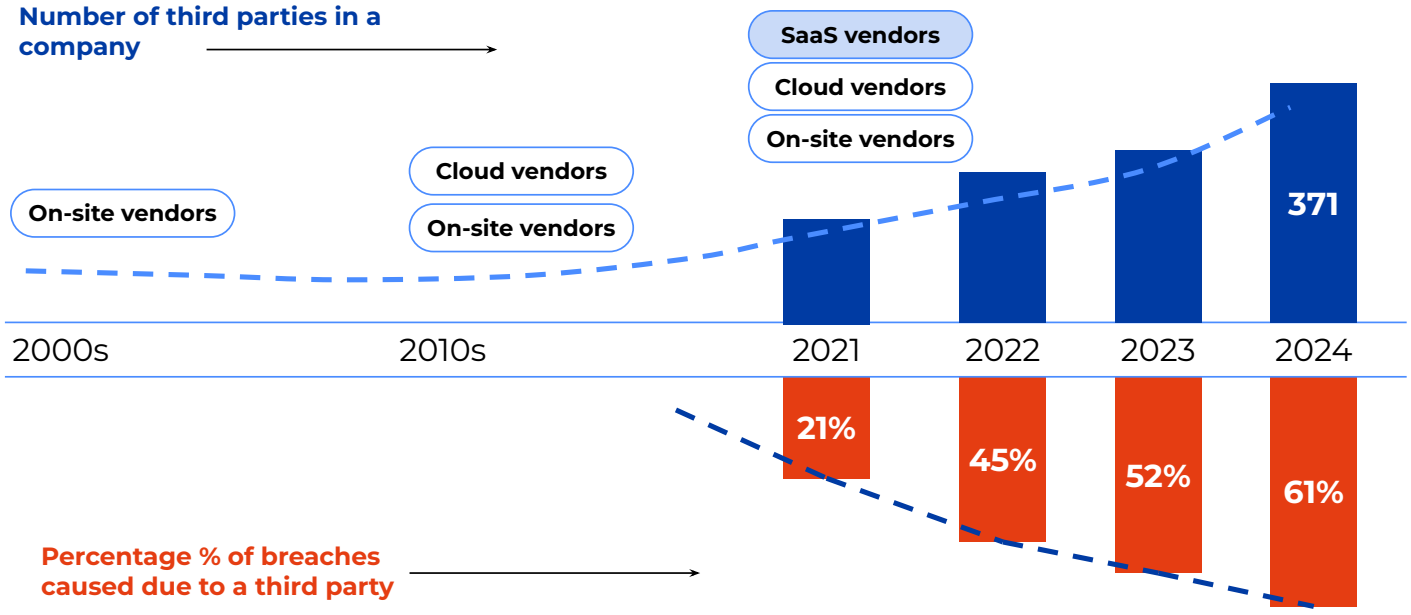
SaaS Sprawl:
Control It Before It Controls You

A strategic approach to secure SaaS applications, cut costs, and stay ahead of breaches

BLUOCEAN

SaaS complexity is increasing threat surface



BLUOCEAN

2019: Salesforce

Hackers gained access to customer data from one of its clients, through malware infiltration on their Salesforce platform, exposing sensitive customer information like credit card numbers and addresses

2021: Microsoft Exchange

Multiple zero-day vulnerabilities in Microsoft Exchange Server were exploited, allowing attackers to access emails, passwords, and administrator privileges.

2023: Okta

Stolen credentials used to access support systems

2023: MOVEit File Transfer Software

A vulnerability in the MOVEit managed file transfer software was exploited, impacting thousands of organizations and nearly 100 million individuals.

2024: Snowflake

Data breach impacting 164+ customers; login credentials exploited to access sensitive data without MFA. Following the public disclosure of breach, Snowflake's stock price declined by 20%

2025: Microsoft Teams

In a series of attacks, Russian cyber criminals sent 3000 spam messages within an hour and then posed as IT support on Teams to get remote system access for **data exfiltration.**

BLUOCEAN

Let's Analyze a Few Third Party SaaS Breaches

Over 1TB of Data Stolen from Disney's Slack Instance

Massive Data Trove (1.1 TB data) - More than 44 million messages, upward of 18,800 spreadsheets and 13,000+ PDFs.

Competitive Advantage - Unreleased Content and Intellectual Property (IP) for media franchises like Fortnite and Aliens: Fireteam Elite

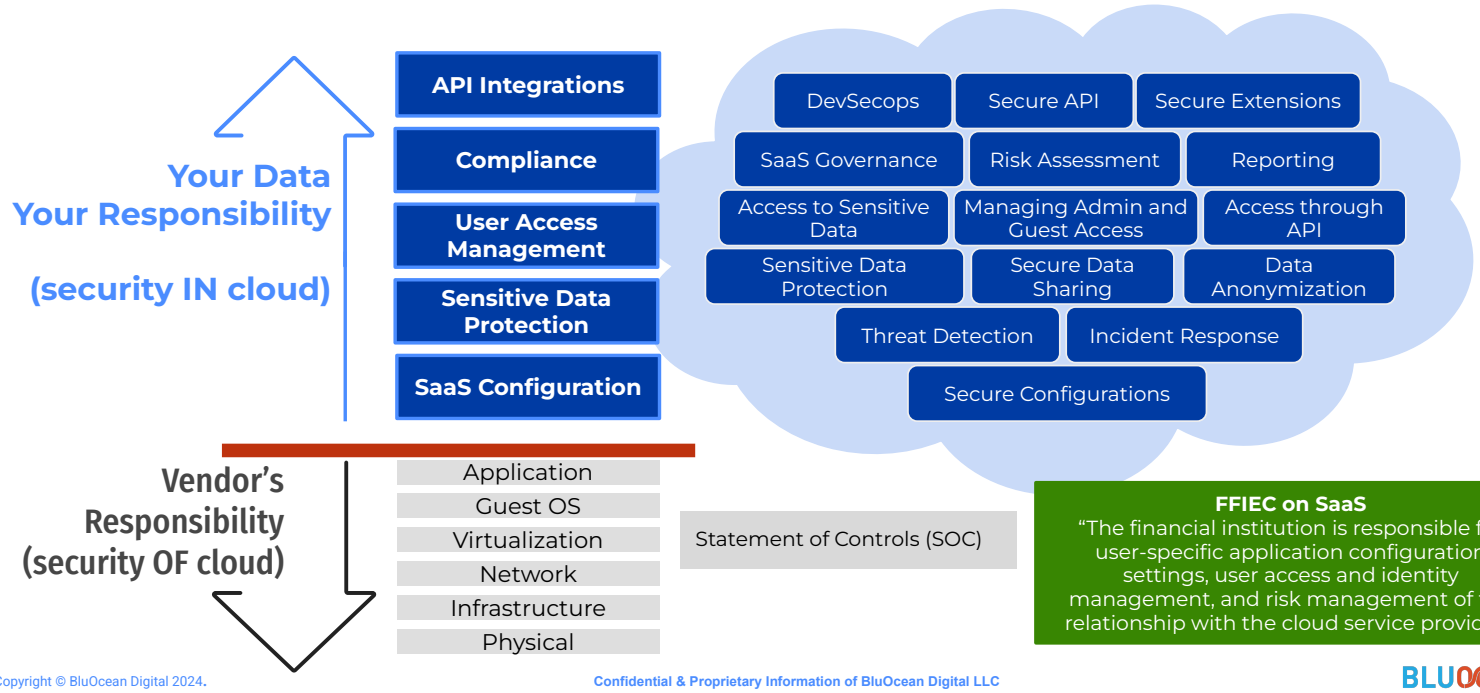
Customer's Trust - Sensitive Credentials

How Did This Happen After Third Party Reviews?

Disney failed to implement critical controls in alignment with the shared accountability model.

- No MFA
- No least privilege
- No threat detection
- No threat monitoring
- No access monitoring
- No data exfiltration monitoring
- No DLP
- No device management

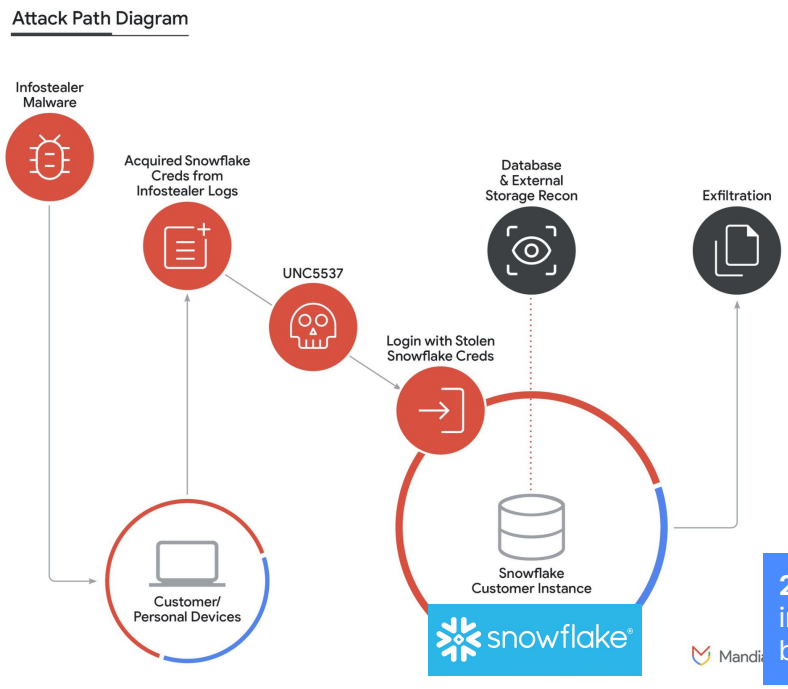
The root cause - Transparency and Clarity on SaaS Security Accountability (SaaS Shared Responsibility Model)



FFIEC on SaaS
"The financial institution is responsible for user-specific application configuration settings, user access and identity management, and risk management of the relationship with the cloud service provider."

BLUOCEAN

Snowflake Cyber Attacks



What happened in the Snowflake breaches?

- Hacker uses infostealer malware to steal credentials
- Scan systems without MFA enabled and finds a Demo Account
- Use stolen credentials to bypass MFA and get access to system
- **Exfiltrated sensitive data in bulk**

243-day detection window for SaaS breaches vs. industry benchmarks (e.g., "Top CISOs detect breaches in <30 days").

BLUOCEAN

Rinse and Repeat 165 Times

So far **165 organizations** have been identified who lost their data (**And Yes most of them weren't aware of it!!**)

And the world is still counting…

https://www.cnbc.com/2024/07/12/snowflake-shares-slip-after-att-says-hackers-accessed-data.html

SaaS Applications: Your New Crown Jewels Under Attack

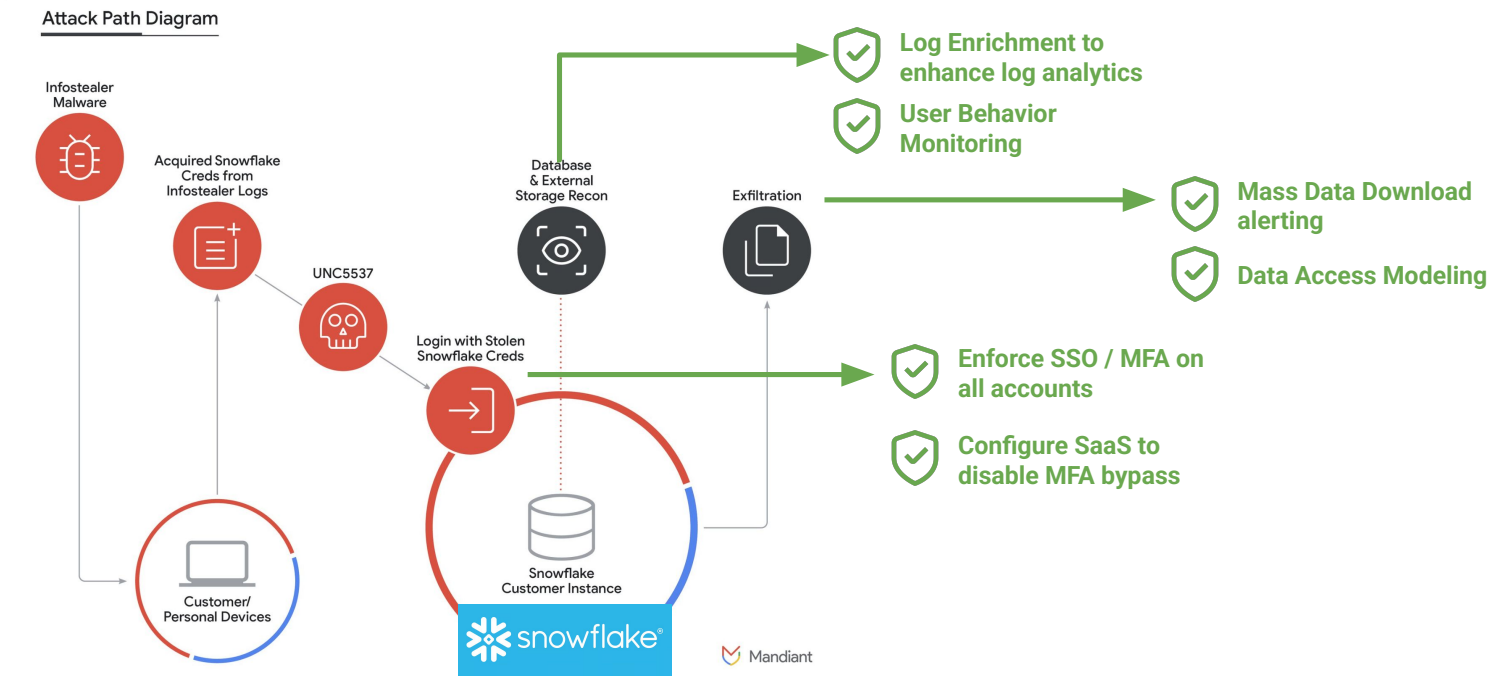
Customer data, financials, and IP in SaaS apps are now hackers' most lucrative targets

Data Stored in SaaS Applications
Customer PII
Customer Financial Data
PCI
MNPI
Intellectual Property
Proprietary Information
Employee Data
Financial Data

Business Functions Performed in SaaS Applications
Sales
Customer Payments
Billing & Invoicing
Telecommunications
Accounting & Finance
IT Operations
Human Resources

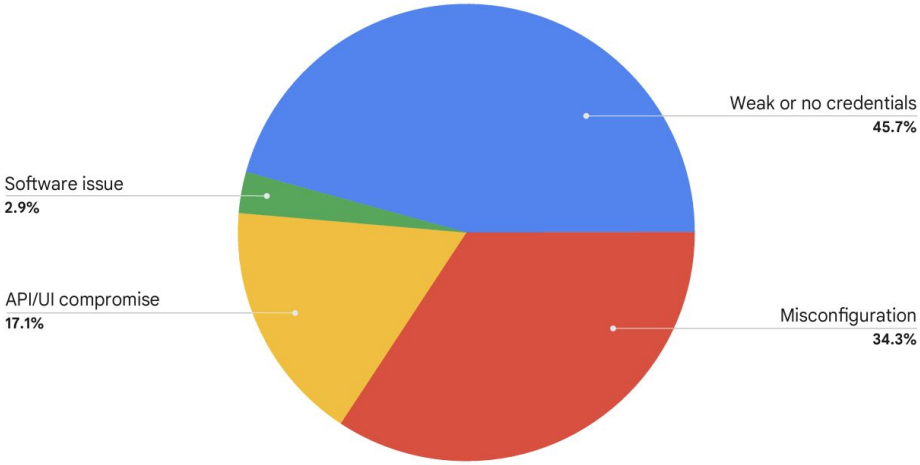
SaaS Applications Supporting Insurance Business Processes
Salesforce
Snowflake
Slack
Atlassian Suite
Box
Microsoft 365
Workday

This Breach Could Have Been Prevented!



Third-Party Reviews Cover Vendors (2.9% of Breaches), Not How Companies Secure SaaS (97.1% of Breaches)

Initial access vectors of concern H2 2024*



The myth of 'vendor-secured' SaaS leaves YOUR configurations, access rules, and data sharing as the real attack surface

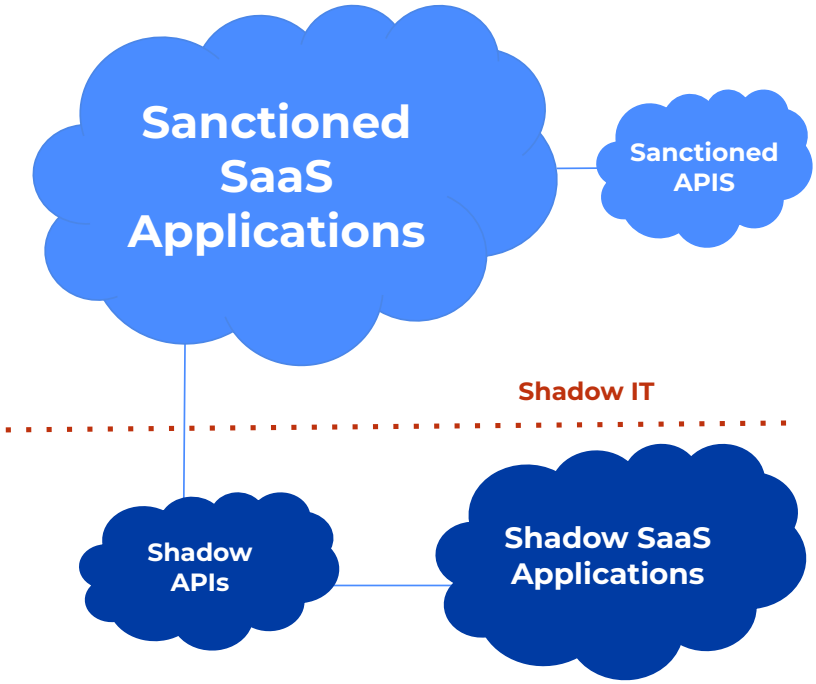
*Google Threat Horizons Report

What's the Solution?

Implement proactive security to continuously monitor, detect and remediate SaaS security issues

BLUOCEAN

1. Conduct SaaS Discovery Within Your Organization



Organizations use an average of 371 SaaS applications.[1]

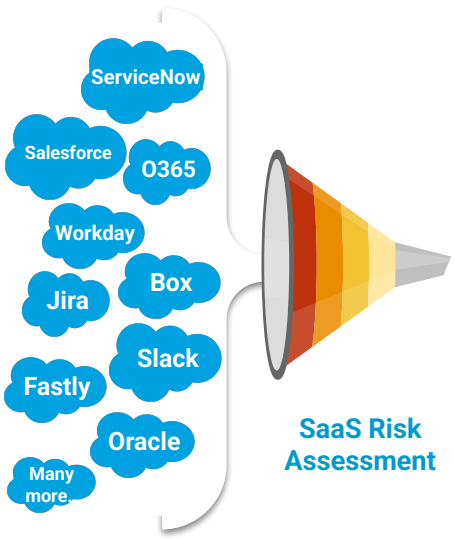
Identify how many SaaS apps are being used. This includes :

- Shadow IT SaaS
- SaaS-to-SaaS connections

Understand risk to business by SaaS applications

1. https://productiv.com/state-of-saas

2. Conduct SaaS Security Risk Assessment



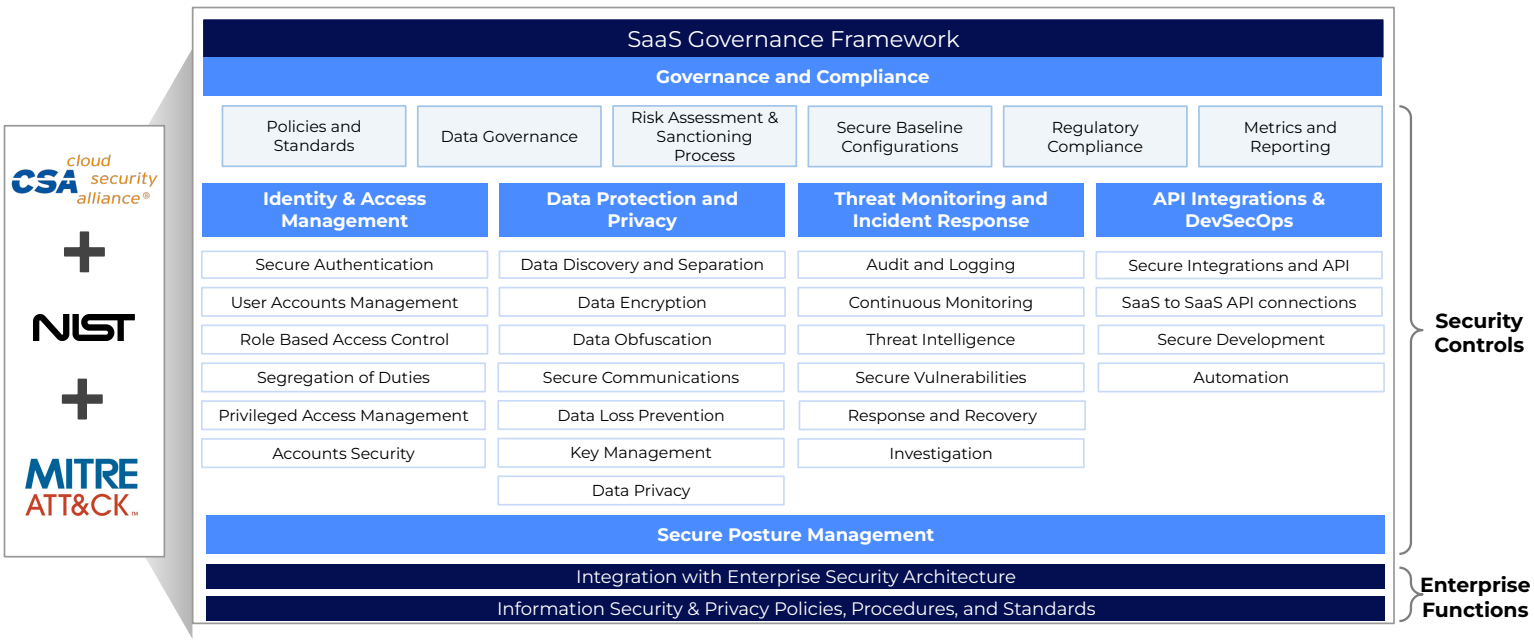
High Risk SaaS applications
Continuous Monitoring with SaaS security products

Medium Risk SaaS applications
Third Party Reviews + SOC2 Reports + Pentesting Reports

Low Risk SaaS applications
SOC2 Reports

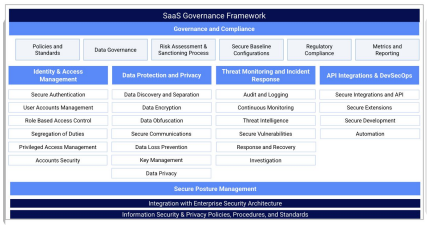
- **Identify SaaS apps supporting critical business functions**
- **Get buy-in from business on risk to business**

3. Define a standards based SaaS governance framework as a foundation to design your SaaS security controls



4. SaaS Security Control Design

Define SaaS security controls for each risk tier post SaaS Risk assessment



High Risk SaaS applications

Medium Risk SaaS applications

Low Risk SaaS applications

- SaaS Governance and Regulatory Compliance
- SaaS Identities and Access Management
- SaaS Data Protection and Privacy
- SaaS Threat Detection and Incident Response
- Secure Integrations
- Secure SaaS API extensions

Design control plan on how to implement security controls for each risk tier

Continuous Monitoring with SaaS security products

High Risk SaaS applications

Robust Third Party Reviews

Medium Risk SaaS applications

Low Risk SaaS applications

BLUOCEAN

5. Implement Continuous Monitoring for SaaS apps

SaaS Security Controls Plan

High Risk SaaS applications

- SaaS Governance and Compliance
- SaaS Identities and Access Management
- SaaS Data Protection and Privacy
- SaaS Threat Detection and Incident Response
- Secure Integrations
- Secure SaaS API extensions

Identify Tools and Setup Architecture

SaaS Security Posture Management (SSPM)

SIEM

CASB

DLP for SaaS apps

Data Privacy tools

IGA tools

GRC tools

ITSM (ServiceNow, JIRA, etc)

Native SaaS Security Features

SaaS Security Controls Implementation

Integrate each SaaS app for continuous monitoring

↓

Implement, fine-tune configuration rules

↓

Implement, fine-tune access and data exposure rules

↓

Implement, fine-tune threat detection rules

↓

Monitor and audit integrations

↓

Implement integrations with SIEM, GRC, JIRA etc. and automated security SOP

BLUOCEAN

Configure six (6) critical use cases to reduce SaaS attack surface

Configuration, Identity & Drift Management

Are my configurations hardened?

Who has access to what? Where are unauthorized accesses?

Are all of my users authenticating with SSO or do I still have local accounts?

What has changed in configuration (drift)?

Threat & Anomaly Detection

Are there anomalous activities by any users?

Am I forwarding critical audit logs and creating high fidelity alerts within my SIEM/SOAR?

How do I respond to potential SaaS incidents?

Security of Connected Apps

What is my attack surface due to SaaS-to-SaaS connections?

How do I control unauthorized connections to other third party apps?

How do I make sure our developers are building secure extensions?

Data Exposure & Access Modeling

Is data exposed to the public internet?

How do I manage data exposure & remediate issues?

How can I monitor for data exfiltration and insider threats?

Governance & Risk Management

What SaaS applications are most critical to my business and are they in alignment with our enterprise risk profile?

Which controls should I prioritize first to reduce risk exposure?

Do I have policies that cover SaaS sanctioning and SaaS-to-SaaS API connections?

Compliance with Regulatory Requirements

How do I identify non-compliant controls?

What SaaS configurations need to be in place to meet compliance standards? (CCPA, GDPR, NIST, SOX, etc.)

How can I ensure my SaaS applications stay in compliance?

BLUOCEAN

A. SaaS Configuration and Compliance

Set & Configure Secure Baseline

Implement SSO, MFA, password policies, session policies, etc.

Detect Configuration Drift

Continuously monitor for drifts and alert accordingly

Monitor Compliance

Monitor and report on compliance with real-time dashboards

Enforce SSO and eliminate local accounts

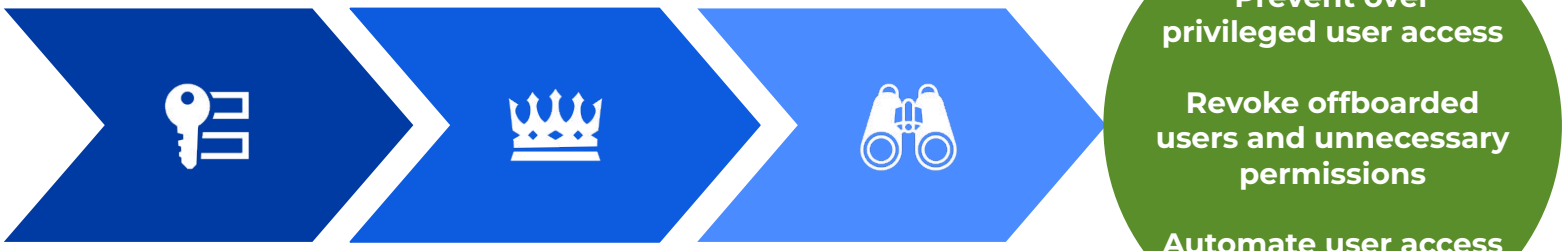
Enforce MFA for all users and prevent MFA bypass

Prevent future audit issues

Nearly 35% of SaaS breaches start with misconfigurations

BLUOCEAN

B. SaaS Identities and Access Management



Set Role, Tenant, & Object Level Access Controls

Restrictive access at application level, granular permissions at object level

Manage Privileged Access

Governance and approval workflow for privileged access

Continuously Monitor Access

Monitor data access and integrate with identity tools for automated access review

Prevent over privileged user access

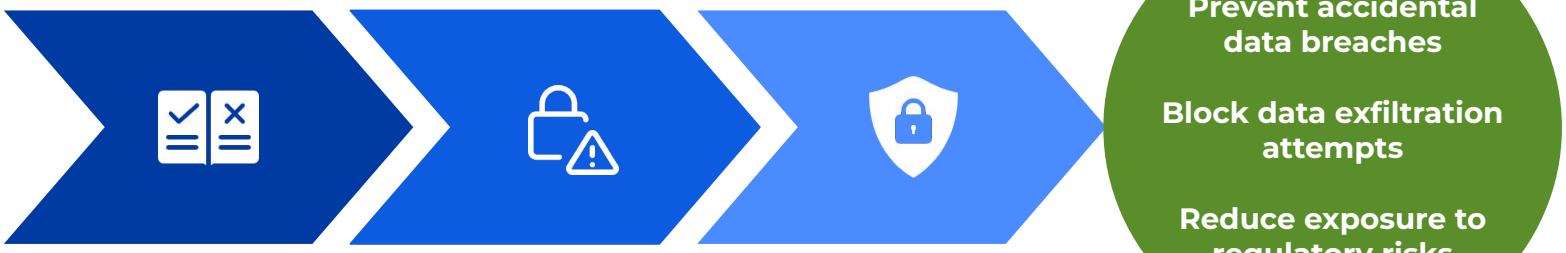
Revoke offboarded users and unnecessary permissions

Automate user access reviews

165+ companies Snowflake instances were hacked through misconfigured demo user accounts

BLUOCEAN

C. SaaS Data Protection and Privacy



Configure Data Sharing Rules

Control and monitor how data is shared with internal vs external users

Prevent Data Leaks & Exposure

Classify sensitive data and configure data leakage policies

Align with Privacy Regulations

Alert on data privacy and compliance violations

Prevent accidental data breaches

Block data exfiltration attempts

Reduce exposure to regulatory risks

31% of organizations suffered a SaaS data breach in 2023[1]

1. AppOmni, State of SaaS Security 2024 Report

BLUOCEAN

D. SaaS Threat Detection & Incident Response

Detect & Respond to Threats

Define incident response workflows and accountability matrix

Centralize and Store Logs

Implement centralized log storage for ingestion by monitoring tools

Baseline User Behavior

Determine anomalies, finetune alerts, and reduce false positives

Detect malicious activity in minutes not days

Alert on compromised user accounts performing anomalous actions

On average SaaS incidents go undetected for up to 243 days

BLUOCEAN

E. Secure SaaS Integrations

Discover & Govern Shadow Integrations

Establish a governance process & implement access control for data sharing

Profile and Prioritize Risks

Risk based tiering of SaaS connections by permissions and vendor

Monitor for Unsanctioned Connections

Alert on integrations that did not go through an approval process

Stop sensitive data from being shared with third parties

Prevent vulnerability exploitation and compromise due to shadow IT

33% of third-party SaaS integrations are granted access to sensitive data[1]

1. Valence, 2024 State of SaaS Security Report

BLUOCEAN

F. Secure SaaS API Extensions

Implement Security Guardrails

Establish guidelines for secure custom SaaS code extensions

Detect Code Vulnerabilities

Leverage SAST / DAST tools to test SaaS custom code

Evaluate SaaS Data Exposure

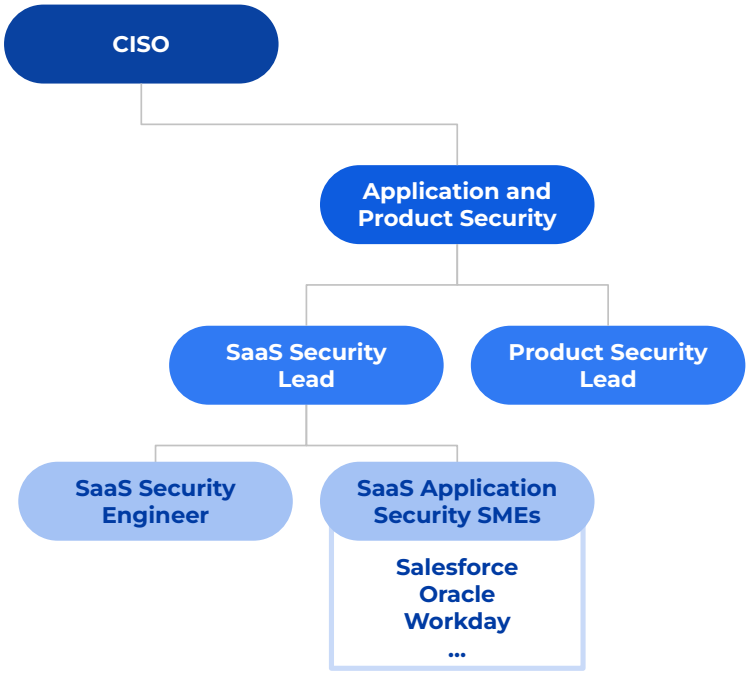
Continuously monitor for unauthorized data sharing via code extensions

Stop code injection and other web application exploits

Stop insecure code from being deployed in your SaaS environment

Critical and high Apex code vulnerabilities can lead to data exposure and corruption in Salesforce

6. Integrate SaaS Security into the CISO Pillar That Fits Your Culture



Preferred Alignment (by priority):

1. Application & Product Security
   (Ideal for organizations prioritizing SaaS as a product/application layer)
2. Cloud Security
   (Suits cloud-centric environments where SaaS is part of broader cloud strategy)
3. Third-Party Risk Management (TPRM)
   (For orgs viewing SaaS vendors as critical third-party risks)

Key Skills for the SaaS Security Team

- Technical Expertise:
  - SaaS application architecture design & hardening
  - DevSecOps for secure SaaS integrations and API extensions
  - Native security controls of top SaaS apps (e.g., Salesforce, Workday, ServiceNow, O365, Snowflake, Zoom etc.)
- Collaboration:
  - Partner with app teams to embed security in SaaS workflows
  - Coordinate with threat/IR teams for anomaly detection and incident response
  - Align with identity/compliance teams for RBAC, MFA, and audit readiness
  - Advise privacy teams on data classification and exposure monitoring

Establish a collaborative operating model between business and security to reduce threat exposure and get results!

Partner with Your security team

Governance	Define SaaS Security policies and standard, application sanctioning and governance process, risk profiling guidelines, and risk metrics
Logging and monitoring configuration	Configure logging integrations and monitoring rules for high risk events
Alerts analysis	Analyze and risk prioritize alerts, continuously enhance exceptions and alert evaluation criteria to reduce false positives
Exception management	Define and implement exceptions management process, documenting accepted risks in the enterprise risk register
Incident response	Equip Security Teams with context and guidance to investigate and remediate application threats

Execution partnership

Combined ownership

Guide application admin teams

SSO, Multi Factor Authentication	Enable Single Sign-On (SSO), enforce MFA and strong password policies for all users
User roles and permissions	Implement Role Based Access Control (RBAC) and restrict API access as per security best practices
Hardened app configuration	Enforce baseline configurations native to each SaaS app as per defined SaaS Security policies
SaaS integrations	Follow defined sanctioning and governance process to approve new SaaS integrations
Remediation and change mgmt	Plan and execute against organisation change management process for remediation of security issues

Business outcomes	Secured high risk SaaS applications	Increased visibility into application deployments	Collaboration between security and application teams	Reduced financial, regulatory and reputational risk	Increased trust from customers

BLUOCEAN

No Overhauls Needed: Start Small, Win Fast

Your 90-Day Roadmap

01

Assess

Identify your 5 most critical SaaS applications and create a list of security risks through a comprehensive assessment.

02

Secure

Quickly implement critical controls aligned by risks like MFA and least-privilege access etc. on your 5 critical SaaS apps using SSPM tools

03

Monitor

Automate continuous monitoring for misconfigurations, overprivileged access, and API risks across your 5 SaaS applications. **Get alerted on issues before they become incidents**

04

Optimize

Integrate your SaaS security into your existing SIEM and SOC workflows. **Scale your program to cover next 5 apps.**

BLUOCEAN

Proactive SaaS Security Automation Slashes Risk

From Months to Minutes

Without Automation

🕒 243 Days Detect time

💾 1TB Data Stolen

💸 Ransom Paid

Automation reduces breach detection time by 90% and data loss by 95%

Unauthorized user logs into Snowflake and begins to download sensitive records

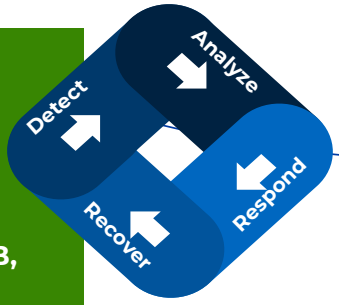
Automated Solution

🔍 Anomaly Detected

⚡ Automated Lockout

✅ Minimal Loss

Tools Used - SaaS App, SSPM, CASB, IDP, SIEM, SOAR



BLUOCEAN

I think I am doing something to secure my SaaS applications?

BLUOCEAN

Myth vs. Reality of SaaS Security

Why your current SaaS security isn't enough?

My SIEM logs cover all my SaaS risks	**Logging Costs**	• SSPM **cuts SIEM costs by 90%**—logs alone miss critical APIs & metadata
SSO protects all SaaS access	**Shadow SaaS**	• **65%** of SaaS apps are shadow IT—IDPs don't secure local accounts
Zero trust = SaaS data is safe.	**API Data Sprawl**	• **17.1%** of incidents involve compromised APIs—data sprawl breaks visibility

The gap between perception and reality is where breaches happen

1. https://www.bettercloud.com/resources/state-of-saasops/
2. https://www.varonis.com/blog/saas-data-risk-report

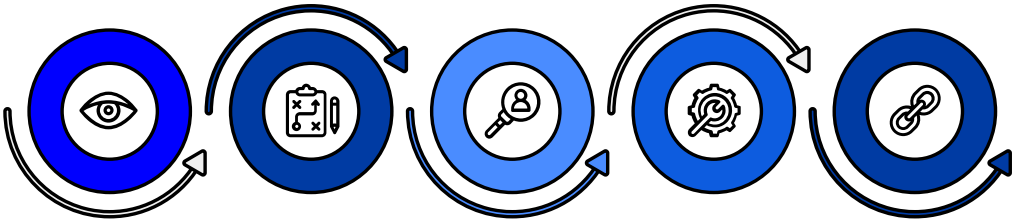
BLUOCEAN

BluOcean Cyber

Our Mission:

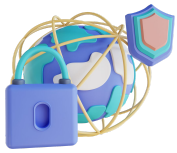
BluOcean's mission is to redefine cybersecurity as a critical strategic business asset. We connect threats to business processes to protect, sustain, and amplify critical business outcomes with verifiable ROI.

BLUOCEAN



Strategy | Governance | Implement | SaaS MDR | Auto Remediate

Secure your SaaS ecosystem: Expert-Led solutions that transform risk into automated remediation



Continuous Monitoring: Real-time visibility into SaaS misconfigurations, identity risks, and data exposure.

Expert-Led Remediation: Certified SaaS engineers fix issues

Compliance Automation: Pre-built policies for GDPR,NIST —no manual audits.

Your zero-trust, IAM, and cloud policies are strong. We'll extend them to SaaS

Our Features

SaaS Security Solution

We focus on risk-to-business impact *to* ***operationalize SaaS Security*** *through* ***Strategy, Implementation, Integration and Monitoring (MDR)***

Expert Support

We bring **SaaS application experts (Salesforce, workday, etc.)** to handle SaaS nuances; you own the roadmap

Pre-built App Security Templates and Shadow SaaS Discovery tool

50+ SaaS Applications Secure-by-design templates. Reduce threats by detecting shadow SaaS

Agile Automation

Continuous monitoring and remediation by SSPM integration with JIRA, SOAR, SIEM, etc. replaces manual audits

Compliance Ready

We bring **templates** to help you with SOX, GDPR, NIST , FFIEC compliance - **No Manual audits**!

Standards based SaaS Framework

Our **NIST, CSA and MITRE based SaaS framework** builds the control foundation

***Vendors sell tools; BluOcean delivers a* business-aligned operating model!**

BLUOCEAN

BluOcean RiskGPS™ Platform

Prioritized, business-driven cybersecurity for optimized cyber budgets and secure growth with verifiable ROI

Cyber Program Defense Planning

Secure stronger investment support with data-driven, high-impact business risk driven resource allocation decisions.

Cyber Budget Aligned with Business Risk

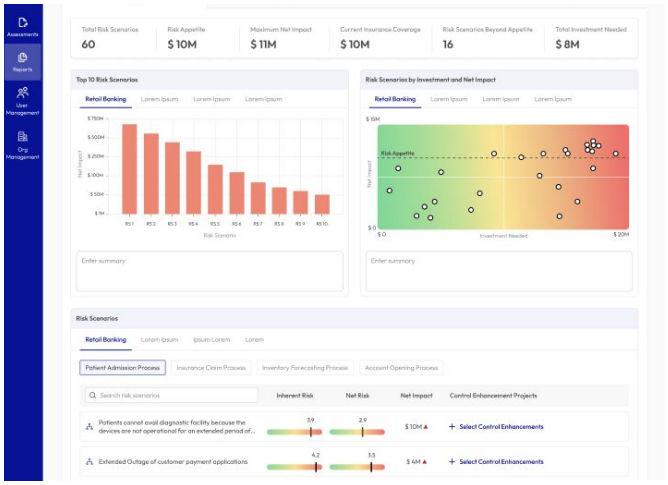
Prioritized security investments using business impact quantification for maximum risk reduction with verifiable ROI.

Crown Jewels Proactive Protection

Focus budget and resources on safeguarding high-value assets that support key operations.

Defense in Depth Security

Align cyber defense spending with business priorities for stronger protection of key assets.



Thank You for Attending Our Presentation!

As a token of our appreciation we are extending an offer. Choose one at no cost for one SaaS instance in the next 30 days:

1. **SaaS Security Gap Analysis**
   Get actionable recommendations to achieve defense in depth SaaS Security
2. **Automated Risk Assessment**
   Get your organization's SaaS security posture evaluated with a leading SSPM tool in real time.
3. **Shadow SaaS Discovery Exercise** (SentinelOne customers only)
   Get an inventory of SaaS applications used by your organization.

Contact us Katie.reilly@bluoceancyber.com, Vishal@bluoceancyber.com

Thank You!

Vishal Chawla
vishal@bluoceancyber.com

Katie Reilly
katie.reilly@bluoceancyber.com

Contact Me

Sign Up for Our Newsletter

Sign Up for Our Newsletter at bluoceancyber.com

BLUOCEAN