

# Capture Security Center Unified Insights

Accelerate time-to-insights at speed and scale

The Capture Security Center Unified Insights is built around the sole purpose of helping business and security leaders and their security operation teams find the correct answers to tough security questions quickly so that they can run a security-first organization.

It lets them do a lot of things right, such as: Maintaining a robust security posture, staying ahead of potential threats and risks, securing company assets, keeping users safe, establishing effective security policies and protocols, fixing security and performance problems fast, and correcting operational issues proactively.

## HIGHLIGHTS

### Business Benefits

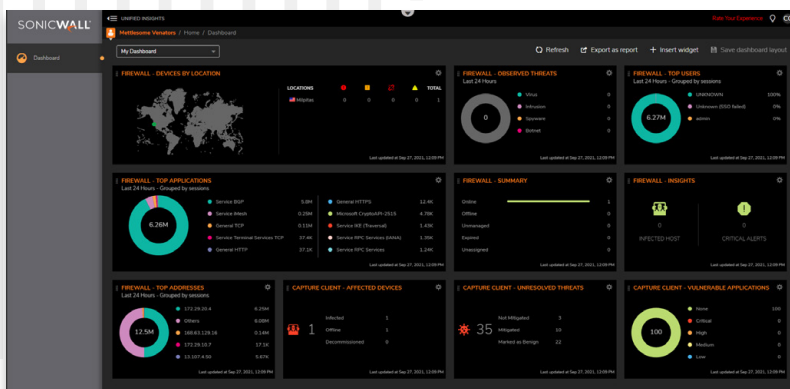
- Validate security posture
- Aid in cyber-defense planning and budgeting
- Fulfill applicable regulatory obligations

### Operational Benefits

- Monitor firewall, wireless and endpoint analytics in one place
- Keep a pulse on users, devices, and networks health metrics
- Calibrate and enhance security controls
- Maintain network health and performance
- Stay on top of all web and application activities

### Security Benefits

- Analyze indicators, gather evidence and perform timely defensive actions
- Triage and zero in on critical alerts that matter most before harm occurs
- Actively survey signs of potential risks, threats, and abnormal activities
- Know what data assets and devices are under attack and at-risk
- Spot and fix network or performance issues fast
- See potential risks and anomalies for early intervention



**Decrease risk by responding faster to security events:**

[sonicwall.com/csc](https://sonicwall.com/csc)

However, many organizations still struggle to achieve their objectives when operating under poor conditions where there are too many data silos, causing data overload and analysis paralysis to an already overwhelmed team. Thus, finding out which devices are down or infected, where attacks are coming from, the types of threats and their volume and frequency, and how many applications are risky becomes a constant source of risks and frustration. This situation leads to a dangerous situation where security stakeholders don't have the necessary visibility and the answers fast enough to do their jobs right.

## Unified Insights

Unified Insights help solve these serious problems by putting the power of centralized security intelligence and global incident response back in the hands of security pros. Analytics from SonicWall firewall, wireless, and endpoint security products merge into one dashboard for central monitoring and troubleshooting. Unified Insights also accelerates time-to-insights at speed and scale, creating unprecedented user experience with intuitive

data visualization across large data volumes for complete security transparency and analytics applications around:

- Improving risk analyses for policy actions
- Exploring data-driven patterns and anomalies across devices, users and applications
- Answering questions about who, what, where and when
- Speeding IT decision-making for real-time risk containment and incident response

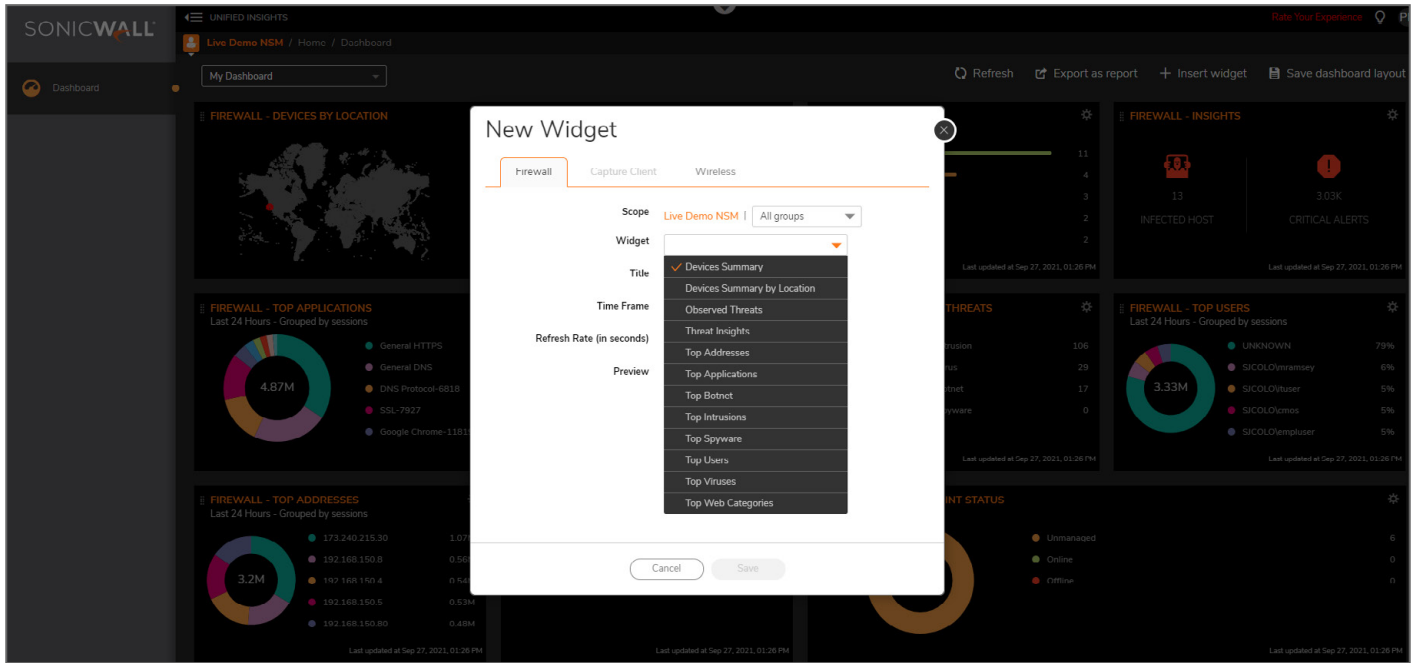


## Build your custom tenant-specific dashboard in a few clicks

The dashboard is customizable for a tailored user experience. Users can pick from a wide range of pre-built widgets and arrange them in a personalized fashion that best suits their intended use on a per-tenant basis. They can use the filtered

information to proactively observe risks and investigate repeating threats to see where attackers are coming from, who is targeted and at-risk, and what parts of the network are most vulnerable to attack.

### Intuitive self-guided customization workflow



### Tenant-specific dashboard



## Single sign-on (SSO) context-aware drill down

With central visibility, users benefit from having a top-down understanding of the state of their security posture combined with the latitude to proactively explore and investigate laterally or drill deep into layers of analytics within their firewall, endpoint and wireless datasets. And based on those investigations and findings, analysts and responders can take corrective actions, tune security policies as needed, and fix whatever problems that come out in the discovery process.

## Licensing

Unified Insights is a value-add service offered at no additional cost, so licensing is not required. The service is built into the SonicWall Capture Security Center single-pane-of-glass cloud management portal. It is automatically enabled and available to customers with tenants that have activated supported products.

## Supported Products

- Any [SonicWall firewall](#) managed by [SonicWall Network Security Manager \(NSM\) SaaS Essential](#)
- Any access point and switch managed by [SonicWall Wireless Network Manager \(WNM\)](#)
- [SonicWall Capture Client](#)

**Gain insights into your entire security ecosystem with Capture Security Center.**

[sonicwall.com/capture-security-center](https://sonicwall.com/capture-security-center)

## About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era and a work reality where everyone is remote, mobile and unsecure. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide. For more information, visit [www.sonicwall.com](http://www.sonicwall.com) or follow us on [Twitter](#), [LinkedIn](#), [Facebook](#) and [Instagram](#).



### SonicWall, Inc.

1033 McCarthy Boulevard | Milpitas, CA 95035

Refer to our website for additional information.

[www.sonicwall.com](http://www.sonicwall.com)

SONICWALL®

### © 2021 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.