Trustwave®

DATA SHEET

Trustwave Threat Detection Complete

24X7 MONITORING & DETECTION OF ADVANCED THREATS

Benefits

- Increased threat visibility
- Earlier breach detection
- Global threat intelligence
- SpiderLabs expertise
- Optimizing existing solutions

Most organizations deploy a variety of devices and solutions to help secure their IT environment. While these solutions perform important functions on their own, their data sources and event logs are also a rich source of information. Analyzing and correlating this data and event information is a vital, yet often misunderstood, component to early detection of threats. Who is the right (best?) person? What threat intelligence source is used to help analyze the information? How are use cases created, and updated, to reflect not only changes in the environment but also new attack techniques? Security professionals recognize the importance of analysis and correlation, but have lessons learned from failed SIEM implementations and need new solutions. Event collection and storage is just the foundation - global threat intelligence combined with expertise and 24x7 analysis are the building blocks for modern threat detection.

Trustwave Threat Detection Complete combines industry leading SpiderLabs Threat Intelligence with SpiderLabs security expertise and a proprietary analysis engine to analyze and correlate events. Collecting data from so many sources increases your security visibility, creating the foundation for detection and response.

Whether stored in the Trustwave cloud, via co-managed hybrid SIEM deployments or direct integration with your existing Security Operations Center (SOC), Threat Detection Complete leverages advanced analytics to identify known bad actors as well as detect anomalous activity. All analytics are performed by SpiderLabs security experts across the Trustwave global Advanced Security Operations Centers (ASOCs). Trustwave Threat Detection Complete up-levels traditional MSSP competencies like device management and log collection, providing the foundation for organizations to consider more proactive security like endpoint detection and response and proactive threat hunting.

Trustwave Threat Detection Complete is a fully integrated service that delivers five distinct elements to detect and investigate attacker activity.

Visibility in the Environment: Visibility is the first step in being able to detect attacker activity. Visibility is provided by collecting logs, events, metrics, reports and other outputs from sources in the environment. This can include traditional security products like IDS, FW, AV and advanced security like endpoint protection and next-gen firewalls. It also includes operating system logs, database audits, proxies and vulnerability reports. And as more enterprises move into virtualization and the cloud, hypervisor logs, Public Cloud Service APIs and Cloud Access Security Brokers.

Trustwave analytics and monitoring capabilities are agnostic. Trustwave will collect all log and event data available to obtain the highest level of visibility into an environment. Trustwave has a dedicated team of experts that ensure support for additional sources can be added as well as continuous evolution as technologies mature.

Acquiring the Data: Log, event and alert data produced in your environment is collected, consolidated, normalized, compressed and securely transported with SSH encryption to the Trustwave network of worldwide ASOCs via the small footprint Log Collector Appliance (LCA). The LCA can be a physical appliance or a virtual image. Processing includes collection via a variety of protocols and methods – syslog, SNMP, SMTP, FTP, SCP, JDBC, WMI, REST API, LEA, FIREPower and SDEE. Once collected, logs are normalized to Trustwave message standard and metadata tags are applied.

This metadata 'tags' each record with enrichment data such as geo-location of IPs, common names for protocols and ports, and Trustwave taxonomy, a human-readable, consolidated grammar for devices' native event and error codes. In developing this vendor-agnostic grammar, Trustwave enables both our analysts and the customer to read and ascertain the nature of events without requiring product-specific knowledge. It also allows all content – rules, learning, analytics, threat hunts and reports to leverage a common taxonomy and operate across all supported sources. Every event and log is tagged with details that associate it to the customer who sent it. This allow every piece of data to be controlled at a detailed level

Analysis and Threat Detection – Automated: All collected events are processed by the Trustwave cloud analysis engine to find known threats, anomalous behavior and suspicious activity. The disposition of data sources in the environment greatly determines the value of the threat detection. Well-positioned, high value sources lead to better threat detection capabilities. This is achieved through multiple layers of processing:

- Cross reference event data points 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. SpiderLabs Threat Intelligence also includes intelligence from our security research, DFIR and Threat Hunt teams
- Stream Analytics using real-time, horizontally-scalable distributed computation systems
- Batch Analytics via distributed processing across clustered systems
- User and Entity Behavior Analytics with use cases, baselines, deviations and anomaly detection
- Machine Learning with distributed learning and centralized prediction via data preprocessing, feature selection, modelling, flow graphs, clustering and classification

Analysis and Threat Detection – Human: The Trustwave ASOCs are organized into customer-centric point of delivery (POD) working groups – analyze and support personnel ordered by industry, nation, threat profile and other group criteria. These PODs provide Threat Triage, Advanced Analysis with containment, SpiderLabs Fusion Intel, threat hunting and reverse engineering. This unique approach allows for deeper analysis, investigation and facilitates response and mitigation. Combined with cutting edge threat hunting techniques, Trustwave Threat Detection Complete can uncover potential threats before they can gain a foothold in your environment and cause damage. A proactive approach like this greatly reduces the amount of time an attacker goes undetected within your network and, as a result, reduces damage.

Unified Data Storage and Access: All raw logs, events, alerts, findings and incidents are stored in our federated multi-tenant data store; a distributed, big data storage platform, supporting tens to hundreds of billions of records per day. Your data is accessible from this storage system via TrustKeeper, the integrated Trustwave portal, providing a single pane of glass to appraise your security posture, communicate with our ASOC as threats are discovered and remediated, and to view and report on your data as you see fit.

ANAB ACCREDITED ISO/IEC 17021 MANAGEMENT SYSTEMS CERTIFICATION BODY

Trustwave® | sure.business

For more information: www.trustwave.com

MTD-0519