Trustwave®

DATA SHEET

Trustwave Threat Detection Essential

SECURITY MONITORING FROM TRUSTWAVE EXPERTS

Benefits

- Increased threat visibility
- Earlier breach detection
- Global threat intelligence
- SpiderLabs expertise

Security professionals today are challenged to keep up with the rapid growth of security threats. Despite organizations spending significantly on security protection, breaches continue to occur. Professionals want to focus more on threat detection and investigation but often these activities get delayed or sidetracked by competing priorities.

The Trustwave Threat Detection Essential service is designed to help security professionals monitor for and detect threats on a regular basis. Trustwave collects data from logs, events, and other sources and securely sends it to the Trustwave cloud. There, events are automatically analyzed to identify threats. At least once a day, an analyst in one of the Trustwave Advanced Security Operations Centers (ASOCs) will review events and findings. If issues are identified, new incidents are created and the customer notified so triage and response may begin. At any time, subscribers to the service can log in to the Trustwave TrustKeeper portal to view and report on their own data as they see fit.

What You Get

Visibility. The Threat Detection Essential service starts by collecting logs, events, metrics, reports and other outputs from sources in the environment. This can include traditional security products like IDS, firewalls, anti-virus as well as advanced security like endpoint protection and next-gen firewalls. It also includes operating system logs, database audits, proxies and vulnerability reports. And as more organizations move into virtualization and the cloud, hypervisor logs, public cloud service APIs and Cloud Access Security Brokers (CASBs).

Data Acquisition. Log, event and alert data is collected, consolidated, normalized, compressed and securely transported the Trustwave cloud via a small footprint Log Collector Appliance (LCA). Once collected, logs are normalized and metadata tags are applied to tag each record with enrichment data such as geo-location of IPs, and common names for protocols and ports.

Analysis and Threat Detection. All collected events are processed by the Trustwave cloud analysis engine to find known threats, anomalous behavior and suspicious activity. Processing includes stream, batch, and user behavior analytics as well as cross referencing event data against SpiderLabs Threat Intelligence for Indicators of Compromise and Known Bad Actors. SpiderLabs Threat Intelligence is a curated superset of multiple public and private feeds, maintained by Trustwave SpiderLabs.

In addition to this automated analysis, at least once a day a security analyst in one of the Trustwave worldwide ASOCs will review events. If ongoing or otherwise serious issues are identified, they'll create a new incident and assist, triage, and advise to help customers get incidents resolved.

Data Storage and Access. All raw logs, events, and incidents are securely stored in the Trustwave cloud. Through the Trustwave TrustKeeper portal, you can view and report on your data anytime.

Why Trustwave Threat Detection Essential

- **Security.** Augment your security threat monitoring with people and technology from Trustwave, recognized as a leader in Managed Security Services (MSS).
- **Value.** The Threat Detection Essential service gives you access to enterprise-level threat monitoring technologies and security analysts at an affordable price. The technologies used to collect, process and analyze data are the same as used by other MSS customers, as are the analysts, using the same Trustwave SpiderLabs threat intelligence and research.
- **Flexibility.** Threat Detection Essential is one of several services from Trustwave for monitoring and investigating threats. A customer starting with Threat Detection Essential can move to other services, like the 24x7 Threat Detection Complete or Managed Detection & Response as their security needs increase.

Trustwave Managed Security Services

Threat Detection Essential is part of a comprehensive portfolio of Managed Security Services offered by Trustwave. From small local businesses to large global enterprises, Trustwave works with hundreds of thousands of customers around the world to solve their security and compliance challenges, enhance resources and support, and drive their business forward. Our Security Solutions portfolio is powered by:

- Deep expertise in advanced security technologies
- Threat Intelligence built in to our services
- "Follow the Threat" global Advanced Security Operations Centers
- 24x7x365 support and dedicated security analysts
- Cloud-based TrustKeeper management portal

Visit the Trustwave website to learn about additional services Trustwave offers for security protection, threat monitoring and detection, and response.

ANAB ACCREDITED ISO/IEC 17021 MANAGEMENT SYSTEMS CERTIFICATION BODY

Trustwave® | sure.business