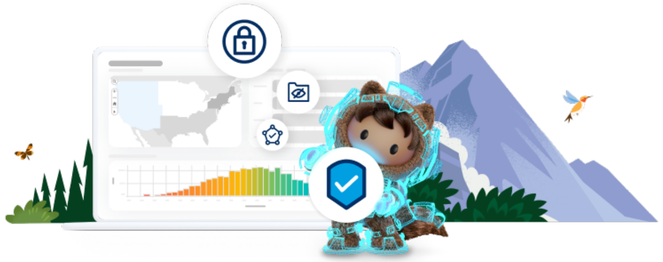
> “I think there will be more … need to safeguard against social engineering attacks that can increasingly take place outside of the traditional corporate environment.”
>
> Director, EMEA

Data Sources and Research Methodology

The Salesforce Global Data Security Study

Salesforce ran a study on trends in data security in Pulse's community of verified technology decision-makers. The 300 respondents – surveyed between July 31 and November 11, 2022 – included VPs and C-Suite InfoSec and IT executives in North America, EMEA and APAC. The executives worked for organizations with more than 1,000 employees.

Explore Tools to Secure Your Customer 360



How to Secure Your Data with Salesforce

Get the tools you need for data protection, privacy, and compliance – all on the world's most trusted platform.

Get the solution brief

Enhance Compliance with Salesforce Security, Identity & Privacy

Compliance regulations shouldn't slow you down. Learn more with this guide.

Get the white paper

How To
Protect, Monitor, and Retain Critical Salesforce Data with Shield
Data Secured
Which API Entities Are Most Used?

How to Protect, Monitor, and Retain Critical Salesforce Data with Shield

Discover four powerful capabilities that help you ensure the sensitive data in your Salesforce Environment is safe.

Get the datasheet

The information provided in this report is strictly for the convenience of our customers and is for general informational purposes only. Publication by Salesforce does not constitute an endorsement. Salesforce does not warrant the accuracy or completeness of any information, text, graphics, links, or other items contained within this guide. Salesforce does not guarantee you will achieve any specific results if you follow any advice in the report. It may be advisable for you to consult with a professional such as a lawyer, accountant, architect, business advisor, or professional engineer to get specific advice that applies to your specific situation.