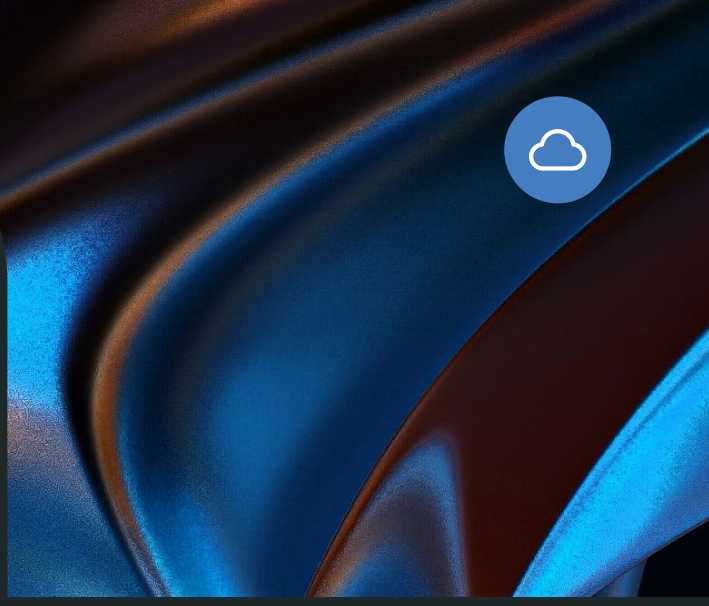
SOLUTION BRIEF

Protecting the protectors across SaaS apps.

SonicSentry MDR for Cloud.



Business today goes beyond just the endpoint. On an average day, employees may log into many different cloud-based software-as-a-service (SaaS) applications to do their jobs. From email to productivity tools like Microsoft 365 and collaboration tools like Slack, all of these tools are treasure troves of crucial business information by themselves, while also being excellent ways into a business for a hacker looking to cause chaos.

While it's easy to think that small-and medium-sized businesses (SMBs) aren't of interest to cyber criminals, the opposite is actually true: often SMBs are more attractive targets because bad actors believe they won't have very good defenses. They can also be caught up in larger attacks that make use of phishing or spoofed login pages for these cloud apps, making security for these important pieces of software even more important.

If you're an MSP helping to keep SMBs secure, you know your clients are counting on you, and you may be wondering how best to address the additional attack surface created by these cloud SaaS apps. The easiest way to think about securing them is to consider them another endpoint and secure them with a combination of technology and monitoring by experts. But how? That's where SonicSentry comes in to help keep you and your customers secure.

SonicSentry MDR for Cloud makes it possible for you to bring powerful security technology backed by the expertise of a 24/7 security operations center (SOC) to your clients' cloud apps. We pair prevention technology with dedicated detection and response monitoring to prevent many common cloud and email threats from reaching your users and quickly mitigate any threats that make it through. SonicSentry MDR for cloud is a combination of these two prevention and response offerings; they can be purchased separately to give your customers the flexibility they need, but combining them creates the ultimate in cloud security.

Prevention with Cloud Email Security

Business email compromise is one of the leading starting points for breaches; in fact, up to 90% of cyber-attacks are believed to begin with a phishing email. Even the most savvy employee can be duped by phishing on a bad day, so phishing prevention is paramount.

Cloud Email Security, powered by Avanan, prevents phishing emails from ever reaching users' inboxes. It scans for over 300 phishing indicators like spoofing and brand impersonation. It uses machine learning to baseline communication used in an organization to tailor its protection to each business and give more accurate detections. Avanan also scans every link in emails and within files to identify malware, helping to prevent breaches before they happen.

SOC monitoring for Cloud Email Security, powered by Avanan, is available as an add-on, or it's included at no additional cost if purchased with Cloud Threat Analytics.

Response with Cloud Threat Analytics

The many SaaS business applications used every day by employees drastically expand an organization's attack surface. Attackers who access these apps can steal important business information or even burrow their way deeper into the network. Monitoring for anomalous activity on these apps is paramount.

Cloud Threat Analytics leverages technology and our 24/7 expert SOC to detect and respond to cyber threats within many common SaaS business apps. The SOC is able to monitor for logins from unapproved or restricted locations, and can quickly isolate a compromised account. The SOC also monitors for and alerts you to admin role and multi-factor authentication changes; this can help you identify insider threats or admins abusing their role.

Pairing Cloud Threat Analytics and Cloud Email Security brings the best of prevention and response together to create MDR for Cloud, empowering you as an MSP to bring the best cyber defense to your customers.

Ready to learn more?

Contact us today to learn how you can get started with a free proof of concept!

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035 | Refer to our website for additional information.

© 2025 SonicWall Inc. ALL RIGHTS RESERVED.
SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners. The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. Except as set forth in the terms and conditions as specified in the license agreement for this product, SonicWall and/or its affiliates assume no liability whatsoever and disclaims any express, implied or statutory warranty relating to its products including, but not limited to, the implied warranty of merchantability, fitness for a particular purpose, or non- infringement. In no event shall SonicWall and/or its affiliates be liable for any direct, indirect, consequential, punitive, special or incidental damages (including, without limitation, damages for loss of profits, business interruption or loss of information) arising out of the use or inability to use this document, even if SonicWall and/or its affiliates have been advised of the possibility of such damages. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

SONICWALL®