SKYFORMATION

Bringing new heights to your Security Operations/SIEM with robust cloud visibility and threat detection

Overview

As an increasing amount of corporate data is moving to business cloud applications (such as Office 365, Google Apps, ServiceNow, Salesforce and private applications), organizations face new security challenges and threats. Cloud applications are known for their data collaboration, accessibility from anywhere and mobile support, among others. But this makes the organization's valuable data that resides in cloud applications harder to govern and to protect from threatening and risky activities. For organizations with a Security Operation Center powered by a SIEM system the best strategy for fast, precise detection of business cloud application threats and compliance concerns is to leverage your existing SIEM, active directory, HR systems, and other security infrastructure like IAM, IDS/IPS, threat intelligence. The key is to extend this infrastructure with a purpose-built platform for cloud application security which delivers three unique capabilities:

Visibility of cloud application activities threats and risks

SkyFormation ensures that each of your cloud applications has a dedicated connector accessing the proprietary interfaces and methods necessary to give you maximum visibility of activities and potential threats/risks that is only possible when combined with the real-correlation and event context your SIEM system already provides. Get visibility of anomalous user access behavior such as sudden changes in location. Detect unauthorized changes in user and admin permissions and privileges, network configurations, security settings, file and resource management, and much more.

Improved security posture with out-of-the-box offering

Building effective cloud application threat detection rules for your SIEM often requires intensive on-going professional services work to ensure the full meaning, context, and real-time correlation can be applied to cloud events. SkyFormation offers out-of-the-box threat detection rules built into your SIEM and is easily customized to your SIEM and infrastructure thereby eliminating the need for expensive, time-consuming development and professional services.

Solution Highlights

SkyFormation Solution allows organizations to:

- Extend your existing Security Operations, SIEM, and infrastructure investments with visibility of granular activities and threat detection for your cloud applications
- Empower your existing Security Operations, SIEM, and infrastructure investments with Shadow-IT discovery, risk assessment and on-going governance
- Ensure single security and compliance solution for any business app whether local or in the cloud including shadow IT
- Save considerable time and expense by using SkyFormation's out-of-the-box and easy to customize detection rules built for your SIEM

Discover and govern cloud applications with zero burdens

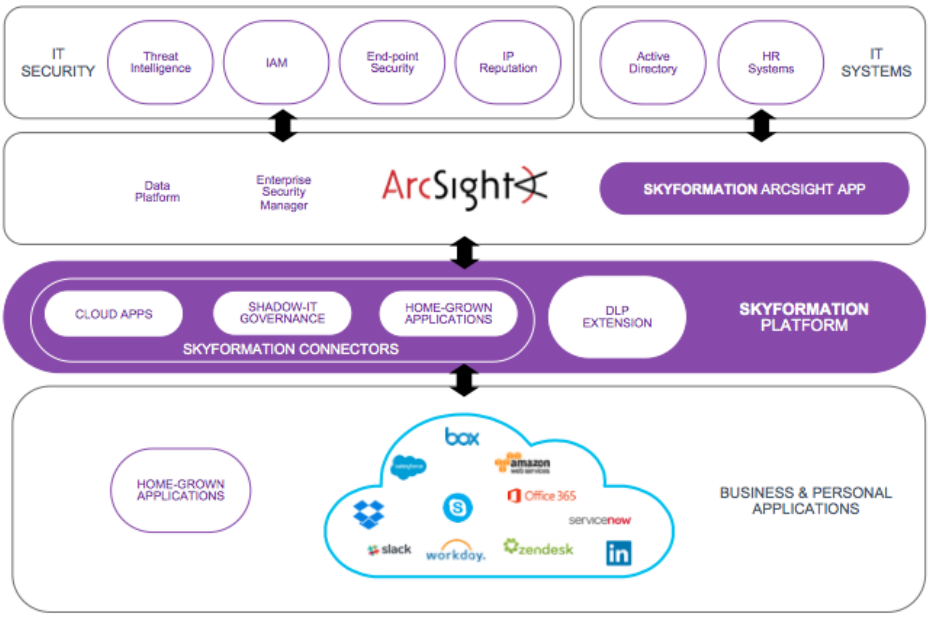
One of the unique challenge organizations face is to know what cloud applications are being used for business needs, and by whom, in order to detect of security and compliance risks. Doing this can require intrusive endpoint software and significant changes to your network and security configurations. With SkyFormation, there is zero impact to your user experience, no impact to network configurations, and no change to security implementations. There is no need to train your Security Operations staff or incur expensive, ongoing support and maintenance costs.

SkyFormation Solution Overview

SkyFormation brings new heights to your existing Security Operations Center and SIEM investments by adding robust cloud applications security and compliance.

SkyFormation extends your existing Security Operations and SIEM system with:

- Out-of-the-box business cloud application connectors
- Translation of all cloud apps security events into one, actionable ready for SIEM and incident response events
- Cloud applications discovery, risk assessment and governance (aka shadow IT)
- Security activities monitoring (users access, security changes and more)
- Data Leakage Prevention (DLP) for cloud applications
- Monitoring of risky security configuration changes
- Out-of-the-box and customized cloud apps threat and anomaly detection
- Remediation (reset password, disable user, remove file etc.)



SkyFormation Solution Functions

SkyFormation Function	Description
Cloud applications discovery risk assessment and governance	Discover the business cloud applications in use, perform risk assessment and keep on going governance.
Users and groups management governance	Monitor user's management changes and detect risky changes.
Secure configuration governance	Monitor security configuration changes as password policy changes, and identify risky changes.
High privileges accounts governance	Monitor activities performed by high privileged accounts in each cloud application, and identify anomalies and risky activities.
Coverage for internally developed applications	Monitor similar security and compliance activities and threats across internally developed applications using SkyFormation developer kit.
Data Leakage Detection and Prevention (Data protection)	SkyFormation provides data protection across business cloud applications by identifying and exposing data leakage events in file sharing solutions; remediate risks using auto-response actions.
Full central audit trail	SkyFormation cloud apps connectors retrieve the available activities from each app and send them to the organization central log and event system.
Threat detection and prevention	SkyFormation SIEM app include out-of-the-box cloud applications threat detection and remediation plugins.

About Skyformation

Founded in 2014, SkyFormation is a cloud application security company that provides visibility and mitigation of the risks associated with cloud services usage in the organization. Building on the strengths of your existing Security Operations, SIEM and other security investments, SkyFormation uniquely detect threats by delivering granular security information on the usage of business cloud services (e.g. Salesforce, Azure, Office365, AWS, etc.), internally developed applications, and shadow IT.