vorlon

WHITE PAPER

2025 SaaS Ecosystem Security Best Practices

Lessons Learned From the 2024 Breaches Heard 'Round the World'

Introduction

In this whitepaper, we will summarize a few major breaches in 2024, analyze their impacts, and provide insights on how businesses can enhance their cybersecurity postures to mitigate similar risks in 2025.

The Verizon DBIR notes a **68% year-over-year increase in third-party breaches**, emphasizing the growing risk associated with these external partnerships. This trend highlights the urgent need for organizations to reinforce their data security measures and enhance their oversight of third-party interactions to safeguard sensitive information effectively.

Year-over-year increase in third-party breaches

68%

2024's Major Saas Ecosystem Data Breaches

Each third-party breach listed below describes the security gaps that were exploited, the consequences of the breach, and how each organization responded.

BANK OF AMERICA

snowflake

AT&T

TOYOTA

ticketmaster

GitHub

HealthEquity

Bank of America

A data breach at Infosys McCamish, a financial software vendor, exposed the sensitive personal information of 57,028 deferred compensation customers of Bank of America. This breach, which occurred on November 3, was perpetrated by the ransomware group LockBit, who accessed the data not through Bank of America's systems but through Infosys McCamish's systems.

The compromised data included names, addresses, dates of birth, Social Security numbers, and other account details. Despite the incident being promptly identified, affected customers were only notified on February 2, nearly three months later. In response, Bank of America offered the affected customers two years of identity theft protection.

Ticketmaster

In May 2024, Ticketmaster experienced a significant cybersecurity breach, affecting an isolated cloud database managed by a third-party provider, which housed limited personal information of some North American customers. This breach exposed customers' emails, phone numbers, and encrypted credit card information. Despite the breach, no further unauthorized activity was detected following a comprehensive investigation with cybersecurity experts.

Ticketmaster has affirmed the security of customer accounts and has not found any impact necessitating password resets. The company has proactively engaged with law enforcement and financial institutions to bolster data protection and is offering affected customers a 12-month free identity monitoring service.

Snowflake

The recent data breach targeting Snowflake's data storage services, identified in May 2024, has potentially impacted up to 165 organizations, affecting potentially hundreds of millions of individuals. The breach was executed by exploiting outdated, stolen credentials and security gaps in multi-factor authentication and access restrictions. Mandiant identified the group responsible as UNC5537, a North American cluster with ties to Turkey, focused on extortion. In response, Snowflake is moving to mandate multi-factor authentication for its customers.

AT&T

In January 2023, AT&T faced a significant data breach involving a third-party cloud vendor, resulting in data theft from over 8.9 million AT&T Mobility customers. The breach, which included subscriber and billing information, occurred through a vendor AT&T used for marketing and personalized content.

The Federal Communications Commission (FCC) has fined AT&T $13 million, holding it responsible for the incident, as the stolen data should have been deleted by the vendor years prior. The settlement also requires AT&T to enhance its data protection practices, including implementing annual compliance audits and a comprehensive information security program. The breach has prompted increased scrutiny from the FCC on how companies manage and protect customer data through their third-party vendors.

Toyota

Toyota confirmed a data breach involving a third-party entity, leading to the exposure of 240GB of sensitive customer and employee data. The breach did not compromise Toyota's systems directly but occurred through a third-party misrepresented as Toyota. The data, leaked by threat actor ZeroSevenGroup on December 25, 2022, included personal, financial, and network information.

While Toyota has not disclosed the third party involved or detailed the number of affected individuals, the incident is part of a series of data security challenges Toyota has faced, including previous breaches and misconfigurations in cloud services. Following these, Toyota has enhanced its data security measures.

Github

In March 2024, GitHub experienced a significant security breach with unauthorized access to its code repositories. The breach potentially exposed sensitive data, including passwords, usernames, email addresses, and other critical details within the repositories. The exact number of affected accounts remains undisclosed, and the methods used by the attackers to gain unauthorized access are still under investigation.

In response to the incident, GitHub implemented several security measures to safeguard its platform. These included enhanced monitoring and detection capabilities, comprehensive investigations, and collaboration with impacted users to mitigate risks. GitHub also advised developers and organizations to strengthen their repository security by enabling two-factor authentication, updating passwords regularly, and auditing access controls. While GitHub has not explicitly contacted affected users, those concerned about their account security can check if their email addresses have been compromised in any data breaches through services like Have I Been Pwned.

Health Equity

HealthEquity, a Utah-based healthcare benefits administrator, notified 4.3 million individuals about a data breach that occurred in March, compromising personal and protected health information. The breach involved unauthorized access to an unstructured data repository outside its core network, containing extensive customer information such as names, addresses, phone numbers, Social Security numbers, employer details, dependent information, and some payment card data. Additional sensitive data included diagnoses and prescription information.

A compromised vendor account's stolen password allowed unauthorized access to the repository, leading to a significant exposure of personal information.

These incidents highlight the importance of continuous improvement in security measures, including implementing multi-factor authentication, regular security audits, and fortifying internal and third-party defenses. These strategies are essential in protecting against the sophisticated techniques employed by attackers targeting sensitive data.

Key Lessons Learned

Each data breach provides critical insights that shape our understanding of effective SaaS ecosystem security. The key lessons learned from the breaches in 2024 highlight the importance of proactive security for SaaS, just like endpoints and cloud. This section offers lessons learned from the breaches of 2024 and highlights key capabilities of a SaaS ecosystem security platform.

Visibility

Establish comprehensive mapping of SaaS apps, APIs, and downstream services. This foundational step is crucial for monitoring the flow of sensitive data and the connections between applications, ensuring that all potential threat vectors are visible and under surveillance.

Threat Detection

It's essential to develop capabilities to identify and assess risks such as unauthorized API activity, inactive or dormant secrets, and anomalous data-sharing behaviors. Early detection of these anomalies plays a pivotal role in preventing breaches.

Automated Response

Implement automated workflows that integrate seamlessly with existing security tools like SIEM, SOAR, and IAM systems. This automation helps in quickly revoking risky access and remediating incidents, minimizing potential damage.

Continuous Monitoring

Constant surveillance to detect policy deviations, misconfigurations, and unauthorized changes is vital. This near real-time monitoring ensures that security postures are consistently enforced and that any deviations are promptly addressed.

Actionable Alerts

Enhance alert mechanisms to deliver prioritized and contextual notifications about anomalies affecting SaaS applications, data flows, and services. These alerts should provide clear, actionable insights, enabling swift response to potential threats.

Compliance-ready Reports

Generate reports that not only support compliance with privacy and security regulations but also provide actionable intelligence for security teams and application owners. These reports should facilitate informed decision-making and continuous improvement of security practices.

By learning from these breaches and enhancing their cybersecurity strategies, organizations can better protect themselves against future threats and minimize the risk of significant financial and reputational damage.

Recommendations and Best Practices

Drawing from the lessons learned in 2024, organizations can enhance their cybersecurity posture through several key practices.

1. **Understanding API Endpoints and Permissions:**
    - Regularly audit and document all API endpoints and the permissions granted to third-party vendors. This helps ensure that only necessary access is granted and that any changes or abnormal activities can be quickly identified.
    - Implement strict governance protocols to manage API access, ensuring that any access given is necessary for the vendor's role and complies with data protection policies.
2. **Reviewing Unused Accounts and Over-Permissive Access:**
    - Conduct periodic reviews of all accounts and secrets, especially those not actively in use, to identify and revoke over-permissive access. This reduces the attack surface by limiting the potential damage from compromised credentials.
    - Implement least privilege access principles across the organization, ensuring that users and systems have only the minimum level of access required to perform their functions.
3. **Monitoring Accounts with Access to Sensitive Data:**
    - Deploy advanced monitoring tools to track and analyze accounts that have access to sensitive data. Use behavioral analytics to detect anomalous access patterns or unauthorized data movements that could indicate a breach.
    - Establish alert systems for unusual activities, such as access requests during odd hours or excessive data downloads, which could signify a security incident.
4. **Regular Security Training and Awareness:**
    - Educate employees about the latest cybersecurity threats and safe practices. Regular training sessions can significantly reduce the risk of breaches initiated through social engineering or human error.
    - Encourage a culture of security within the organization where employees understand their role in protecting sensitive information and are vigilant against potential threats.
5. **Implementing Robust Incident Response Plans:**
    - Develop and regularly update an incident response plan that includes procedures for addressing various types of security breaches, including data leaks through third parties.
    - Conduct simulated breach exercises to test the effectiveness of response plans and make necessary adjustments based on performance during these simulations.

By integrating these practices into their cybersecurity strategy, organizations can better defend against the sophisticated and evolving threats seen in 2024, while maintaining compliance with regulatory requirements and protecting customer trust.

Conclusion

The cybersecurity landscape of 2024 has taught us invaluable lessons about the evolving nature of threats and the critical need for proactive security for SaaS ecosystems. As we have seen, breaches are not confined to direct attacks on an organization's own systems but often involve complex interactions with vendors and overlooked access points such as API endpoints and outdated credentials.

A proactive security program should include a thorough detection and response program. Organizations should understand and monitor API interactions, regularly review permissions and access controls, and enhance their ability to detect and respond to incidents swiftly. By doing so, organizations can not only protect their own assets but also fortify the broader ecosystem against the threats of tomorrow. Our shared goal should be to transform these lessons into actionable strategies that preempt breaches before they occur, ensuring everyone's data is safe and secure.

About Vorlon

Vorlon is the first easy way to secure complex SaaS ecosystems. With Vorlon, your SaaS finally gets proactive security coverage like you have for your endpoints and cloud. After an agentless, proxy-free setup, you can monitor sensitive data flows, manage secrets, detect anomalies, and revoke access. Powered by patent-pending DataMatrix® technology, Vorlon creates an algorithmic model of your applications and connected services for faster, AI-driven remediation. Backed by Accel and SOC 2 Type 2 Certified, Vorlon is trusted by Fortune 500 companies and startups.

Learn more at vorlonsecurity.com.