DATA SHEET

Trustwave Managed Threat Detection: On-Site SIEM Options

EASIER SIEM OWNERSHIP COMBINED WITH 24X7 THREAT MONITORING

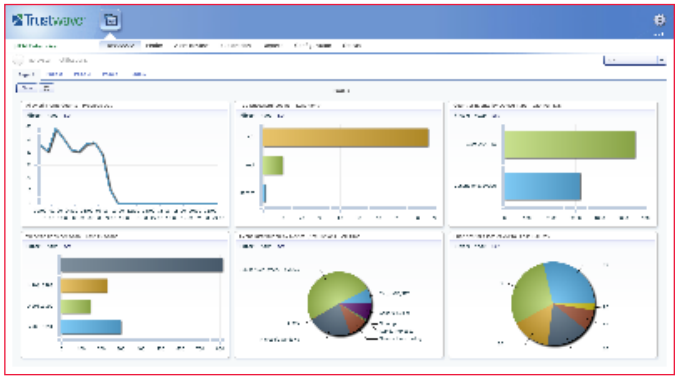
Benefits

- Increased threat visibility
- Earlier breach detection
- Global threat intelligence
- SpiderLabs expertise
- Optimizing existing solutions
- Local SIEM backed by 24x7 threat monitoring

Most organizations are challenged to keep up with advanced threat detection. Analyzing and correlating log and event information coming from devices and solutions in their IT environment takes time and expertise. For this reason, many organizations choose the Trustwave Managed Threat Detection (MTD) service to provide 24x7 security monitoring. And while most of these organizations prefer to leverage the MTD service in the Trustwave cloud, some require an on-site SIEM. For these organizations, Trustwave offers MTD with Hybrid SIEM or Co-Managed SOC options.

The Trustwave Managed Threat Detection service helps organizations of all sizes monitor for and detect threats 24x7. MTD combines a proprietary analysis engine to analyze and correlate events from a broad array of devices and solutions with industry leading SpiderLabs Threat Intelligence and security expertise from SpiderLabs experts. More information about the Trustwave MTD service is available in the Services area the Trustwave website under Managed Threat Detection.

Easier SIEM Ownership



The Hybrid SIEM and Co-Managed SOC options are designed to make SIEM ownership easier and help organizations with unique SIEM requirements while still delivering 24x7 security monitoring. For years, organizations have been challenged to successfully deploy and operate SIEM solutions. Often that's due to lack of training, lack of security resources to manage the SIEM, or simply fatigue when the SIEM generates more alerts than the security team can manage. Trustwave Hybrid SIEM and Co-Managed SOC enables organizations to overcome these challenges by taking on management of the SIEM solution and providing 24x7 monitoring of alerts. Customers can log in to the SIEM anytime for additional analysis and reporting while day-to-day management and monitoring is handled by Trustwave.

With Trustwave MTD with Hybrid SIEM or Co-Managed SOC, you get the all the benefits of 24x7 security monitoring from Trustwave with the capabilities of an on-site SIEM.

Hybrid SIEM

Trustwave MTD with Hybrid SIEM is an option for organizations that want 24x7 security monitoring and their own Trustwave SIEM. Trustwave provides management of the SIEM, which can be deployed as a physical or virtual appliance or in popular cloud infrastructure providers like Amazon Web Services (AWS) or Microsoft Azure. Management includes regular tasks like monitoring for availability, applying patches, and updating or replacing hardware if needed. Offloading this day-to-day effort to Trustwave lets security professionals at the customer site focus on other important items while knowing regular care of the SIEM is taking place.

There are different reasons why organizations would want an on-site Trustwave SIEM. For example, organizations with unique data retention requirements such as having a local data retention requirement or wanting to archive data for longer periods of time than offered in the standard Trustwave MTD service. Organizations that want to create unique SIEM rules or reports should also look at a Hybrid SIEM option.

Co-Managed SOC

Trustwave MTD with Co-Managed SOC is like Hybrid SIEM, where an organization using this service gets 24x7 security monitoring and an on-site SIEM that's managed by Trustwave. A key difference is the SIEM can be the Trustwave SIEM or a SIEM solution from another provider and is integrated with the organization's SOC, security team, and internal processes. Organizations with an existing SOC and security team might leverage Co-Managed SOC so they can partner with Trustwave and improve their security maturity.

An organization not getting value from an existing SIEM solution should consider this service. Partnering with Trustwave can augment their existing SOC and SIEM investment while at the same time offering a roadmap and plan to increase security maturity.

What Do You Need To Achieve?

Trustwave Managed Threat Detection (MTD) service helps organizations of all sizes monitor for and detect threats 24x7. The Hybrid SIEM and Co-Managed SOC options give organizations the same security monitoring while also augmenting current tools and expertise.

Complementary Services

Trustwave Managed Threat Detection is one of several services Trustwave offers for managed detection and response. Others include:

- **Trustwave Managed Detection and Response (MDR) for Endpoints** Trustwave Managed Detection & Response (MDR) for Endpoints combines people, process and technology to identify and respond to endpoint attacks. It's a comprehensive service that delivers 24x7 monitoring and notification, incident response and remediation, as well as, when needed, proactive threat hunting.
- **Trustwave Digital Forensics and Incident Response (DFIR) consulting** For organizations that have been the victim of a security breach, Trustwave DFIR consulting services can help quickly determine the source, cause and extent of the breach. In addition, proactive IR services can help organizations solidify their security posture against advanced threats.

Trustwave®

For more information: www.trustwave.com