Datasheet

Security Monitoring

Triage. Investigate. Remediate.

Rooted in 20 years of experience and with hundreds of customers, Cygilant SOCVue Security Monitoring collects security events across your IT infrastructure, network, and applications. Our Security Analysts triage and investigate potential security incidents to give you rapid actionable recommendations.

Combining log management and security information and event management (SIEM) technology with machine learning, Cygilant helps you to proactively eliminate threats and meet compliance objectives.

Cygilant saves you time spent digging through the noise of thousands of events, or analyzing raw log files, to determine what is happening in the network.

Cygilant's simple integrated service

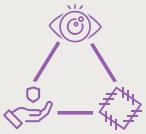
Whether augmenting a security program or starting from scratch, Cygilant hunts, detects and quickly responds to threats by leveraging its dedicated Cybersecurity Advisors, 24×7 Security Operations (SOC) team and our SOCVue Platform.

Cybersecurity Advisors

Dedicated experts work one-on-one with you as an extension of your team to identify and meet your security goals.

24×7 SOC Team

We operate global Security Operation Centers (SOCs) with four tiers of humans from level 1s to 4s working around the clock.



SOCVue Platform

SOCVue simplifies and consolidates multiple streams of security data to help detect and respond to threats faster and effortlessly collaborate.

Security Monitoring Benefits

- **Improved security posture** – comprehensive, up-to-the-minute threat intelligence, visibility into security events, real-time incident notification and guidance to quickly address security issues.
- **Dedicated cybersecurity experts** – Our security experts work for you doing time-consuming incident investigation and analysis. You get time back to focus on other priorities. We monitor your systems outside of business hours for round the clock coverage.
- **Save money** – Cygilant's affordable Cybersecurity-as-a-Service reduces capital investments in costly dedicated security technology.
- **Consolidated reporting** – Daily and monthly security and compliance reports across your systems.

How it Works

What You Get with Cygilant

The Cygilant Security Monitoring subscription includes:

- **More cybersecurity resource**– an extension of your own security and IT staff providing continuous 24x7 monitoring of your security environment.
- **Cygilant SOCVue platform** – Manage your incident response process with integrated dashboards, ticketing, and reporting through Cygilant's security operations platform.
- **Managed SIEM** – Choose LogPoint or AlienVault. The SIEM is installed, configured and maintained by Cygilant Cybersecurity Advisors.
- **Alerts** – The team develops a set of correlation rules to trigger alerts for suspicious activity or security violations. Rules are regularly fine-tuned and policies updated.
- **Audit log management** – Cygilant implements a formal process for the maintenance, monitoring and analysis of audit logs as recommended by SANS/CIS Critical Security Controls.
- **Security and compliance reporting** – Monthly security scorecard reports, scheduled event reports on a daily or weekly basis, automated compliance reports for common regulatory frameworks and custom reports as needed.

Join 200+ businesses that trust Cygilant

Fitchburg State University · BankNewport · Donor Network West · elevate · University Credit Union

Let's talk: 1-877-564-7787

CYGILANT®

Boston | Belfast