InsiderSecurity

Simplify Your Cloud Security

Cloud Security.
Cloud Asset Visibility.
Misconfiguration Monitoring.
In a single solution.

STAR LEVEL TWO

ISO 27001 Certified

How can CSX help you?

As businesses move to the cloud, attackers increasingly target cloud data and assets. Cloud service providers are responsible for parts of cloud security under the shared responsibility model, but there are significant security gaps which are the user's responsibility.

Keeping your cloud data safe is complex and bewildering, especially if you use multiple clouds and various SaaS. How can you ensure that your cloud data and infrastructure are secure and uncompromised?

CSX is designed to make cloud security simple. Leveraging cybersecurity analytics and machine learning, CSX offers security coverage across the entire cloud stack, whether it is Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS).

CSX is built for multi-cloud from the start. For businesses, CSX reduces operational complexities and minimizes the demands on scarce manpower.

CSX secures your entire cloud stack and helps you avoid potentially devastating security breaches.

What is CSX?

CSX uses cybersecurity analytics and artificial intelligence to uncover cyber risks early, especially threats that would otherwise go undetected.

- Detect malicious activity and compromised accounts in the cloud
- Remediate threats and fixes misconfigurations
- Improve cloud asset visibility
- Detect misconfigurations and exposed data

CSX Overview

Secure your entire cloud stack
A single solution that covers various IaaS, PaaS and SaaS, including Microsoft 365 and Google Workspace.

Use one solution for multiple clouds
An easier solution for orgainzations that have multi-cloud environments e.g., AWS, Azure, OCI, or GCP.

Cover the gaps in the shared responsibility model
With cloud services, service providers are only responsible for parts of the cloud security, under the shared responsibility model. CSX helps you cover the security gaps that are not covered by the service providers.

Detect malicious activity
Monitors and detects malicious user activity and data activity, especially in SaaS services.

Know what cloud assets you have
Provides asset visibility by automatically discovering your cloud assets and inventory. Get a comprehensive overview of your cloud resources, across all clouds.

Avoid misconfigurations
Misconfiguration is one of the top causes of cloud data breaches. Maintain secure configurations with notifications and recommendations, ensuring your cloud environment adheres to security standards and best practices.

Remediate quickly
Immediately fix any issues and close the loop in your investigation with remediation and response in the dashboard.

Save time
Cybersecurity AI makes sense of your cloud activities and helps you to save effort and time.

Simplify cloud security with CSX

Some use cases

Data Theft

Detecting unusual account and data access activity early is crucial to preventing significant data loss. Early detection and remediation can stop a breach before it escalates.

Compromised Accounts

CSX analyzes login and account behavior to identify suspicious activities indicative of compromised cloud accounts. For example, an attacker using a stolen account might try to gain additional privileges or access restricted cloud assets.

Suspicious VM Activity

Attackers often create new Virtual Machines (VMs) within compromised cloud accounts to bypass existing restrictions. This tactic allows attackers to evade firewall rules and permissions on current VMs and maintain a foothold in the cloud environment.

Suspicious Privileged Activities

Attackers compromise privileged cloud accounts to gain more access to the victim's data and infrastructure. Monitoring for suspicious privileged activity helps to prevent a serious data loss.

Suspicious Application or Plugin Access

In today's SaaS and cloud environment, numerous third-party applications and plugins enhance productivity. However, some applications may request excessive permissions or be outright malicious. Bad actors might install such apps to maintain access to a victim’s cloud environment.

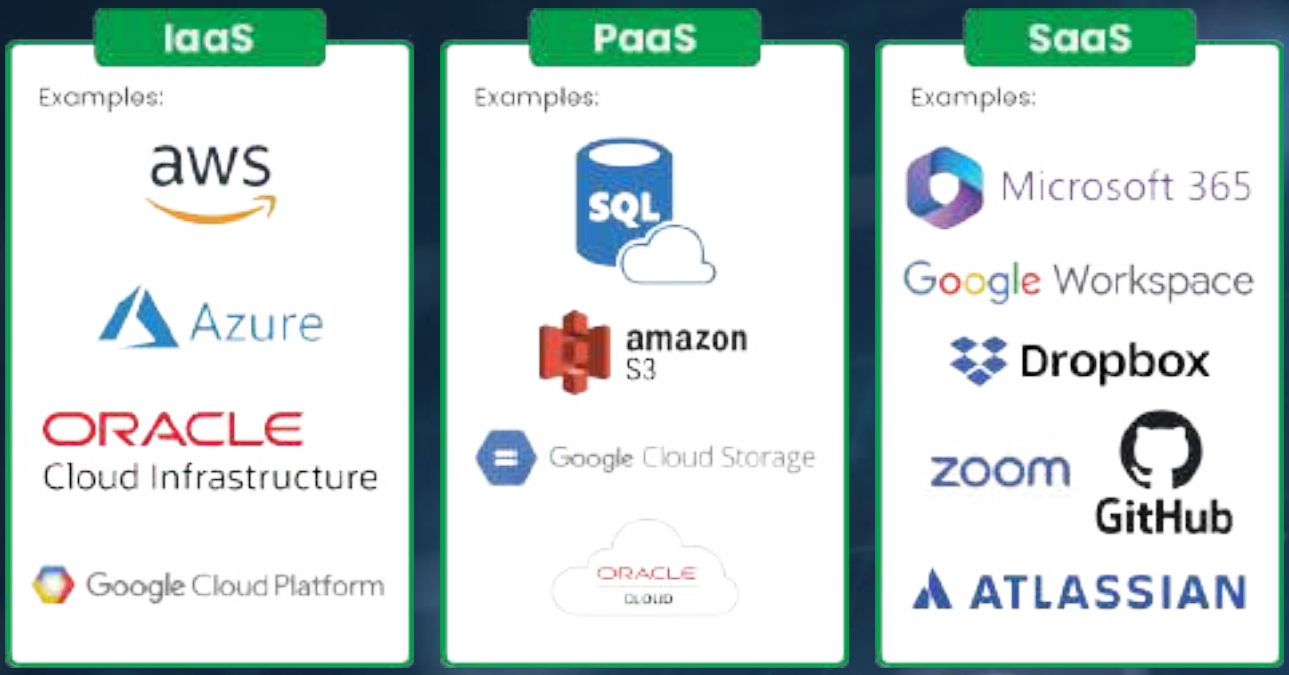
Misconfiguration of Data Assets or Folders

Organizations frequently share data both internally and externally, making it challenging to track all shared files, especially those inadvertently made public. Malicious actors scan for publicly accessible and unprotected cloud storage to steal data.

Misconfiguration of Audit Settings

Activity audit logs in cloud systems are vital for tracking account activities, such as management and data operations. Malicious actors might disable these audit logs to conceal their actions.

Securing all cloud layers against threats



Spotlight on M365 security monitoring

Are you concerned if your company's accounts are compromised, and a hacker may be accessing your company data and emails?	CSX detects if your online accounts have been hijacked by hackers.
How can you discover if there is a disgruntled employee or insider threat stealing your valuable company data?	Our award-winning solution detects suspicious user activity due to insider threats and hackers automatically.
Can you identify if a user has accidentally exposd confidential documents on OneDrive to the public?	Smart behavior analytics discover if files are accidentally left exposed

M365 threat scenarios covered

1 Suspicious Login Activity

CSX detects suspicious login activity using indicators such as frequency, time and location.

2 Privilege Escalations

CSX keeps track of admin roles and access rights, and alerts when there is a risky privilege escalation.

3 Suspicious Data Access

CSX detects suspicious file downloads and analyses other data operations such as delete, edit, create, and restore.

4 File Permission Change

CSX detects suspicious changes to file sharing permission.

5 Unauthorized Sharing

Unauthorized shared links are constantly tracked by CSX to detect suspicious access to sensitive information.

6 Non-owner Mailbox Access

CSX detects non-owner mailbox permissions.

7 Unauthorized Policy Change

CSX keeps track of Microsoft's policies to detect suspicious changes

Contact us and schedule a meeting today.

sales@insidersecurity.co

+65 6270 4029

www.insidersecurity.co

2 International Business Park, #06-01, Singapore 609930