iboss × Microsoft

SOLUTION BRIEF | MAY 2022

SPEEDING TIME TO VALUE

iboss Integration with Microsoft® Azure Sentinel

The Challenge

SOC analysts require high fidelity contextual information to detect threats, along with simplified and automated workflows for immediate response.

The Solution

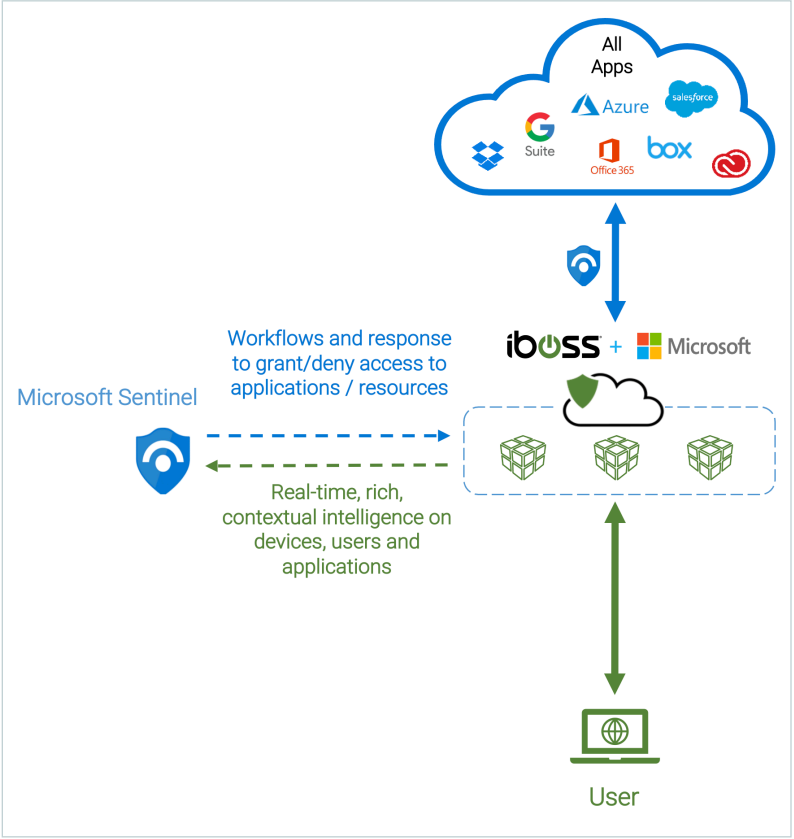
iboss Provides Rich Contextual Intelligence to Microsoft Sentinel

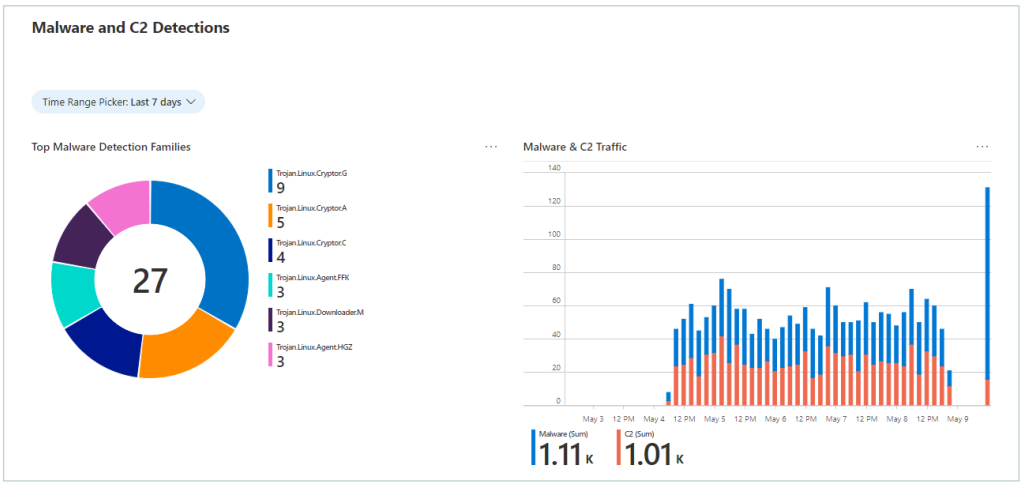
iboss' unique integration with **Microsoft Azure Sentinel** results in ingestion of high fidelity logs from iboss about users and their resource access requests. The integration simplifies risk assessment from user web access.

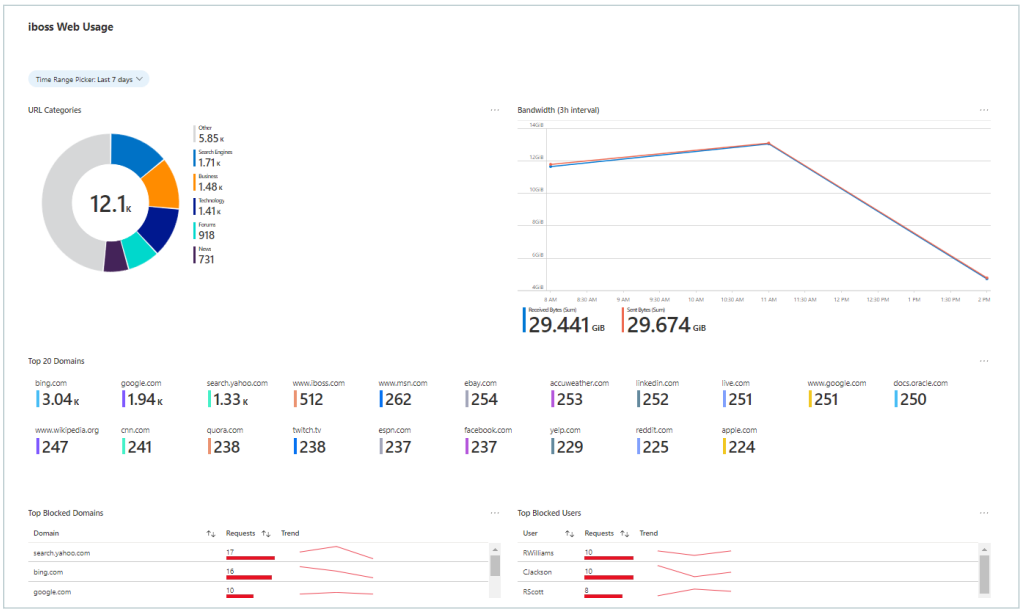
iboss Speeds Time to Value with Microsoft Sentinel

The unique iboss integration with **Microsoft Azure Sentinel** is achieved through a connector application available from within the Microsoft Azure Marketplace. The application activates the integration quickly without need to deploy a virtual machine in **Microsoft Azure**.

The iboss connector package in **Microsoft Azure** marketplace also contains a workbook that prepopulates dashboards for iboss data into **Microsoft Azure**. These dashboards provide immediate insight into web usage and threats.







iboss and Microsoft Sentinel Insure Data Privacy and Compliance

The **Microsoft Sentinel** implementation leverages a unique tenant ID per customer to ensure separation of customer data in both iboss and in **Microsoft Sentinel.**

iboss and Sentinel Integration Eliminates Need for Custom Configuration

The iboss integration parses data into the Common Event Format (CEF) standard for seamless ingestion of iboss data into **Microsoft Sentinel**. Data is normalized to the appropriate fields when forwarded to the schema of the connected **Microsoft Sentinel** instance. This normalization removes the need for aligning custom tables within **Microsoft Sentinel**.

iboss' Microsoft Sentinel Integration Enables Rapid Response

iboss provides high fidelity threat detection from which the administrator can take action with **Microsoft Sentinel's** SOAR functionality to detect and respond to threats or remediate compromised endpoints.

About iboss®

iboss is a cloud security company that enables organizations to reduce cyber risk by delivering a Zero Trust service designed to protect resources and users in the modern distributed world. Applications, data and services have moved to the cloud and are located everywhere while users needing access to those resources are working from anywhere. Built on a containerized cloud architecture, iboss delivers security capabilities such as SWG, malware defense, browser isolation, CASB and data loss prevention to protect all resources, via the cloud, instantaneously and at scale. This shifts the focus from protecting buildings to protecting people and resources wherever they are located. Leveraging a purpose-built cloud architecture backed by 230+ issued and pending patents and more than 100 points of presence globally, iboss processes over 150 billion transactions daily, blocking 4 billion threats per day. More than 4,000 global enterprises trust the iboss Cloud Platform to support their modern workforces, including a large number of Fortune 50 companies. iboss was named one of the Top 25 Cybersecurity Companies by The Software Report, one of the 25 highest-rated Private Cloud Computing Companies to work for by Battery Ventures, and CRN's top 20 Coolest Cloud Security Companies of 2022. To learn more, visit www.iboss.com

+1 877.742.6832
sales@iboss.com

101 Federal St
Boston, MA 02110