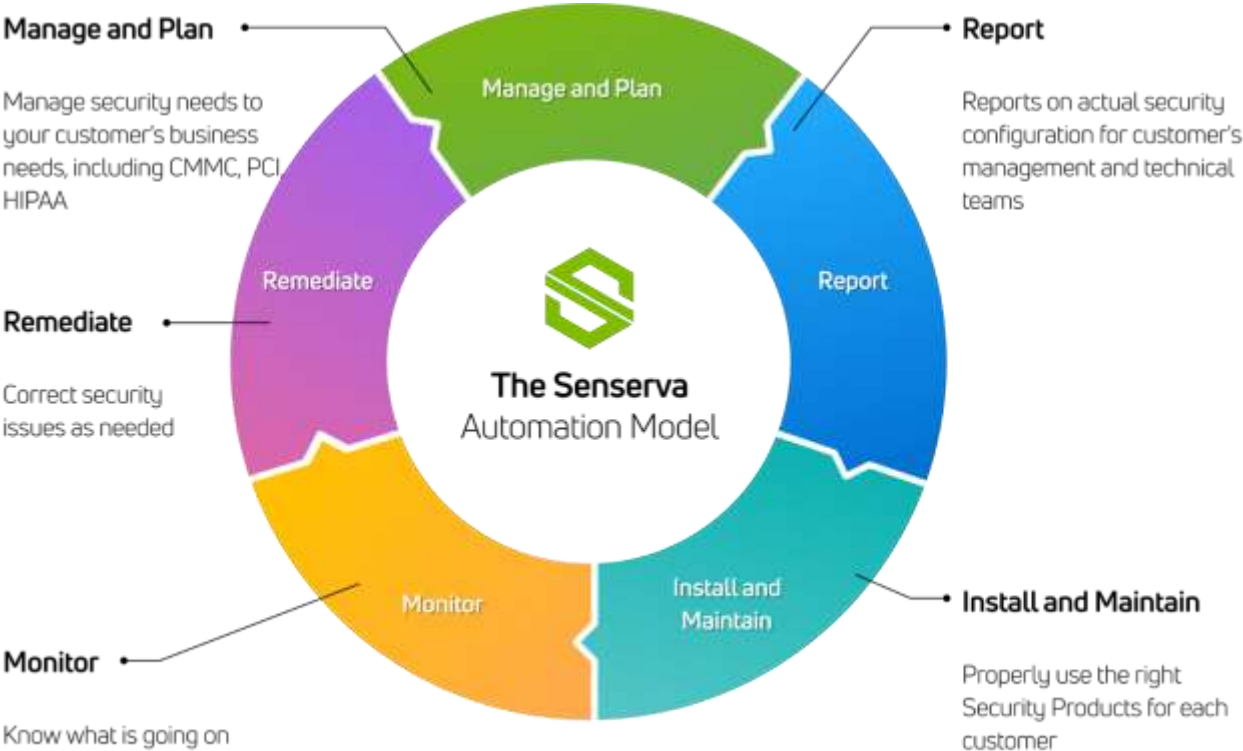


Senserva Optimizes Microsoft CSPM for MSSPs

Senserva helps MSSPs ensure the proper use Microsoft security across all their customers from one interface. To do this Senserva intelligent security automation solutions combine security data from Microsoft Security products to analyze, and manage critical security configuration information across your customers, enhancing product efficiency and the effectiveness of your team.

Information has little value until it is correlated, analyzed and summarized and put in the hands of the right person to act on it.

Senserva is Full Solution Focused



Simplifying Security Management for Microsoft MSP/MSSPs

Senserva provides broad, customizable security automation for Microsoft Intune, Defender, Sentinel and Entra that builds on your current investment. Customers can work with it out of the box or collaborate with Senserva to tailor it to their specific needs.

Ensuring Optimization of the Right Security Products

With countless security products available, it's challenging to determine which ones are needed. Senserva guides users to the right products, many of which are already licensed via Microsoft E5 or other licenses, and ensures these products are running properly to meet the business's security and compliance needs.

Our Mission

Senserva's mission is to simplify security by helping choose the right tools, continually ensuring their proper operation, and providing actionable insights through comprehensive reporting and business intelligence.

Simplify the Complex

Security management is a multifaceted endeavor. A typical enterprise has thousands of endpoints to secure, users to onboard and offboard, patches to install, servers and cloud services to oversee, and various security products and licenses to manage. Security analysts play a critical role in ensuring that all these components align with compliance standards.

Senserva Provides Focus Across Microsoft Security Products

Senserva simplifies security management by continuously collecting and analyzing security data from Microsoft products with advanced scanning engines. This automates the configuration and output of security products, requiring users only to monitor reports highlighting configuration drifts, security trends and emerging or present risks.



Advanced Drift Detector

Unified Security Dashboard

Generative AI Driven Secure Advisor

Advanced Drift Detector

Senserva's Advanced Drift Detector is an industry-first solution that analyzes multiple security products across tenants for security posture drifts. It provides detailed explanations on why a drift has occurred, how to fix it, or how to work around it, covering thousands of drift types.

Unified Security Dashboard

Our Unified Security Dashboard offers a Single Pane of Glass view across all security products in your environment. Driven by Power BI, this dashboard provides insights into your security product usage and reviews critical information not found elsewhere.

Simplifying Security Management

Senserva simplifies security by guiding users to the right tools, ensuring their proper operation, and providing actionable insights through comprehensive reporting and business intelligence.

Easy to Use

At Senserva we believe that easy-to-use solutions are the cornerstone of effective automation. Users appreciate straightforward interfaces, clear instructions, and minimal learning curves. An intuitive solution reduces friction and encourages efficient utilization.

Data Driven

Senserva recognizes that not all data is equally valuable for security purposes. Senserva's approach to data-driven decision-making revolves around ensuring that security automation leverages the right data at the right time. By curating relevant information, Senserva ensures that security processes are based on accurate and actionable insights. This avoids noise and enhances efficiency.

Getting All the Right Data is Key

Senserva collects security and other critical data, analyzes it, stores it, and makes recommendations based on it. Security automation relies on this data, including configuration data, event logs, and reporting data generated by Senserva. The principle of 'Garbage In, Garbage Out' applies; the effectiveness of security measures depends on the quality of the data driving them.

The data volume can be immense, with much of it managed daily by Microsoft before we even see it. Microsoft and other vendors feed data into security products, which in turn create or generate new data. MSP/MSSPs and business owners need to understand this data to effectively address potential security issues.

Making the Right Data Make Sense

Senserva advanced analysis and reporting reviews and provides advice for thousands of configurations in seconds.

Customer Feedback

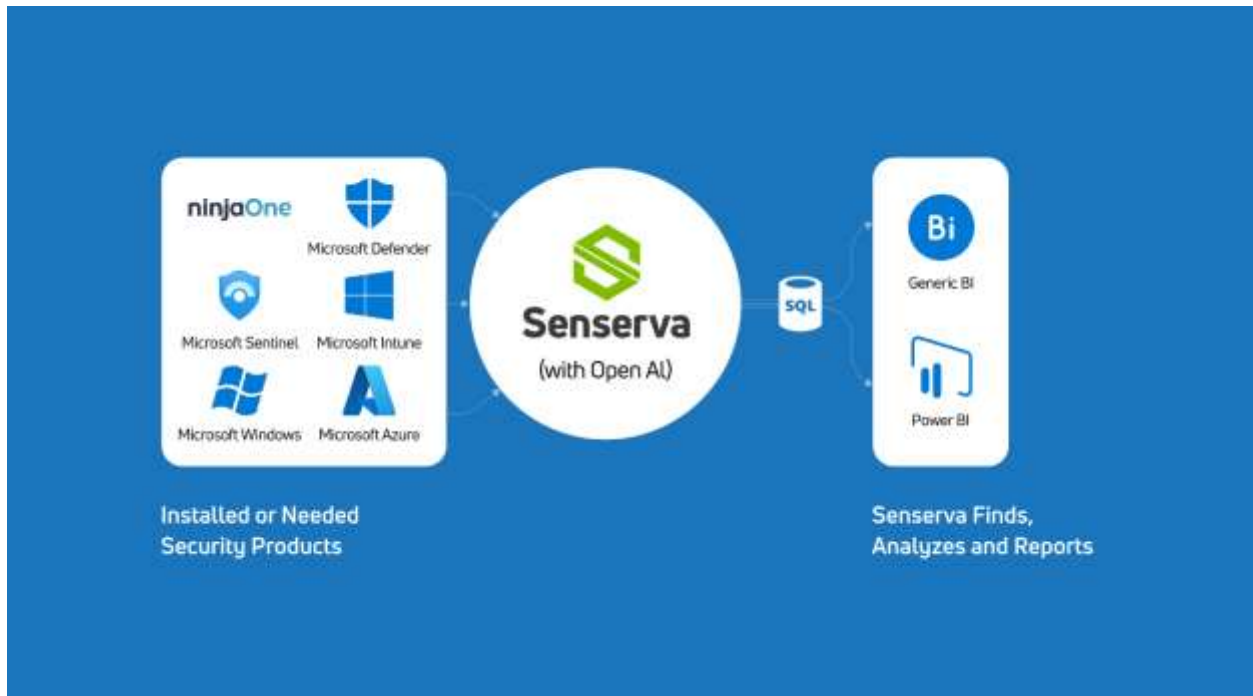
"Our partnership with Senserva has been instrumental in co-creating cutting-edge security solutions, harnessing the power of Microsoft technologies. This dynamic synergy not only enhances our capabilities but also guarantees our customers receive tailored, forward-thinking security solutions that seamlessly adapt to their ever-evolving needs." **Wade Dauphinee, Senior Vice President of Bulletproof's Managed Security Services Division**

"Members of MISA, like Senserva, offer solutions that extend Microsoft security to quickly identify and remediate security incidents before they cause business impact", said **Eric Burkholder, PM, Technology Partnerships, Microsoft Sentinel at Microsoft Corp.** *"The integration of Microsoft Sentinel with the Senserva's award-winning Cloud Management Solutions allows us to work together to enhance customers' security posture with less complexity."*

"Brave North Technology approached Senserva to enhance security protocols and solutions for our managed service clients. From day one, we have been impressed with the dedication to a true partnership and the depth of experience and knowledge of the Senserva team. The innovative solutions and ability to leverage Microsoft tools is impressive and cutting-edge. The

significant value provided for our clients is huge and the flexibility provided by Senserva sets them far above other partners." **Joel Barker, President & CEO of Brave North Technology**

Senserva Data Flow



Example Reports

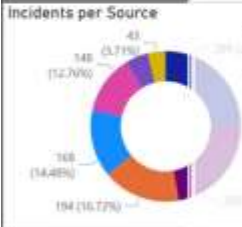
Senserva detects thousands of drifts across various products and tenants in seconds. Managing drift is crucial for security, but it can be challenging due to the multitude of products and settings. Each of these settings must have a clear answer regarding how it should be configured, and once set, it needs to remain consistent.

Month:
 November 2023
 December 2023



of Incidents
1.279K

of High Severity
195



Security Operations Dashboard Across all Tenants and Security Products

ID	Description	Severity	Date
20362	Suspicious file activity on one endpoint	High	11/12/23
20363	Impersonation attempt on one endpoint	High	11/12/23
20364	Adaptive application control policy violation was audited	Informational	11/12/23
20365	Global Administrator Attempted Sign-in	Medium	11/12/23
20366	Exchange workflow Mailbox Accessed operation anomalous	Medium	11/12/23



TOP 10 Countries of Origin (Last 6 Months)

Country	Count	Percentage	Month
United States	34	45.33%	November 2023
Germany	25	33.33%	November 2023
United States	24	57.14%	December 2023
Latvia	14	18.67%	November 2023
Germany	13	30.95%	December 2023
United Kingdom	3	7.14%	December 2023
Spain	2	2.67%	November 2023
Total	117		