Managed Azure Sentinel

SecureSky
Dynamic Cloud Security

Who We Are

SecureSky delivers a complete portfolio of cloud security solutions to help organizations protect their cloud applications, services and infrastructure.

Utilizing cloud-native, third-party and SecureSky patented technologies, our solutions meet the security, compliance and budget requirements of today's dynamic enterprises.

SecureSky solutions include Security Consulting, focused on identifying risk and deploying protective controls and policies and Managed Detection and Response (MDR), which provides Azure Sentinel deployment, tuning and management, active threat detection and threat hunting, expert response and continuous protective control optimization.

Azure Sentinel Overview

Azure Sentinel is a cloud-native, security information and event manager (SIEM and SOAR) platform that uses built-in threat analytics to analyze large volumes of data across an enterprise.

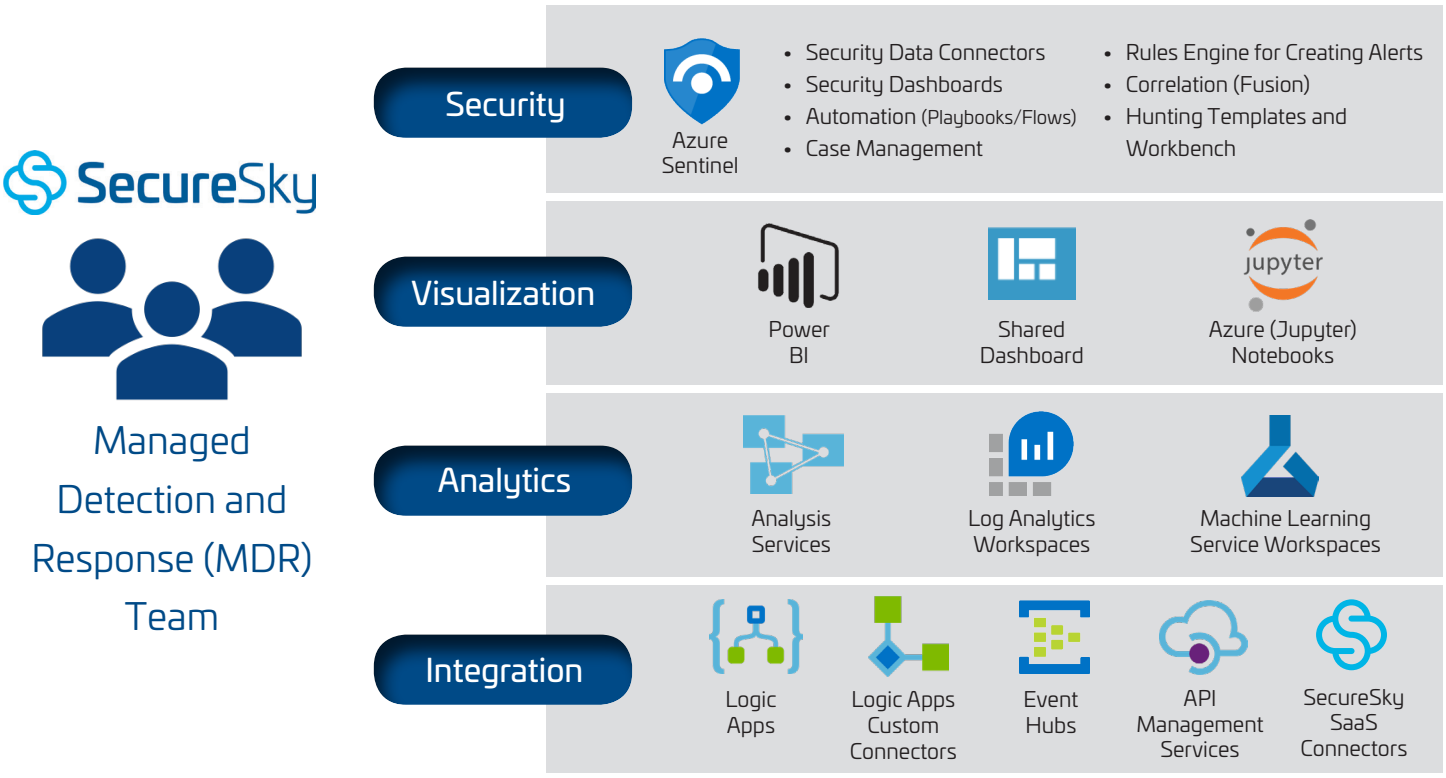
Sentinel aggregates data from all traditional on-premise sources and cloud environments, enabling analysis of millions of records in seconds.

Sentinel includes built-in connectors for easy onboarding of popular security solutions, security data from cloud applications, and supports open standard formats like Common Event Format (CEF) and Syslog.

Sentinel has no upfront cost, with pricing based on usage.

Sentinel Security Features and Interface with Other Azure Modules

The Azure Sentinel application is built on top of three major categories of Azure infrastructure, allowing high-scale, flexible security. This enables rapid deployment, visibility to hybrid environments, powerful analytics and automated response.



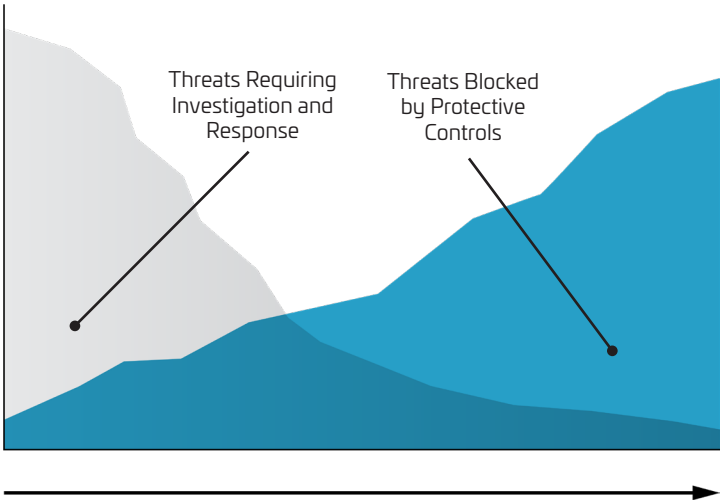
Managed Azure Sentinel

SecureSky
Dynamic Cloud Security

Continuous Optimization of Protection and Detection

Organizations today constantly find themselves reacting to threats and, with a growing cybersecurity skills shortage, are challenged to find resources capable of advanced detection, investigation and response.

SecureSky's Managed Detection and Response (MDR) focus is to evaluate lessons learned from detection and response activities, and deploy protective measures to stop that threat from recurring.



Over time, as protective controls and detection policies are strengthened and unneeded "noise" is tuned out, threat volumes will decrease, allowing detection and response resources to focus on true threats to the environment.

SecureSky Sentinel Deployment Services include:

- Onboarding of log data
- Use of native-Sentinel or SecureSky's SaaS connectors, or build custom connectors for services and applications
- Deployment of storage/analytics cost reduction techniques
- Creation of custom dashboards
- Enablement of Fusion and enhancement of correlation features
- Creation of cross-platform connection for Sentinel Analytics
- Development of threat hunting templates
- Design of log storage schemas and configuration of short and long-term storage repositories
- Building and tuning of alerting rules for investigative case generation
- Expansion of threat hunting capabilities
- Setup of playbooks to execute automatically when an alert is triggered
- Integration of use cases requiring manually run playbooks inside an alert
- Building and tuning of response mechanisms.

Sentinel MDR Services include:

- 24/7 monitoring and event response
- Continuous validation of security configurations
- Ongoing tuning and optimization of protective controls
- Scenario-based, trigger-based and free-form threat hunting.

Contact Us

For more information, please contact us.

e: info@SecureSky.com
p: +1 833.4SecSky (+1 833.473.2759)
w: SecureSky.com

Rev. Aug. 2019