snowflake®

SOLUTION BRIEF

SNOWFLAKE FOR SECURITY ANALYTICS, REGULATORY COMPLIANCE AND ANTI-FRAUD

Aggregate and analyze all your data in the cloud for better, faster, and more cost-effective threat defense and regulatory compliance

BUILT FOR THE CLOUD

Get fast time to value, zero maintenance, built-in product security, and an elastic architecture that instantly and infinitely scales up, down and out.

COST EFFECTIVE

Only pay for the compute you use, and store all your data for long periods at storage rates as low as $23/TB/month after compression.

SPEED AND SCALE

Scale to petabytes of stored data and automatically adjust compute up or down to deliver fast performance and quick query results.

ADVANCED ANALYTICS

Write flexible, custom detection rules to accurately detect threats and minimize false positives. Create rules that correlate across data sources, use Boolean logic, detect outliers off baselines, and leverage external data lookups.

ALL DATA TYPES

Ingest machine data, semi-structured data, and structured data from both cloud-based and on-premises data sources for full threat visibility.

FLEXIBLE, OPEN PLATFORM

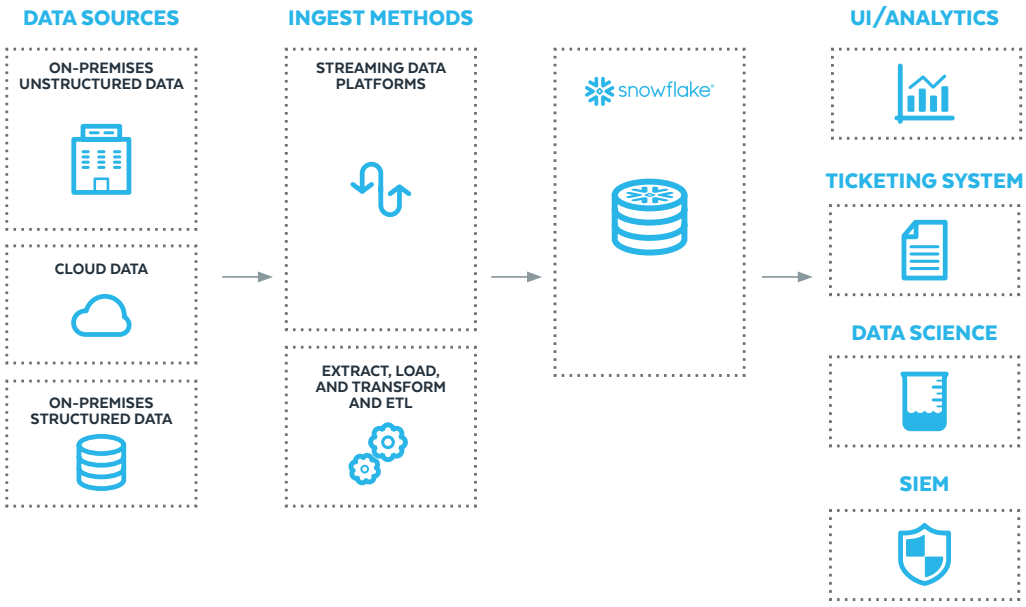
Create tailored rules, visualizations, and investigation interfaces. Integrate with existing SIEMs and anti-fraud products, threat intelligence feeds, BI tools, and data science technologies.

Organizations and their customers are constantly under attack from cybercriminals, nation states, malicious insiders, and fraudsters armed with advanced tactics. In addition, a wide range of compliance mandates require organizations to retain massive amounts of security event data for months and even years.

Traditional cybersecurity and anti-fraud products come up short. They are often on-premises solutions and difficult to manage and scale. Their costly licensing and hardware costs forces you to index only a fraction of your event data and for a very limited time. This is especially dangerous since it often takes six months or more from the time a cyber threat enters an organization to when it's detected. It's critical that you capture and store event data from this time period in order to investigate these threats effectively. In addition, traditional cybersecurity and anti-fraud products offer limited, inflexible detection and analytical capabilities. They also often ingest unstructured/machine data or structured data, but not both. The result is the limited ability to detect, investigate and report on threats thereby increasing your risk of losing data, losing harmed customers and failing to meet compliance requirements.

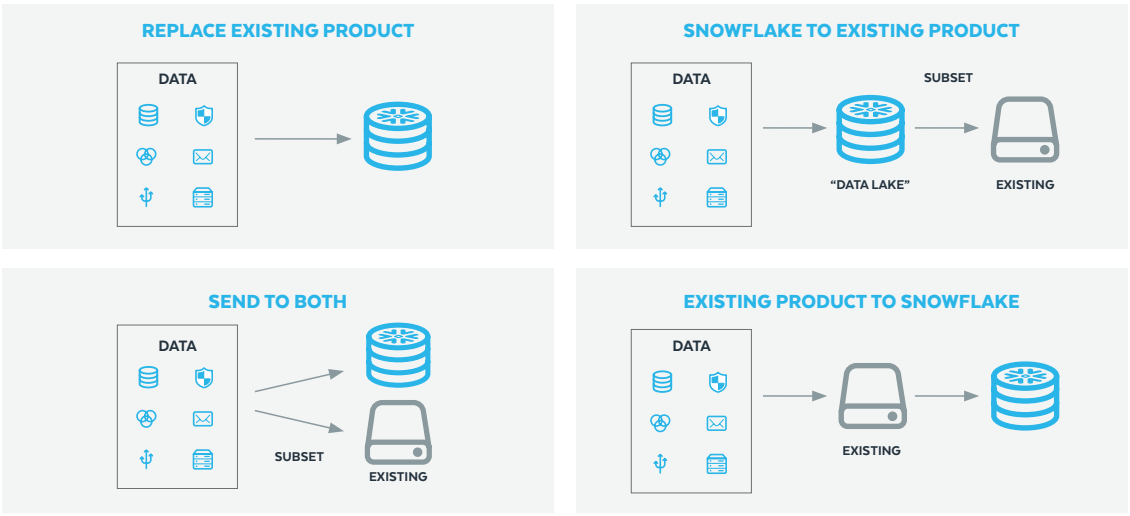
With Snowflake, the cloud-built data warehouse, you can index all of your relevant cybersecurity and anti-fraud machine- and customer-generated data. With storage costs as low as $23/TB/month, and infinitely and instantly elastic compute, you can cost-effectively store and perform fast analytics on petabytes of data going back many months or years for better threat detection, investigations and visualizations, and also to ensure regulatory compliance.

Snowflake's Cloud-Built Architecture



With Snowflake's highly flexible architecture, you can ingest all your structured, semi-structured, and unstructured data. Snowflake also integrates with existing security information and event management (SIEM), and anti-fraud products, business intelligence tools, ticketing systems and data science technologies. In addition, security is baked into Snowflake, with data encrypted from end to end and permission to revoke data access at any time. Snowflake is SOC II Type 2 certified, HIPAA and PCI compliant, and FedRAMP Ready.

Snowflake Can Complement Your Existing SIEM/Fraud Products

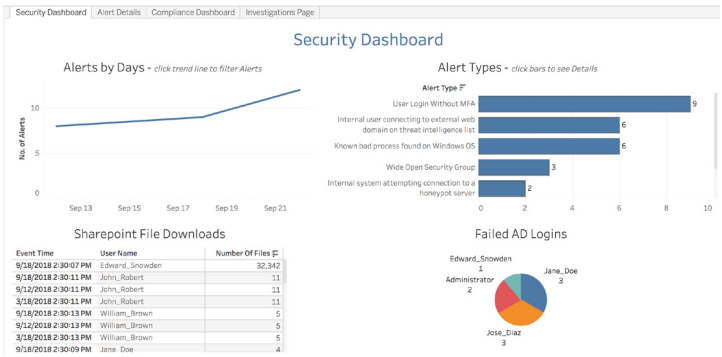


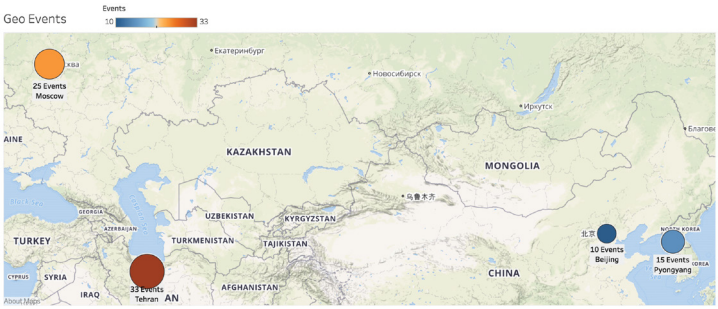
Above are four options to deploy Snowflake as your primary solution or as a complementary solution to your existing configuration. Snowflake can be your primary security analytics/SIEM or anti-fraud product, or can complement existing products you have. For example, you can use Snowflake for more cost-effective, long-term event storage, or to perform immediate analytics on high-volume data too expensive to put into existing products.

User Interfaces and Visualizations for Security Analytics

Snowflake customers can create a wide range of user interfaces, visualizations, and reports aligned to their needs, processes, and workflows. No more frustration from a user interface "locked down" by a vendor. Customize your user interface at will, with reporting, alerting, and investigation interfaces from leading business intelligence partners of Snowflake.

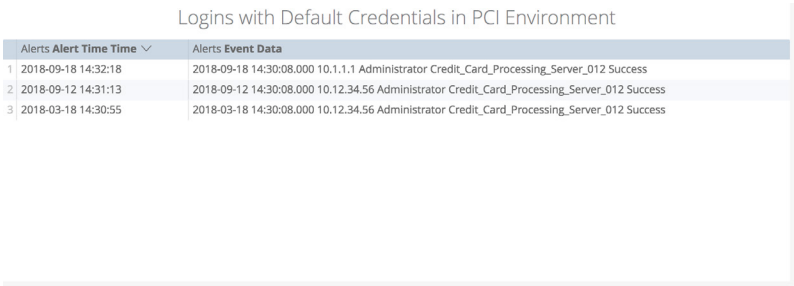
Cybersecurity Dashboard

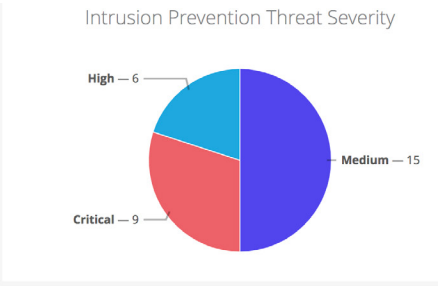


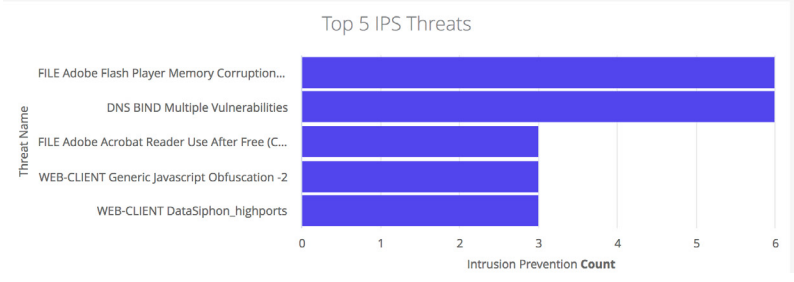


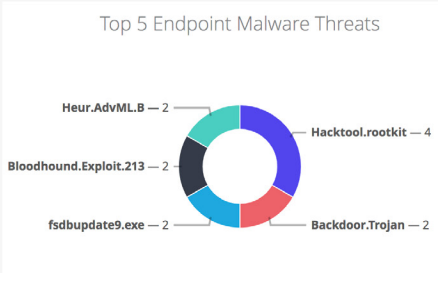
With Tableau, you can show alerts from SQL detection rules written in Snowflake and visualize raw security events as a table, pie chart, and geo-IP map.

Cybersecurity/Compliance Dashboard









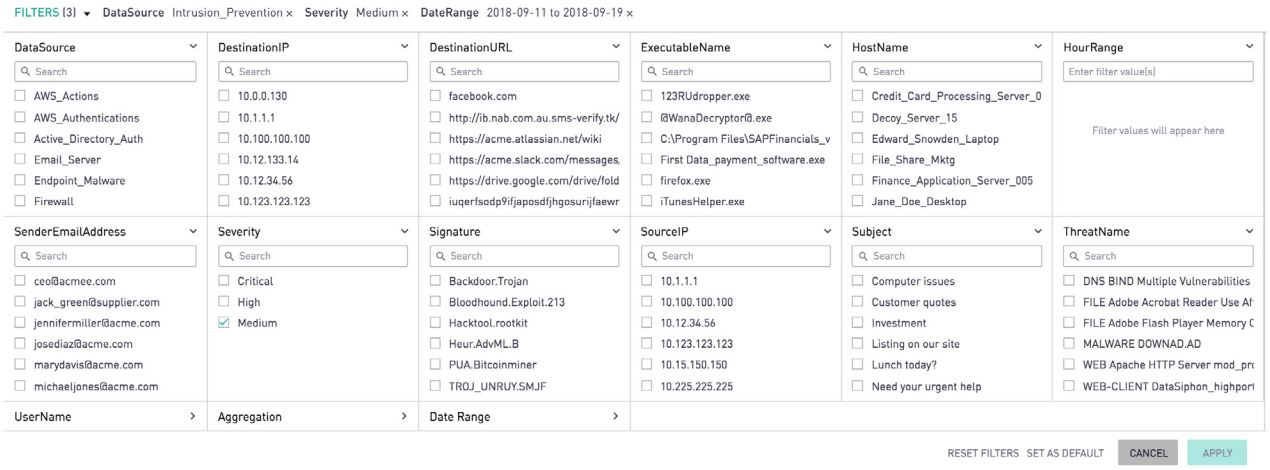
With Looker, you can show alerts from SQL detection rules written in Snowflake and visualize raw security events as a table, pie chart, bar chart, and a donut chart.

Cybersecurity Alert Review Page

ALERT TIME	ALERT TYPE	DESCRIPTION	EVENT DATA	SEVERITY
2018-09-18 21:33:47	User Downloading Suspiciously Large Number of Files	User Edward_Snowden downloaded many more files (Folder - All Finance, Folder - All Engineering, Fo	2018-09-18 14:30:07.000 10.1.1.1 Edward_Sno	2
2018-09-18 21:33:01	Known bad process found on Windows OS	Windows host William_Brown_Laptop is infected with malware @WanaDecryptor@.exe running on pat	2018-09-18 14:30:13.000 William_Brown_Laptop C	2
2018-09-18 21:32:18	User Accesses PCI Assets with Admin Rights	Endpoint 10.1.1.1 accessed PCI Asset Credit_Card_Processing_Server_012 using admins right with	2018-09-18 14:30:08.000 10.1.1.1 Administrator C	2
2018-09-18 21:32:09	Known bad process found on Windows OS	Windows host Mark_Smith_Laptop is infected with malware 123RUdropper.exe running on path C:	2018-09-18 14:30:16.000 Mark_Smith_Laptop C:	2
2018-09-18 21:32:01	Internal user connecting to external web domain on threa	Source IP 10.1.1.1 connected to known bad URL www.sghx34.ru using GET with status 200.	2018-09-18 14:30:07.000 10.1.1.1 Mozilla/5.0 (Wi	2
2018-09-18 21:32:00	Internal user connecting to external web domain on threa	Source IP 10.255.255.254 connected to known bad URL iuqerfsodp9ifjaposdfjhgosurijfaewrwergwe	2018-09-18 14:30:16.000 10.255.255.254 Mozilla	2
2018-09-18 21:31:48	Internal user connecting to external web domain on threa	Source IP 10.12.34.5 connected to known bad URL http://ib.nab.com.au.sms-verify.tk/2611de124b	2018-09-18 14:30:08.000 10.12.34.56 Mozilla/5.0	2
2018-09-18 21:31:47	Internal system attempting connection to a honeypot ser	Source IP 10.1.1.1 attempted to connect to honeypot system 10.0.0.130 using TCP with status Allo	2018-09-18 14:30:07.000 Allow TCP 10.1.1.1 10.0	2
2018-09-18 21:31:25	Known bad process found on Windows OS	Windows host Edward_Snowden_Laptop is infected with malware @WanaDecryptor@.exe running on	2018-09-18 14:30:08.000 Edward_Snowden_Lapto	2
2018-09-12 21:34:02	Known bad process found on Windows OS	Windows host William_Brown_Laptop is infected with malware @WanaDecryptor@.exe running on pat	2018-09-12 14:30:13.000 William_Brown_Laptop C	2
2018-09-12 21:32:28	Known bad process found on Windows OS	Windows host Edward_Snowden_Laptop is infected with malware @WanaDecryptor@.exe running on	2018-09-12 14:30:08.000 Edward_Snowden_Lapto	2
2018-09-12 21:32:01	Internal system attempting connection to a honeypot ser	Source IP 10.1.1.1 attempted to connect to honeypot system 10.0.0.130 using TCP with status Allo	2018-09-12 14:30:07.000 Allow TCP 10.1.1.1 10.0	2
2018-09-12 21:31:57	Internal user connecting to external web domain on threa	Source IP 10.1.1.1 connected to known bad URL www.sghx34.ru using GET with status 200.	2018-09-12 14:30:07.000 10.1.1.1 Mozilla/5.0 (Wi	2
2018-09-12 21:31:51	Known bad process found on Windows OS	Windows host Mark_Smith_Laptop is infected with malware 123RUdropper.exe running on path C:	2018-09-12 14:30:16.000 Mark_Smith_Laptop C:	2
2018-09-12 21:31:33	Internal user connecting to external web domain on threa	Source IP 10.12.34.56 connected to known bad URL http://ib.nab.com.au.sms-verify.tk/2611de124	2018-09-12 14:30:08.000 10.12.34.56 Mozilla/5.0	2
2018-09-12 21:31:13	User Accesses PCI Assets with Admin Rights	Endpoint 10.12.34.56 accessed PCI Asset Credit_Card_Processing_Server_012 using admins right w	2018-09-12 14:30:08.000 10.12.34.56 Administra	2
2018-09-12 21:30:47	Internal user connecting to external web domain on threa	Source IP 10.255.255.254 connected to known bad URL iuqerfsodp9ifjaposdfjhgosurijfaewrwergwe	2018-09-12 14:30:16.000 10.255.255.254 Mozilla	2
2018-03-18 21:33:16	Known bad process found on Windows OS	Windows host Edward_Snowden_Laptop is infected with malware @WanaDecryptor@.exe running on	2018-03-18 14:30:08.000 Edward_Snowden_Lapto	2
2018-03-18 21:32:45	Known bad process found on Windows OS	Windows host Mark_Smith_Laptop is infected with malware 123RUdropper.exe running on path C:	2018-03-18 14:30:16.000 Mark_Smith_Laptop C:	2
2018-03-18 21:32:43	Internal user connecting to external web domain on threa	Source IP 10.255.255.254 connected to known bad URL iuqerfsodp9ifjaposdfjhgosurijfaewrwergwe	2018-03-18 14:30:16.000 10.255.255.254 Mozilla	2
2018-03-18 21:32:15	Internal system attempting connection to a honeypot ser	Source IP 10.1.1.1 attempted to connect to honeypot system 10.0.0.130 using TCP with status Allo	2018-03-18 14:30:11.000 Allow TCP 10.1.1.1 10.0	2
2018-03-18 21:32:03	Internal user connecting to external web domain on threa	Source IP 10.1.1.1 connected to known bad URL www.sghx34.ru using GET with status 200.	2018-03-18 14:30:07.000 10.1.1.1 Mozilla/5.0 (Wi	2
2018-03-18 21:31:58	Known bad process found on Windows OS	Windows host William_Brown_Laptop is infected with malware @WanaDecryptor@.exe running on pat	2018-03-18 14:30:13.000 William_Brown_Laptop C	2
2018-03-18 21:31:27	Internal user connecting to external web domain on threa	Source IP 10.12.34.56 connected to known bad URL http://ib.nab.com.au.sms-verify.tk/2611de124	2018-03-18 14:30:08.000 10.12.34.56 Mozilla/5.0	2
2018-03-18 21:30:55	User Accesses PCI Assets with Admin Rights	Endpoint 10.12.34.56 accessed PCI Asset Credit_Card_Processing_Server_012 using admins right w	2018-03-18 14:30:08.000 10.12.34.56 Administra	2

This cybersecurity alert/incident review page from Sigma Computing shows information on alerts from the result of SQL detection rules written in Snowflake. An incident responder would use a page such as this to see new alerts that need investigating and respond by clicking on any alert to see underlying detail including the raw events.

Cybersecurity Alert Investigation Page



Created with Periscope Data and based on data in Snowflake, this interface provides numerous ways for an incident responder to quickly get the who, what, where, when, and why from petabytes of data and across many data sources, users, and machines to deliver faster threat investigations, response, and remediation.

ABOUT SNOWFLAKE

Snowflake is the only data warehouse built for the cloud, enabling the data-driven enterprise with instant elasticity, secure data sharing and per-second pricing, across multiple clouds. Snowflake combines the power of data warehousing, the flexibility of big data platforms and the elasticity of the cloud at a fraction of the cost of traditional solutions. Snowflake: Your data, no limits. Find out more at **snowflake.com**