Secure Your AI Enterprise

Key Security Trends in the Age of AI

Contents

Introduction

Artificial intelligence and generative AI are increasingly at the heart of business strategies everywhere. These technologies, which rely heavily on vast amounts of data, offer incredible opportunities to create new customer experiences and offload manual employee tasks.

However, implementing AI tools can also introduce data security and privacy challenges.

AI models process terabytes of information. As a result, managing data can get complex quickly. At the same time, these tools present unique risks that must be proactively and carefully addressed. This report dives into the latest trends in security for AI, exploring the obstacles businesses face today and how you can equip your organization to employ AI in a safe and trusted manner.

Mind the gap

Balancing fast innovation and trusted security

Organizations are eager to harness AI's potential. However, that eagerness can put undue pressure on IT teams. Today, **88% of IT workers** report that they're unable to meet leadership's demands. With a significant **AI trust gap** across the industry, organizations cannot sacrifice trust for speed. It's clear that there must be a balance between innovation and security.

The growing demand for AI-driven projects strains IT departments to deliver complex solutions quickly while maintaining strong security measures. Around **67% of IT departments** report facing difficulties in harmonizing business and security demands, while almost half of IT workers struggle to strike a balance between speed, business value, and security when implementing new technology.

When organizations successfully balance AI innovation with strong security practices, they can innovate freely, improving their creative and strategic processes. By incorporating security protocols early into one's AI strategy, companies can double down on their core value proposition with the force-multiplier of AI, while safeguarding the organization's data, reputation, and overall security posture.

of IT departments report facing difficulties in harmonizing business and security demands

Salesforce 3rd Edition State of IT Report

01

What are the biggest roadblocks to secure AI implementation?

01 What are the biggest roadblocks to secure AI implementation?

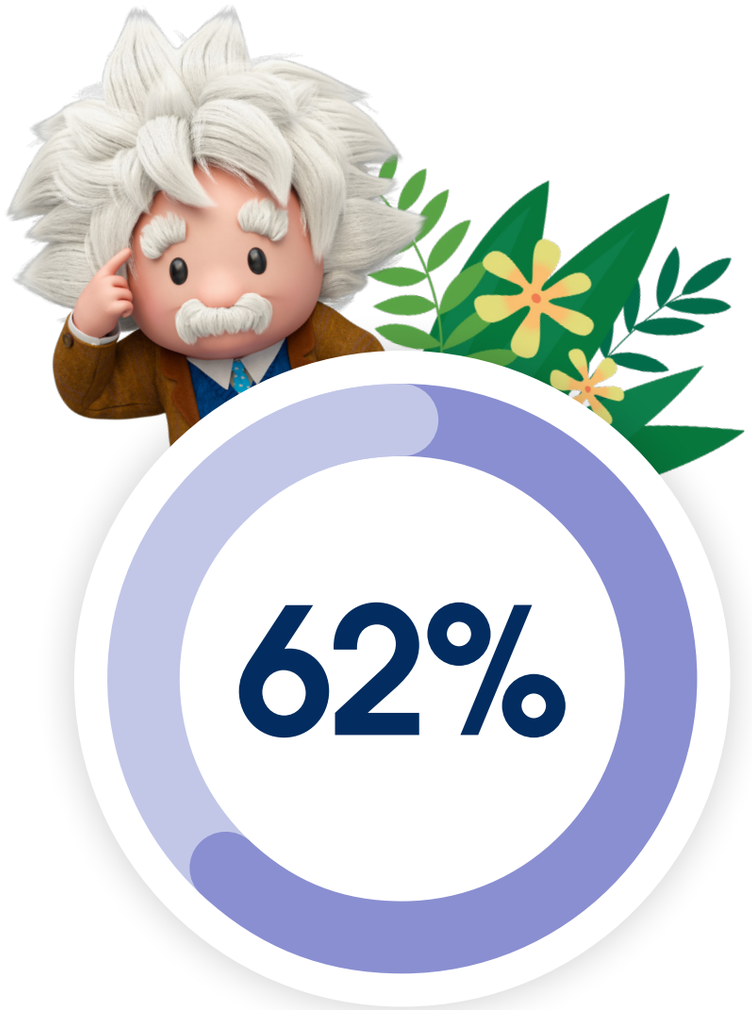
Many organizations face significant challenges when trying to integrate AI into their projects. IT teams have to wade through technological hurdles, staffing shortages, or a growing threat landscape before they're able to fully leverage AI's benefits.

Let's explore some of those challenges and examine how IT leaders can make the most of their AI investments.

Legacy systems make AI more vulnerable to attacks

Just over a third of IT leaders identified legacy infrastructure and systems as a significant challenge for digital transformation. These outdated systems often lack the advanced security features and integration capabilities to support modern AI technologies. As a result, they become vulnerable points within an organization's IT landscape, potentially exposing sensitive data to cyber threats.

This challenge is compounded by legacy systems, with almost 62% of IT leaders stating their organizations aren't equipped to leverage AI technologies while integrating with existing systems. Legacy systems typically operate in isolated silos, making it difficult to integrate and secure data across an organization.



of IT leaders said their organizations aren't equipped to leverage AI technologies while integrating with existing systems

Mulesoft 2024 Connectivity Benchmark Report

01

Such fragmentation slows the development and deployment of AI solutions and increases the risk of data breaches and other security incidents by expanding an organization's threat surface. Addressing these challenges requires organizations to modernize their IT infrastructure, often centralizing data first to ensure that future AI implementations are impactful and secure.

There is a critical shortage of IT security professionals

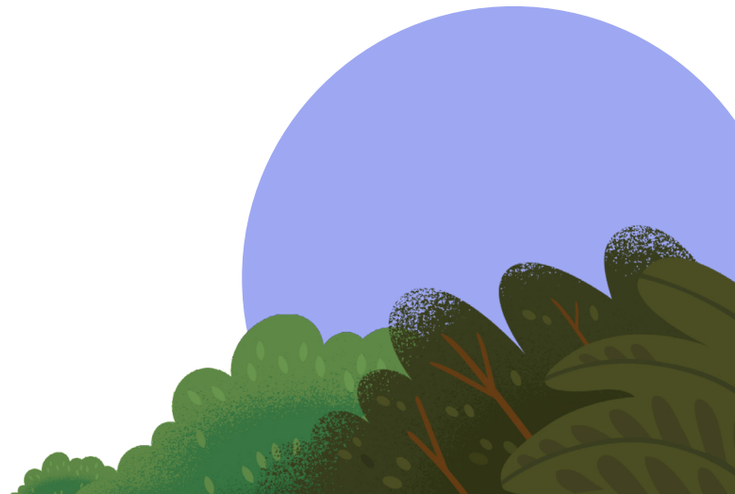
Due to the rapid pace of technological advancements and the increasing sophistication of cybercriminals, the demand for qualified IT security professionals has never been higher. However, demand is outpacing supply, placing more pressure on existing security teams. A striking **67% of cybersecurity workers** reported that their organizations face a shortage of cybersecurity staff necessary to prevent and troubleshoot security issues. At a time when organizations must protect their AI systems from emerging threats, the growing cybersecurity workforce gap can leave AI implementations vulnerable to attacks.

The skills gap in cybersecurity is widespread, with **92% of current cybersecurity professionals** acknowledging that their organizations lack the necessary skills in one or more areas. Lack of expertise hinders the ability to effectively secure AI applications that rely on sensitive data. Without proper security protocols implemented by skilled security IT professionals, many organizations and their AI systems are at increased risk of breaches, which could lead to data loss and operational disruptions.

The security talent shortfall

The global cybersecurity workforce is short by **4 million professionals**, with skills gaps most prominent in the following areas:

- Cloud computing
- AI and machine learning
- Zero trust implementation



01 Cybercriminals are getting more sophisticated

As technology advances, cybercriminals will continue to evolve their tactics. For example, some cybercriminals today are developing AI models that can bypass AI-based security measures. Others are using adversarial attacks to specifically target AI and machine learning models and cause them to misbehave. The increasing sophistication of cyberattacks presents a mounting challenge to secure AI implementation.

With the average cost of a breach in the US reaching $4.45 million – a **15% increase over three years** – sleeping on security is an expensive risk. But these breaches aren't just costly. They're also damaging to customer trust and company reputation. To securely adopt AI, organizations must embrace a comprehensive security strategy covering the infrastructure and application layers.

Improving data quality, strengthening security, and building out AI capabilities are the **top three priorities** for analytics and IT leaders. These priorities highlight the need to balance AI innovation and robust security standards.

Now that we've examined the challenges, let's look at some of the biggest areas of concern when it comes to ensuring secure AI adoption.

IT leaders rank security threats as their top challenge. Now, with AI entering the scene, these challenges are only growing.

- **48% of IT teams** worry that their current security infrastructure can't keep pace with the rapid advancements in AI technology
- **54% of IT leaders** acknowledge the need for enhanced security measures to successfully implement generative AI

02

AI concerns and consequences

02 AI concerns and consequences

There are many security factors to consider in today's age of AI. Three critical concerns are data governance, security, and resilience. Let's examine what differentiates these concerns and why they're key to securing AI.

Data governance

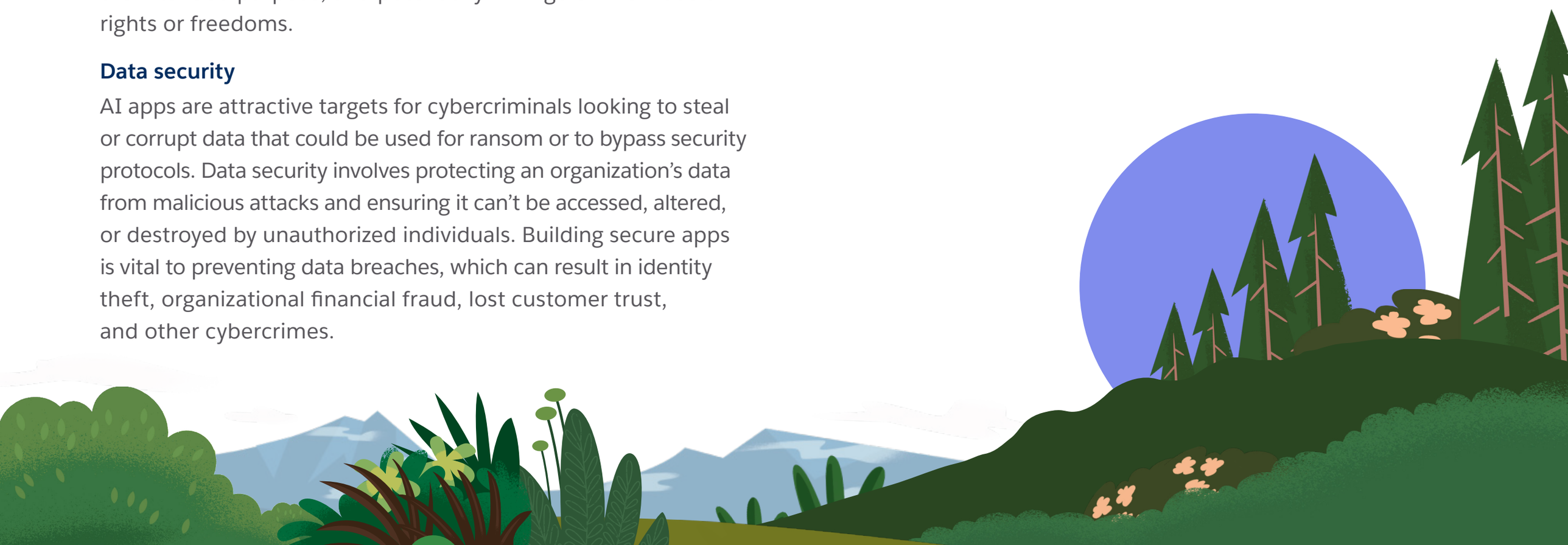
In AI, governance and privacy concerns stem from large datasets that include personal details, like a customer's home address or bank account information. Effective data governance and privacy help protect personal information from unauthorized access and ensure that individuals have control over their data. Without the proper data privacy measures, AI systems may unintentionally disclose private information, use data beyond the intended purpose, and potentially infringe on individuals' rights or freedoms.

Data security

AI apps are attractive targets for cybercriminals looking to steal or corrupt data that could be used for ransom or to bypass security protocols. Data security involves protecting an organization's data from malicious attacks and ensuring it can't be accessed, altered, or destroyed by unauthorized individuals. Building secure apps is vital to preventing data breaches, which can result in identity theft, organizational financial fraud, lost customer trust, and other cybercrimes.

Data resilience

Data resilience refers to the ability to recover from events that affect data integrity and availability. For AI, this means withstanding and quickly recovering from events like cyberattacks, internal human errors, or hardware failures that can happen due to natural disasters. Resilient systems keep critical operations running smoothly while data is promptly restored, ensuring reliability and trust in AI applications.



02 Where are these concerns felt the most?

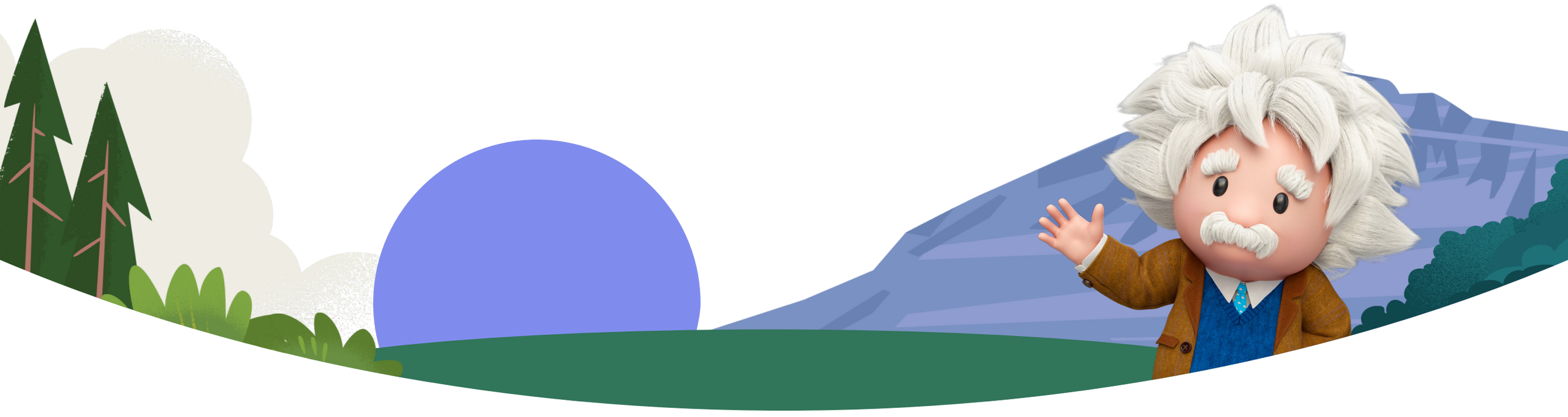
Security concerns are highest in the energy and utilities, public sector, manufacturing, and financial services industries, due to the critical nature of the sensitive data involved.

In the **energy and utilities industry**, infrastructure is essential for maintaining daily life and national security, making it a prime target for cyberattacks that could disrupt services and cause widespread impacts. Similarly, the **public sector** deals with vast amounts of personal and confidential information. Breaches in this sector can seriously impact customer privacy and national security.

In the **manufacturing and financial services industries**, stakes are also high. Manufacturing companies often rely on intricate supply chains and automation systems that, if disrupted by a cyberattack, could halt production and lead to significant economic losses. Additionally, intellectual property and trade secrets are at risk, which could damage competitive advantage and innovation.

Financial services handle vast amounts of sensitive financial data, including personal information and transaction records, meaning cyberattacks can result in financial fraud, identity theft, and significant economic disruption.

Given the potential consequences, ensuring robust security measures in these industries is critical to maintaining operational integrity and protecting sensitive data.



02 The consequences of pushing innovation over security

Addressing security concerns is key to building trusted AI. Even when the drive to innovate with AI is strong, security must be prioritized alongside innovation. That's because failure to ensure proper data governance and privacy, data security, and data resilience comes with serious risks, including:

- **Loss of user trust:** If users perceive that their data is not handled with the highest level of privacy, they may lose trust in the organization.
- **Legal and regulatory penalties:** Non-compliance with data privacy laws can result in significant fines and legal actions.
- **Reputational damage:** Privacy breaches can damage an organization's reputation, leading to a loss of customers and partners.
- **Data breaches:** Insufficient security measures can result in data breaches, exposing sensitive information.
- **Financial loss:** The costs associated with a security breach can be substantial, including legal fees, compensation, and loss of business.
- **Intellectual property theft:** Poor security can lead to the theft of proprietary algorithms or business strategies.
- **Operational disruption:** Without resilient data systems, AI applications may fail, causing operational disruptions.

Prioritizing security means being proactive and taking comprehensive steps to ensure privacy, security, and resilience from day one. By taking the steps to understand how secure and resilient your enterprise is against threats, you can make the necessary changes to prepare your IT landscape for secure AI implementation.

of IT leaders cite security as a top priority

Salesforce 3rd Edition State of IT Report

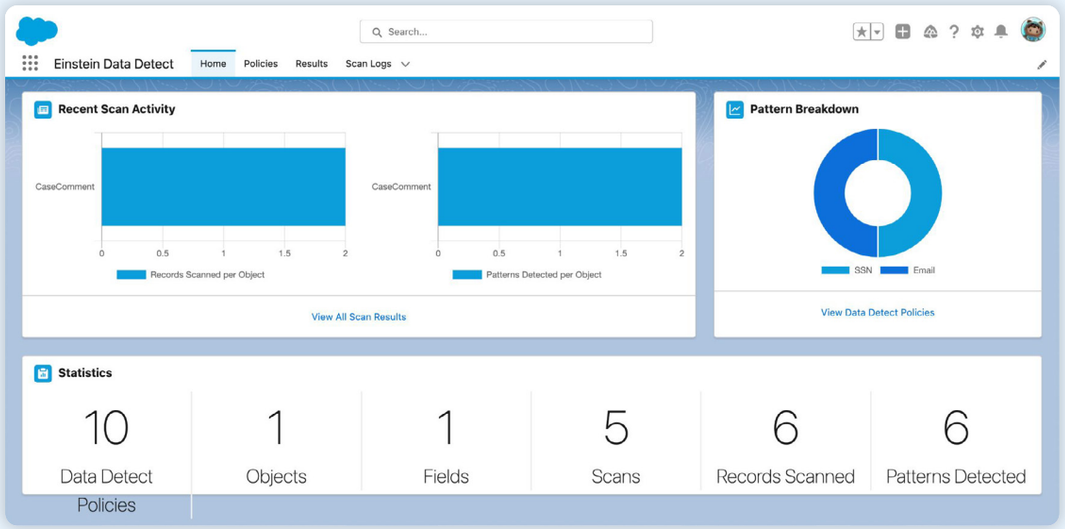
03

How to strike a balance between security and AI innovation

03 How to strike a balance between security and AI innovation

Designed for powerful AI app development, the Salesforce Platform helps organizations build generative AI apps and automation on their unified CRM data. It also helps ensure data security, privacy, and resilience so teams can develop solutions quickly without derailing their strategies.

Explore some of the security solutions that come with the Salesforce Platform and how they work to protect AI-driven initiatives so teams can innovate while staying secure.

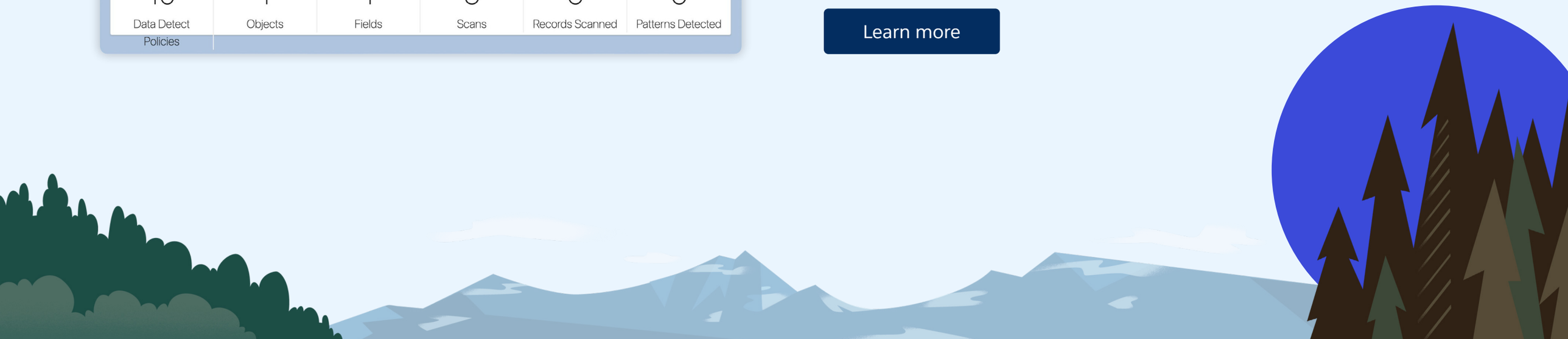


Monitor activity and mitigate threats with Salesforce Shield

Salesforce Shield is a suite of security tools built to secure sensitive data within Salesforce. Shield can help you maintain data visibility, prevent security threats, and comply with global privacy regulations.

- **Block unauthorized or unlawful activity:** Create real-time security rules to prevent undesired events with Event Monitoring.
- **Find and classify sensitive data quickly:** Use pattern matching to easily locate critical customer data and address non-compliant information with Data Detect.
- **Give sensitive data additional security:** Encrypt sensitive data at rest and manage keys with Platform Encryption.
- **Meet compliance and industry regulations:** Track changes to critical data and retain data history indefinitely, or until you choose to delete it with Field Audit Trail.

Learn more

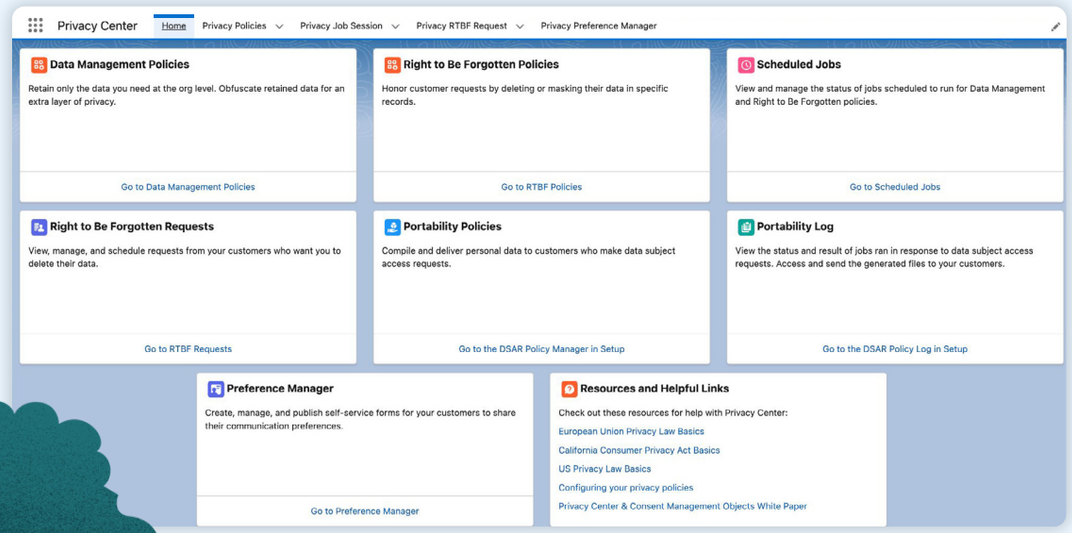


03 Simplify data compliance and verify consent with Salesforce Privacy Center

Privacy Center includes data management tools that help you manage and comply with privacy laws and support your legal obligations related to data storage, deletion, and masking.

- **Manage and protect sensitive data:** Securely manage the data lifecycle and perform anonymization, pseudonymization, and deletion.
- **Control customer data requests:** Create policies to fulfill Right To Be Forgotten quickly (RTBF) and Data Subject Access Requests (DSARs).
- **Streamline customer preferences:** Easily customize forms in Privacy Center's Preference Manager to capture consent and keep data consistent across your organization.

Learn more

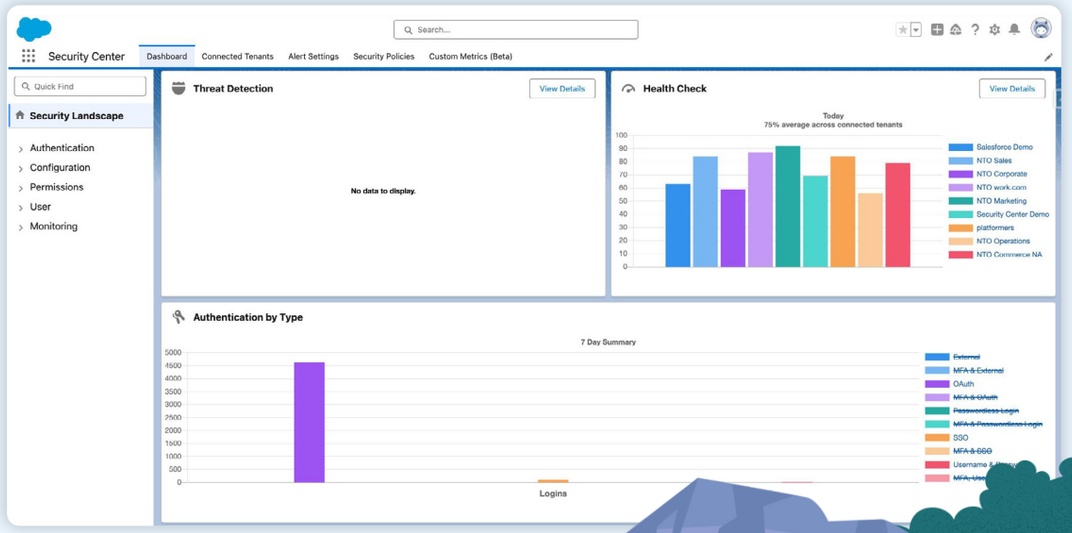


Grant the right access for AI processes with Salesforce Security Center

Security Center provides a unified view of security data across Salesforce environments, allowing administrators to continuously monitor and manage your security posture.

- **Improve security performance:** Track your organization's security posture and gain insight into key changes like inactive users, unusual login activity, user access permissions, configurations, and more.
- **Reduce security risks:** Simplify security management with an operational view of your entire Salesforce rollout.
- **Eliminate potential blind spots:** Aggregate metrics in a consolidated view, set up alerts, and apply consistent security policies across all of your connected tenants.

Learn more



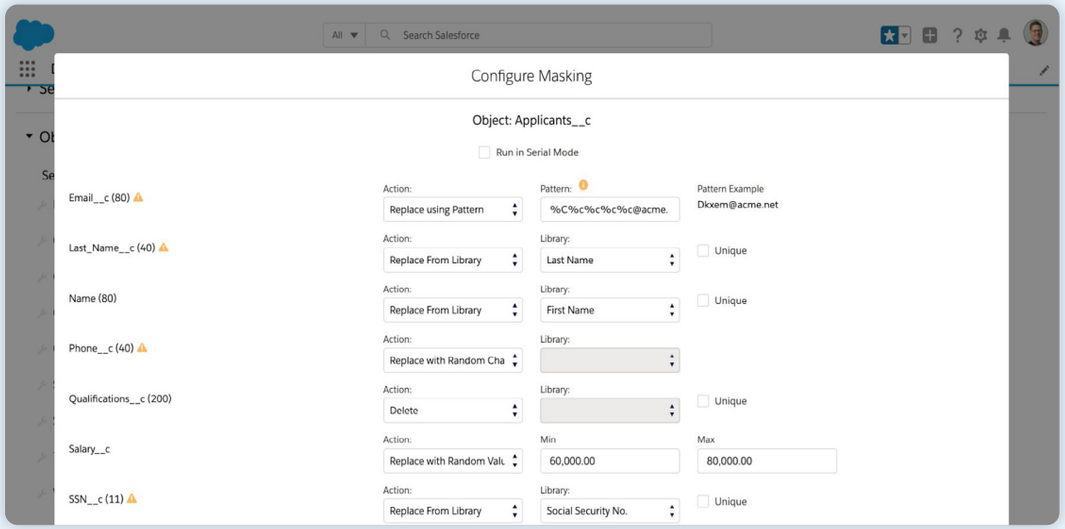
03

Protect data for AI prompts and training with Salesforce Data Mask

Designed to help Salesforce administrators and developers secure sensitive data within Sandbox environments, **Data Mask** helps protect information during development, testing, and training processes.

- **Work with realistic data:** Increase developer productivity while maintaining a secure testing environment.
- **De-identify data and manage compliance:** Protect your PI and PII by anonymizing data to securely build and customize with a 100% native approach.

Learn more

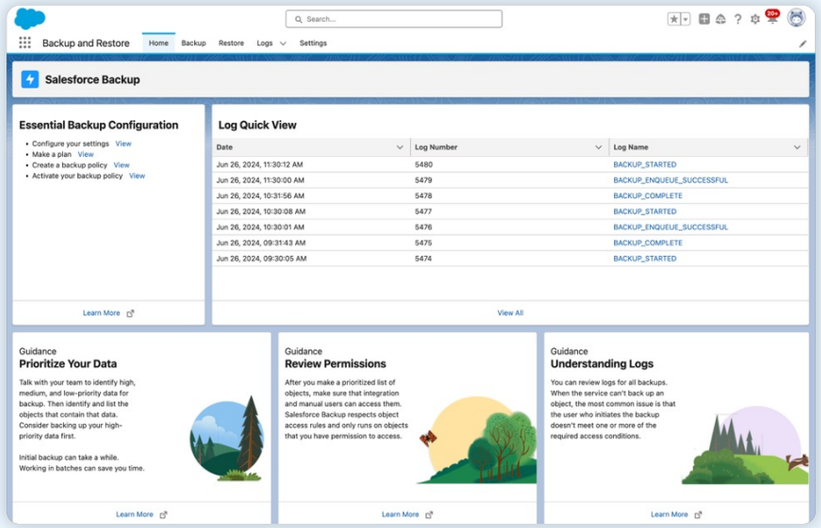


Prevent data loss and corruption with Salesforce Backup

Preserve data integrity and ensure business continuity while adopting AI technologies. **Salesforce Backup** makes it easy to set policies that ensure CRM data is securely backed up and can be swiftly restored in the event of data loss or corruption.

- **Easily deploy backups:** Use an intuitive interface that lets administrators configure and manage backup tasks without requiring extensive technical expertise.
- **Quickly restore data:** In the event of data loss or corruption, use rapid data restoration to minimize business downtime.

Learn more



03 Helping customers secure their digital transformations

Salesforce helps organizations in highly regulated industries balance innovation and security to protect sensitive information and maintain customer trust. Read about some of their stories below.

Humana

Healthcare

Humana built a digital pharmacy to give members a hassle-free way of getting their prescriptions. Shield allowed the company to encrypt sensitive health data and meet strict HIPAA compliance standards. By partnering with Salesforce, Humana moved away from costly middleware and saved $6 million yearly in security-related costs.

"We don't just buy a product with Salesforce. We have a partner, who is like our extended support team and monitoring team,"

said Hendry Wiebe, Cloud Services Management Fellow at Humana.

Read the story

RBC Wealth Management

Financial Services

With the help of Salesforce experts, **RBC Wealth Management** brings 26 disparate systems together to provide clients with more personalized banking experiences. Given the tight regulations around financial services firms, the company uses encryption and other security measures within Salesforce Shield to protect sensitive personal and financial data.

Read the story

Conclusion

Launch your AI journey from a secure, trusted foundation with Salesforce

Launch your AI journey from a secure, trusted foundation with Salesforce

With Salesforce, you shouldn't have to sacrifice security while implementing AI apps. Starting your initiative with a security-first approach is crucial for safeguarding sensitive data, maintaining customer trust, and ensuring compliance – all while providing an optimal, personalized customer experience.

The Salesforce Platform enables you to prioritize both security and innovation by offering integrated security features such as encryption, secure access controls, and continuous monitoring. These capabilities help protect your data against breaches and unauthorized access while you develop the solutions of tomorrow using advanced technologies. Learn more about how Salesforce helps protect your organization today while innovating for the future.

Salesforce Platform security

Read the 3rd State of IT Report

Contact an expert to learn more