



Sensato Cybersecurity Solutions

United We Stand. Divided We Fall.

A unified threat management (UTM) approach for cybersecurity delivers operational simplicity and lower costs while providing an integrated command post to better manage assets, risk, intelligence, breach detection, analytics and counter measures.

You can buy every best-of-breed cybersecurity tool on the market, but all those whistles and bells can become a distraction rather than alerting you to a serious breach. Worse, different solutions from different vendors may be making a lot of noise but if they're not talking to each other, that's all it is—noise.

“None of it matters if it all doesn't come together and empower you at the moment when you're being attacked,” says cybersecurity expert and Sensato CEO John Gomez. “The last thing you want when your system is under attack is having to go searching to figure out how to do an rsync or SCP or SFTP transfer because you haven't done it before and you've got to get the logs off the system before you shut it down to stop the attack from spreading.”

It's no wonder that solutions have multiplied as [the threats have multiplied](#), but using different solutions from different vendors to address each security task can become operationally expensive and difficult to manage.

“A lot of people have to come together to defend an organization, but there hasn't been a single approach or a holistic way of doing cybersecurity,” says Gomez. “Unfortunately, that's one of the big things attackers actually rely on—that we're not going to be holistic in our defenses.”



INFO@SENSATO.CO



@SENSATOCYBERSEC



844.736.7286



@SENSATO
CYBERSECURITY
SOLUTIONS



Sensato Cybersecurity Solutions

COMMAND CENTRAL LIKE YOU ALWAYS IMAGINED

A unified threat management (UTM) solution puts every piece of the security puzzle on one screen—kind of like standing at the helm of the Starship Enterprise:

- **Breach detection agents**—Deception technologies are one of the only things that actually scare attackers, so, of course, you should plant them liberally and strategically. [Sensato's Nightingale](#) started out as a BDA solution, designed to detect a breach as quickly as possible.
- **Continuous threat intelligence**—A stream of threat intelligence from a variety of sources is critical. Sensato designed the Nightingale Agile platform to include an Open Intelligence Feed of open source intelligence from government defense agencies and other sources.
- **Network intrusion detection**—This is a given, but the NIDS is one piece of a UTM that simply cannot fail. Sensato's Nightingale is built on a telecom-grade platform to ensure reliability.
- **Asset management**—Organizations often don't know what's on their networks. A robust UTM like Sensato's Nightingale provides a system that builds a complete accounting of all assets, similar to how attackers scan and inventory a system they've breached. Nightingale also incorporates a social graphing model to determine and locate an organization's most important assets—those systems that can absolutely never go down.
- **INFOCON protocols**—Speed is of the essence when you're under attack. INFOCON protocols allow you to move your entire organization to a higher defensive posture with a single command. Much like the protocols practiced in hospital trauma centers every day, these standing orders trigger action informed by training and preparation.
- **Unified dashboard**—One of the biggest obstacles to effective management of cybersecurity attacks is the decentralized nature of an array of siloed products. Nightingale brings the entire cybersecurity operation into a single feed, where IT security professionals can see the current risk level,



INFO@SENSATO.CO



@SENSATOCYBERSEC



844.736.7286



@SENSATO
CYBERSECURITY
SOLUTIONS



Sensato Cybersecurity Solutions

receive alerts, launch response protocols in the event of a breach, run forensics on the breach, and shut it down.

- **Journaling**—In the midst of an attack, it can be difficult to document every action taken to protect assets. Nightingale automatically keeps a time-stamped journal for future review and auditing.
- **Reminders**—Keeping track of everything you need to do to stay in compliance with government regulations can be a daunting chore. Nightingale includes reminders to help organizations maintain public policy compliance as part of the natural workflow.
- **Forensic analytics**—You need to be able to quickly see where an attack is occurring, the timeline of an attack, and the history of an attack. Nightingale gives you a full picture of every step of an attack so you can respond in real-time and perform a full analysis later to address system vulnerabilities.

“Since the ‘80s, investment in cybersecurity has gone up every year, and yet every year the number of successful cyberattacks has also gone up,” says Gomez. “We decided we needed to build a single, integrated cybersecurity platform to bring order to the chaos and help unify IT security teams in more effectively defending against attack.”



INFO@SENSATO.CO



@SENSATOCYBERSEC



844.736.7286



@SENSATO
CYBERSECURITY
SOLUTIONS