**CONNECTWISE**

# ConnectWise SIEM
## A Threat Detection Platform Built for MSPs

Collection and analysis of client log data for active threats is foundational to good defense-in-depth. What's normal activity? What's out of baseline? What needs investigation? Finding needles in the haystack requires log ingestion across all clients and automated analysis informed by real-time threat intelligence. ConnectWise SIEM streamlines this process without the costs, complexity, and staffing typical for traditional SIEM configuration and baselining—and is backed by 24/7 monitoring and response by expert analysts. You gain greater control and visibility of your clients' environments to root out threats while leveraging the force multiplier of a world-class SOC (security operations center).

## Centralize threat visibility and analysis, informed by cutting-edge threat intelligence

### Multi-tenant threat detection that covers YOU as well as your clients

Your customers aren't the only ones under attack by cyber criminals; stories of attacks and breaches of MSPs are common news. This not only makes you vulnerable, but allows access to your clients through your network. Protect your house with ConnectWise SIEM, then protect your clients.

### Advanced security without the advanced price tag

Adding an advanced service offering is daunting—staffing is potentially a massive investment. Leveraging the ConnectWise SOC means you can add staff (and expertise) without adding headcount. We partner with you, handling threat detection and monitoring.
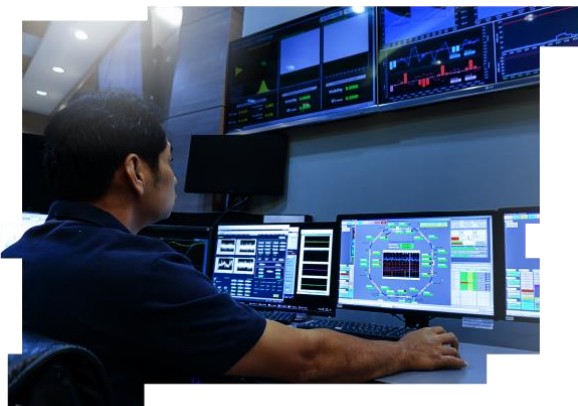
### Easy set-up; works with your existing security stack

After an easy one-hour installation and setup, your network will be monitored by certified analysts. ConnectWise SIEM offers a view of raw indicators of compromise so your team can participate; or use it as a window to watch our SOC do the dirty work.

ConnectWise SIEM works with all of your existing endpoint protection and other security products - no need to buy any additional solutions or change what you're already using.

### Managed detection with data transparency

ConnectWise SIEM is a complete threat detection and response platform: intrusion detection (IDS), threat intelligence management (TIP), and event logging with next-gen SIEM. Multitenancy allows you to manage clients, while the ConnectWise SOC escalates identified threats to you for remediation.

### Integrated with ConnectWise Manage and Automate

ConnectWise SIEM syncs with your clients in ConnectWise Manage® to provide real-time threat activity notifications along with tickets auto-generated to whichever service boards you choose. Receive real-time threat activity notifications. Respond to SIEM incidents with ConnectWise Automate® scripts, quarantine machines, and more. With ConnectWise SIEM, and you can generate network and log-based tickets in response to any scenario you can imagine. Speak with a ConnectWise representative to learn about latest integrations.



## "Perception is reality. This tool helps me sleep at night."

— ROB WILKINSON, VP, Service Delivery, Apex IT Group

# Affordable, holistic threat detection built for MSPs

## Explore the Features of ConnectWise SIEM

### Multi-Tenancy

ConnectWise SIEM is built with multi-tenancy at its core. Easily manage alerts for as many clients as you want.

### Threat Hunting

While the ConnectWise SOC works to alert you of real threats, your team is free to drill down into the same alert data for investigation and analysis of network traffic and log data.

### Log Ingestion

You can ingest logs from syslog and MS Windows event logs and retain them to meet client compliance requirements.

### Intel Agnosticism

In addition to the infusion of real-time threat intelligence from the ConnectWise Cyber Research Unit, the ConnectWise SIEM connects to and consumes the best sources of threat intel to help keep pace with evolving threats. 'Sightings' of reported threats are shared within a community of partners to deepen threat visibility.

### Threat Management

ConnectWise SIEM allows you to manage your own threat indicators along with build out of a threat repository at the fraction of the costs typical of threat intelligence platforms (TIP), giving you even greater control of your threat data.

### Reporting

Enhanced reporting and visualizations deliver extra insights to you and the ConnectWise SOC into your client endpoints and network data traffic.

## Easy and affordable threat detection!
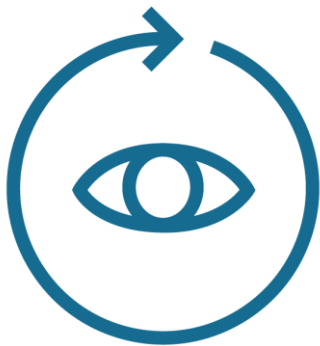
**Full network visibility informed by real-world threat intelligence**

**24/7 monitoring and response without hiring additional staff**

**Reporting that eases the burdens of compliance requirements**

ConnectWise SIEM, an easy, flexible, and powerful tool for protecting you and your clients backed by 24/7, world-class SOC monitoring and response.

Contact us for a live Demo @ManagedServices@dandh.com