Trustwave®

DATA SHEET

Data Source Ingestion Value

March 2024

This document helps you to understand how Trustwave categorizes and ranks data sources based on their threat detection and response (TDR) value, fidelity, and utility. You will learn how Fusion operates as a security operations platform and as an analytics and correlation engine. In the **Supported Data Sources** table, you will review which supported data sources we support, their TDR value, and how we ingest them into Fusion. In **Definitions**, you can read the explanation for security terms that we used in this document.

Trustwave Fusion overview

Trustwave Fusion is a cloud-native security operations platform that serves as the primary interface for our services. Security analysts and our clients use it to:

- Review logs and findings.
- Analyze potential threats.
- Drive operational workflow associated with the incident handling process.

Fusion can operate differently depending on which services clients purchase. That can affect both the data ingested into the platform and the type of analysis it may perform against these data types.

Fusion as a security operations platform

In the *managed detection and response (MDR)* service and the *Co-Managed SOC/SIEM service*, most of the threat detection logic resides within the EDR or SIEM application. These technologies send their output to Fusion and then this data goes through systematic processing which includes:

- Normalization
- Correlation
- AI and ML processing
- Application of high-fidelity SpiderLabs Fusion *use cases*
- Intelligence enrichment
- Subsequent presentation to Trustwave analysts for real-time monitoring and response (where applicable).

Fusion provides Trustwave analysts with a threat-centric interface that streamlines analyst activities. Fusion also supports timely and consistent handling of threat findings.

For MDR services, a combination of EDR **logs and alerts** will be sent into the Fusion platform and processed against Fusion use cases. The resulting *high-fidelity* alerts will then follow the systematic data processing steps.

For Co-Managed SOC / SIEM services, only the **alerts** will go into the Fusion platform. This reduces the amount of redundant data sent into Fusion, saving on client bandwidth and duplicate storage costs. Only the most high-fidelity data is sent to our SOC for active monitoring. If SOC requires additional context, analysts use API enrichment tools to reach back into the SIEM. They may also go directly from Fusion into the SIEM for additional insight.

Fusion as an analytics and correlation engine

In the *threat monitoring service* (formerly *managed threat detection (MTD)*), Fusion operates as an analytics and correlation engine utilizing Trustwave cyber threat intelligence. Fusion presents SOC analysts with alerts generated from specific data sources known for supporting strong threat detection outcomes. While this functionality might sound like an SIEM application, Fusion is not an SIEM.

SIEM tools focus on more than threat detection. They also emphasize compliance, policy management, and even health and availability monitoring. Such tools require a broad data ingestion capability and client context to manage specific organizational risks. The design paradigm for SIEM tools is typically that of “more data is better.”

Since Fusion is a shared platform primarily focused on threat detection for a broad global client base, the design paradigm for Fusion is more aptly stated as “the right data is better.” To this end, Trustwave retains sole discretion in determining the global conditions of the use case catalog. The platform imports a limited number of high-fidelity data sources to improve the outcomes of threat detection. *Lower fidelity* data types are included because they may provide context for deeper investigations. Custom or client-specific use cases **are not** created in the Fusion platform.

Not all data sources are considered equal from a threat detection point of view. Trustwave has established a set of criteria that helps to classify what is the threat detection value of specific data sources and to explain how those data sources will be used after ingestion into the Fusion platform.

Threat Detection and Response Tiers Defined

To provide optimal threat detection and response for all our clients, Trustwave is constantly reviewing supported data sources and their corresponding promotion rules. Trustwave has developed a tiering system as a guide to distinguish categories of data sources. Data sources are ranked by their threat detection utility and their ability to integrate with Fusion.

Tier	Alert Class	Definition
A	High Fidelity	Third-party tools managed by Trustwave such as SIEMs, EDRs, XDR, finished cloud alerts, or enriched alerts with integrated SOAR response actions - these data sources are selected by Trustwave for being industry leaders. Trustwave is committed to the continued development of use cases for these data sources. Clients can expect that these data sources will produce high-fidelity findings that provide significant security utility.
B	Medium-High Fidelity	These data sources produce lower fidelity findings, and the logs aren't as rich as Tier A data sources. However, they bring valuable threat indicators and are used within a larger threat investigation context. Additionally, logs from these data sources could be considered noisy.
C	Compliance/Threat Context	These data sources typically don't have rules written against them and are ingested for compliance reasons. However, they may trigger findings when combined with threat intelligence and they can be referenced within an ongoing threat investigation.
D	Low/No-Fidelity	Unsupported

Supported data sources

In the table, you will see Fusion-supported data sources with their TDR value and acquisition method. Some data sources can be ingested using various methods (API, Syslog, Flatfile, DBreader).

In the **Content Available** column, you can check whether specific data sources have Fusion use cases written for them. To learn more about the concept of the Fusion use cases, refer to the *Fusion use cases reference sheet*.

Vendor	Device	Device ID	TDR Value	Acquisition	Content Available
Amazon.com	AWS GuardDuty	1001	A	API	✓
Cisco Systems	Snort	25	A	Syslog	✓
CrowdStrike	CrowdStrike Falcon	1015	A	API	✓
Google	Google Cloud Security Command Center	1078	A	API	
IBM Corporation	IBM Security QRadar	860	A	Syslog/API	✓
LogRhythm	LogRhythm SIEM Platform	935	A	API/Flatfile	✓
Microsoft Corporation	Microsoft Entra ID Protection (formerly Azure AD Identity Protection)	1058	A	API	✓

Vendor	Device	Device ID	TDR Value	Acquisition	Content Available
Microsoft Corporation	Microsoft Entra ID Sign-in logs (formerly Azure AD sign-in Logs)	1059	A	API	
Microsoft Corporation	Microsoft Defender for Identity	1062	A	API	✓
Microsoft Corporation	Microsoft Defender for Cloud	1063	A	API	✓
Microsoft Corporation	Microsoft Defender for Cloud Apps	1056	A	API	✓
Microsoft Corporation	Microsoft Office 365 Security and Compliance	1064	A	API	✓
Microsoft Corporation	Microsoft Defender for Endpoint	1032	A	API	✓
Microsoft Corporation	Microsoft Sentinel	990	A	API	✓
Netskope	Netskope Next-Gen Secure Web Gateway (SWG)	851	A	API	✓
Palo Alto Networks	Prisma Cloud Workload Protection	1075	A	API	
Palo Alto Networks	Palo Alto Cortex XDR	964	A	API	✓
SentinelOne	SentinelOne Singularity Complete	1039	A	Syslog/API	✓
Splunk	Splunk Enterprise Security	730	A	Syslog/API	✓
Trustwave	Trustwave IDPS (Traffic Sensor VM)	25	A	Syslog	✓
Trustwave	Trustwave DbProtect	719	A	Syslog	
Trustwave	Trustwave MailMarshal	798	A	Syslog	
VMware	VMware Carbon Black EDR (formerly CB Response)	821	A	API	✓

Vendor	Device	Device ID	TDR Value	Acquisition	Content Available
VMware	VMware Carbon Black Endpoint (formerly CB Defense)	884	A	API	✓
VMware	VMware Carbon Black App Control (formerly CB Protection)	659	A	Syslog	
Amazon.com	Amazon AWS CloudTrail	754	B	API	✓
Amazon.com	Amazon AWS Security Hub	1079	B	Syslog/API	
Amazon.com	Amazon AWS VPC Flow	1080	B	Syslog/API	
Amazon.com	AWS WAF	1011	B	Syslog/API	✓
Barracuda	Barracuda CloudGen Firewall	1060	B	Syslog	
Barracuda	Barracuda NG Firewall	939	B	Syslog	✓
Barracuda	Barracuda Spam Firewall	668	B	Syslog	
Barracuda	Barracuda WAF	940	B	Syslog	
Barracuda	Barracuda Web Security and Filtering	352	B	Syslog	
BeyondTrust	BeyondTrust Privileged Access Management (PAM) via S3	1082	B	API	
BlackBerry	Cylance Protect	804	B	Syslog	✓
Check Point	Check Point Firewall	5	B	Syslog	✓
Check Point	Checkpoint Unified Threat Management	690	B	Syslog	
Cisco Systems	Cisco ASA	6	B	Syslog	✓
Cisco Systems	Cisco Secure Endpoint (formerly AMP for Endpoints)	841	B	API	
Cisco Systems	Firepower Secure IPS	157	B	Syslog	✓
Cisco Systems	Cisco Meraki MX	772	B	API	
Citrix	Citrix ADC/NetScaler	496	B	Syslog	
CyberArk	CyberArk PTA	1038	B	Syslog	✓

Vendor	Device	Device ID	TDR Value	Acquisition	Content Available
Darktrace	Darktrace Enterprise Immune System	986	B	Syslog	✓
FireEye	FireEye Helix	1031	B	API	✓
FireEye	FireEye MPS	553	B	Syslog	✓
Forcepoint	Forcepoint Cloud Security	1041	B	API	✓
Forcepoint	Forcepoint Sidewinder	845	B	Syslog	
Forcepoint	Forcepoint Web Security	735	B	Syslog	✓
Fortinet	FortiGate NGFW	262	B	Syslog	✓
Google	Google Alert Center	1054	B	API	
Google	Google Cloud Audit Logs	1053	B	API	
IBM Corporation	IBM AIX Operating System	245	B	Syslog	✓
IBM Corporation	Red Hat Enterprise Linux	245	B	Syslog	✓
Imperva	Imperva Application Security (formerly Incapsula)	810	B	Syslog	
Imperva	Imperva SecureSphere	507	B	Syslog	✓
Imperva	Imperva WAF	1071	B	API	
Trellix	Trellix ePolicy Orchestrator (ePO) (formerly Endpoint Security AV (ePO))	1	B	DB reader	✓
McAfee	McAfee Network Security Platform	118	B	Syslog	
Microsoft Corporation	Microsoft Azure Firewall	1073	B	API	
Microsoft Corporation	Microsoft Azure WAF	1049	B	API	
Microsoft Corporation	Microsoft Defender for IoT	1072	B	Syslog	
Microsoft Corporation	Microsoft Azure Activity	867	B	API	

Vendor	Device	Device ID	TDR Value	Acquisition	Content Available
Microsoft Corporation	Microsoft Entra ID Audit	1057	B	API	
Microsoft Corporation	Microsoft Graph	918	B	API	✓
Microsoft Corporation	Microsoft Graph - Azure AD Identity Protection (IPC)	918	B	API	✓
Microsoft Corporation	Microsoft Graph - Defender for Identity	918	B	API	✓
Microsoft Corporation	Microsoft Graph – Defender for Cloud Apps	918	B	API	✓
Microsoft Corporation	Microsoft Graph – Defender for Cloud	918	B	API	✓
Microsoft Corporation	Microsoft Intune	943	B	API	
Microsoft Corporation	Office 365 Audit	873	B	API	✓
Microsoft Corporation	Microsoft Windows	136	B	Syslog	✓
Microsoft Corporation	Microsoft Windows Defender	899	B	Syslog	
Open-Source Software	Netfilter IPTables	305	B	Syslog	
Open-Source Software	Suricata	736	B	Syslog	
Oracle	Oracle Cloud Guard	1067	B	API	
Oracle	Oracle Cloud Infrastructure Audit	1068	B	API	
Oracle	Oracle Cloud WAF via API	1069	B	API	
Palo Alto Networks	Palo Alto Prisma Cloud	961	B	API	

Vendor	Device	Device ID	TDR Value	Acquisition	Content Available
Palo Alto Networks	Palo Alto Networks Next-Generation Firewall	464	B	Syslog	✓
Sophos	Sophos Central	908	B	Syslog/API	
Sophos	Sophos Unified Threat Management (UTM)	701	B	Syslog	
Symantec	Symantec Endpoint Security	460	B	Syslog	
Tessian	Tessian Cloud Email Security	1066	B	API	
Trend Micro	Control Manager/Apex One	35	B	Syslog/API	✓
Trend Micro	TippingPoint IPS	43	B	Syslog	
Trend Micro	Trend Micro Deep Security	311	B	Syslog	
Trend Micro	Trend Micro XDR	1074	B	Syslog/API	✓
Trend Micro	TrendMicro IWSVA	1065	B	Syslog	
Zscaler	Zscaler NSS	771	B	Syslog	✓
Zscaler	Zscaler ZPA	1070	B	Syslog	
A10 Networks	A10 Networks EX Series	721	C	Syslog	
A10 Networks	A10 Networks Thunder CFW Series	1019	C	Syslog	
Aerohive Networks	Aerohive Access Point (AP)	888	C	Syslog	
Akamai	Akamai Cloud Security	1036	C	API	
Amazon.com	Amazon CloudWatch	946	C	API	
Amazon.com	Amazon SSM Agent	988	C	Syslog	
Apache Foundation	Apache HTTP Server	156	C	Syslog	✓
Apple	Apple Mac OS X	560	C	Syslog	
Arista	Arista Switch	936	C	Syslog	
Aruba	Aruba ClearPass	734	C	Syslog	

Vendor	Device	Device ID	TDR Value	Acquisition	Content Available
Aruba	Aruba Wireless Switch	293	C	Syslog	
Avaya	Avaya Ethernet Routing Switch	645	C	Syslog	
Avaya	Avaya Secure Router	598	C	Syslog	
Avocent	Avocent KVM	877	C	Syslog	
Barracuda	Barracuda Email Security Gateway	1055	C	Syslog	
Barracuda	Barracuda SSL VPN	657	C	Syslog	
BeyondTrust	BeyondTrust PowerBroker Server	578	C	Syslog	
BeyondTrust	Secure Remote Support (formerly Bomgar Remote Support)	820	C	Syslog	
Bitglass	Bitglass	852	C	API	
BlackBox	BlackBox IP Camera	887	C	Syslog	
Cisco Systems	Cisco IOS/Catalyst/AP/WAAS	34	C	Syslog	✓
Cisco Systems	Cisco IronPort	126	C	Syslog/Flatfile	
Cisco Systems	Cisco IronPort SMA	720	C	Syslog	
Cisco Systems	Cisco Ironport Web Proxy	483	C	Syslog	
Cisco Systems	Cisco ISE	704	C	Syslog	
Cisco Systems	Cisco NAC	623	C	Syslog	
Cisco Systems	Cisco Secure ACS Windows/Unix	92	C	Syslog	
Cisco Systems	Cisco Umbrella	1024	C	API	
Citrix	Citrix XenApp	649	C	Syslog	
Clavister	Clavister CorePlus	634	C	Syslog	
Cloudera	Cloudera Manager	896	C	Syslog	
Cloudflare	Cloudflare WAF	1051	C	API	

Vendor	Device	Device ID	TDR Value	Acquisition	Content Available
CredibanCo	Credibanco SIA/SAT	980	C	Flatfile	
Cybera	Cybera Edge Appliance	926	C	Syslog	
CyberArk	CyberArk Password Vault	498	C	Syslog	✓
Draytek	Draytek Vigor	767	C	Syslog	
Duo Security, Inc.	Duo Security	814	C	API	
Eclipse	mosquitto	1012	C	Syslog	
EdgeWave	EdgeWave iPrism	706	C	Syslog	
Epicor	Epicor Eagle OS	865	C	Syslog	
Ericsson	Ericsson SGSN-MME	909	C	Syslog	
Ericsson	Ericsson TSS	874	C	Syslog	
Extreme Networks	ExtremeXOS	786	C	Syslog	
F5 Networks	F5 BIG-IP	258	C	Syslog	
F5 Networks	F5 BIG-IP ASM	540	C	Syslog	
F5 Networks	F5 BIG-IP Global Traffic Manager	279	C	Syslog	
ForeScout Technologies	ForeScout CounterACT	229	C	Syslog	
Fortinet	FortiWeb	751	C	Syslog	
H3C	H3C S5120-SI Series Switch	947	C	Syslog	
Hewlett-Packard Devel. Comp.	HP OpenVMS	350	C	Syslog	
Hewlett-Packard Devel. Comp.	HP Security Voltage	868	C	Syslog	
Hewlett-Packard Devel. Comp.	HP-UX Audit	114	C	Syslog	

Vendor	Device	Device ID	TDR Value	Acquisition	Content Available
Hewlett-Packard Devel. Comp.	Nimble Storage	892	C	Syslog	
Hitachi Data Systems	Hitachi Unified Storage	750	C	Syslog	
Hitec Laboratories	Hitec Laboratories DataStore32	679	C	Syslog	
Huawei	Huawei Eudemon	1005	C	Syslog	
Huawei	Huawei Firewall	883	C	Syslog	
Huawei	Huawei NMS	886	C	Syslog	
Huawei	Huawei Router	906	C	Syslog	
Huawei	Huawei SDH	895	C	Syslog	
Huawei	Huawei Switch	819	C	Syslog	
IBM Corporation	IBM AIX	27	C	Syslog	
IBM Corporation	IBM iSeries	487	C	Syslog	
IBM Corporation	IBM Mantra	620	C	Syslog	
IRONSCALES LTD	IronTraps	992	C	Syslog	
Isilon Systems	OneFS	1009	C	Syslog	
Juniper Networks	Juniper NetScreen/ISG/SSG	12	C	Syslog	
Juniper Networks	Juniper Networks Junos	125	C	Syslog	
Juniper Networks	Juniper SSL VPN	11	C	Syslog	
KEMP Technologies	KEMP LoadMaster	871	C	Syslog	
Lancope	Lancope StealthWatch	61	C	Syslog	
Main Street Softworks	Monetra	863	C	Syslog	

Vendor	Device	Device ID	TDR Value	Acquisition	Content Available
ManageEngine	ADAudit Plus	1021	C	Syslog	
ManageEngine	Password Manager Pro	904	C	Syslog	
McAfee	McAfee DLP	1033	C	Syslog	
McAfee	McAfee Email Gateway	130	C	Syslog	
McAfee	Mcafee SMG via Syslog	469	C	Syslog	
McAfee	McAfee Solidifier	703	C	Syslog	
McAfee	McAfee Web Gateway	525	C	Syslog	
Micro Focus	SUSE - Generic Unix Syslog	245	C	Syslog	✓
Microsoft Corporation	Microsoft IIS	40	C	Syslog/API	
Microsoft Corporation	Microsoft IIS HTTP/FTP	927	C	Flatfile	
Microsoft Corporation	Microsoft Network Policy Server	779	C	Syslog	
Microsoft Corporation	Microsoft Sharepoint	708	C	Syslog	
Microsoft Corporation	Microsoft UAG	707	C	Syslog	
Microsoft Corporation	Ubuntu - Generic Unix Syslog	245	C	Syslog	✓
Motorola	Motorola WS2000	574	C	Syslog	
Nagios	Nagios via Syslog	267	C	Syslog	
NetApp Appliance Inc.	NetApp Storage	316	C	Syslog	
NetScout	Arbor Sightline (formerly Peakflow SP)	314	C	Syslog	
Network Box	Network Box UTM	805	C	Syslog	
NIB Bank	NIB Mobile/Ambit	866	C	Syslog	

Vendor	Device	Device ID	TDR Value	Acquisition	Content Available
Nginx Inc.	Nginx HTTP Server	815	C	Syslog	
Nokia	Nokia ESS	890	C	Syslog	
Nokia	Nokia PSS	880	C	Syslog	
Odoo S.A.	Odoo/OpenERP	932	C	Syslog	
Okta	Okta	891	C	API	
Open Source Software	Fedora - Generic Unix Syslog	245	C	Syslog	✓
Open Source Software	Generic DHCPD	503	C	Syslog	
Open Source Software	Generic Syslog	9999	C	Syslog	
Open Source Software	ISC BIND	187	C	Syslog	
Open Source Software	Puppet Agent	776	C	Syslog	
Open Source Software	Red Hat Audit	431	C	Syslog	
Open Source Software	Samba	555	C	Syslog	
Open Source Software	Sendmail/SpamAssassin	237	C	Syslog	
Open Source Software	Squid Proxy	33	C	Syslog	
Open Source Software	strongSwan	950	C	Syslog	
Open Source Software	Varnish Cache	928	C	Syslog	
Oracle	Sun Directory Server	234	C	Syslog	
Oracle	Sun Solaris BSM Audit	30	C	Syslog	

Vendor	Device	Device ID	TDR Value	Acquisition	Content Available
PGP	PGP Universal Server	506	C	Syslog	
ProofPoint	Proofpoint TAP	1052	C	API	
Pulse Secure	Pulse Connect Secure	945	C	Syslog	
Quanta Computing	Quanta	930	C	Syslog	
Rapid7	Rapid7 InsightIDR	1027	C	Syslog	
Raritan	Raritan PX PDU	879	C	Syslog	
Riverbed Technology	Riverbed RiOS	737	C	Syslog	
RSA Security	RSA Authentication Manager	473	C	Syslog	
RSA Security	RSA SecurID	0	C	Syslog	
SalesForce	SalesForce	869	C	API	
Sangfor	Sangfor NGAF	960	C	Syslog	
SAP	SAP Access Log	799	C	Syslog	
SEL Inc.	SEL RTAC	917	C	Syslog	
SolarWinds	SolarWinds Network Performance Monitor	985	C	Syslog	
SonicWALL	SonicWALL Aventail	455	C	Syslog	
SonicWALL	SonicWALL SonicOS	345	C	Syslog	
Sophos	Sophos Anti-virus	64	C	Syslog	
Sophos	Sophos Cyberoam UTM Firewall	759	C	Syslog	
Sophos	Sophos Email	562	C	Syslog	
Sophos	Sophos Enterprise Console	924	C	Flatfile	
Sophos	Sophos Secure Web Gateway	755	C	Syslog	
Sophos	Sophos XG Firewall	937	C	Syslog	

Vendor	Device	Device ID	TDR Value	Acquisition	Content Available
Spectracom Corp.	SecureSync	876	C	Syslog	
Symantec	Blue Coat SG	71	C	Syslog/Flatfile	
Symantec	Symantec Brightmail via EM	466	C	Syslog	
Symantec	Symantec Data Center Security	1037	C	Syslog	
Symantec	Symantec Endpoint Protection	1043	C	API	
Symantec	Symantec VIP	850	C	Syslog	
Thycotic	Thycotic SecretServer	640	C	Syslog	
Trend Micro	Cloud Integrity	1047	C	API	
Trend Micro	Deep Discovery Inspector	800	C	Syslog	
Trend Micro	Generic OSSEC Audit	732	C	Syslog	
Trend Micro	Trend Micro IWSS	546	C	Syslog	
Trend Micro	TrendMicro Deep Discovery Analyzer	902	C	Syslog	
Trustwave	Mod Security	513	C	Syslog	
Trustwave	Trustwave Jumpbox	941	C	Syslog	
Trustwave	Trustwave TrustOS	594	C	Syslog	
VeriFone	VeriFone POS	576	C	Syslog	
VMware	VMware ESX	420	C	Syslog	
VMware	VMware PSC	938	C	Syslog	
VMware	VMware VirtualCenter	856	C	Syslog	
WatchGuard Technologies	WatchGuard BorderWare Firewall	516	C	Syslog	
WatchGuard Technologies	WatchGuard Firebox	346	C	Syslog	
Xura	Mavenir BT Application	872	C	Syslog	

Data Sources ingested by Fusion for the MDR service

In the table below you see which data sources are included with the **MDR Service** bundle and have the unlimited Ingestion of high-fidelity alerts and data sources that are ingested for high-fidelity alerts and will count towards the events per day (EPD).

Vendor	Device	Ingestion limit
VMware	VMware Carbon Black EDR (formerly CB Response)	Unlimited
CrowdStrike	CrowdStrike Falcon	Unlimited
Microsoft Corporation	Microsoft Defender for Endpoint	Unlimited
Palo Alto Networks	Palo Alto Cortex XDR	Unlimited
SentinelOne	SentinelOne Singularity Complete	Unlimited
Amazon.com	AWS GuardDuty	EPD
Microsoft Corporation	Microsoft Entra ID Protection (formerly Azure AD Identity Protection)	EPD
Microsoft Corporation	Microsoft Entra ID Sign-in logs (formerly Azure AD Sign-In logs)	EPD
Microsoft Corporation	Microsoft Defender for Identity	EPD
Microsoft Corporation	Microsoft Defender for Cloud (formerly Azure Security Center)	EPD
Microsoft Corporation	Microsoft Defender for Cloud Apps (formerly Cloud Apps Security)	EPD
Microsoft Corporation	Microsoft Azure AD Audit Logs	EPD
Microsoft Corporation	Microsoft Graph	EPD
Microsoft Corporation	Microsoft Graph – Defender for Identity	EPD

Vendor	Device	Ingestion limit
Microsoft Corporation	Microsoft Graph – Defender for Cloud Apps	EPD
Microsoft Corporation	Microsoft Graph – Defender for Cloud	EPD
Microsoft Corporation	Microsoft Graph – Azure AD Identity Protection (IPC)	EPD
Microsoft Corporation	Office 365 Audit	EPD

All other data sources can be ingested with the **MDR Elite service** and will count towards the events per day (EPD).
No additional data sources can be ingested with the MDR service.

Definitions

Co-Managed SOC / SIEM Service: A Trustwave delivered service that provides shared management of a supported client premise or cloud-based SIEM application that receives logs and events from a variety of client data sources and that contains the relevant use-case logic to generate alerts. Alerts from the SIEM platform are sent into Trustwave Fusion to be processed by Trustwave Security Analysts.

Fusion: Trustwave Fusion is a cloud-native Security Operations Platform that serves as the primary interface for our services. It is used by both our Security Analysts as well as our clients to review logs and findings, analyze potential threats, and drive operational workflow associated with the incident handling process.

High-Fidelity: References the utility of a given data source and the high likelihood that this source will allow either Fusion or our Security Analysts to identify the presence of a verifiable security incident.

Low-Fidelity: References the utility of a given data source and the low likelihood that this source will allow either Fusion or our Security Analysts to identify the presence of a verifiable security incident.

Managed Detection and Response Service (MDR): A threat detection and response service designed around the management and monitoring of supported Endpoint Detection and Response (EDR) applications. Alerts and logs from the EDR application are sent into Trustwave Fusion to be processed by Security Analysts.

MDR Elite: A threat detection and response service bundle that includes everything from the standard MDR service with additional features added on. For details, please see the service description.

Threat Monitoring Service or Managed Threat Detection Service (MTD): A threat detection service that collects logs and events from high-fidelity security-centric data sources for processing within the Trustwave Fusion platform and subsequent analysis and escalation by Fusion Machine Learning algorithms or Trustwave Security Analysts.

Use Case: The programmed logic within a SIEM platform or Trustwave Fusion that is designed to analyze ingested data for specific threat conditions aligned to common standards such as the Mitre Attack Framework, NIST, Kill Chain, and Trustwave standards.

About Trustwave

Trustwave is a globally recognized cybersecurity leader that reduces cyber risk and fortifies organizations against disruptive and damaging cyber threats.

Trustwave's comprehensive offensive and defensive cybersecurity portfolio detects what others cannot, responds with greater speed and effectiveness, optimizes its client's cyber investment, and improves security resilience. Trusted by thousands of organizations worldwide, Trustwave leverages its world-class team of security consultants, threat hunters, and researchers, and its market-leading security operations platform to decrease the likelihood of attacks and minimize potential impact.

Trustwave is an analyst-recognized leader in managed detection and response (MDR), managed security services (MSS), cyber advisory, penetration testing, database security, and email security. The elite Trustwave SpiderLabs team provides industry-defining threat research, intelligence, and threat hunting, all of which are infused into Trustwave services and products to fortify cyber resilience in the age of inevitable cyber-attacks.

For more information about Trustwave, please visit https://www.trustwave.com.

Revision History

Version	Date	Changes

5.3	03/26/24	• Content and style improvements
		• Added the following data sources to the supported data sources list:
		  • Microsoft Intune
		  • Google Cloud Security Command Center
		  • Microsoft Azure Firewall
		  • Akamai Cloud Security
		  • Cisco Meraki MX
		  • Cisco Secure Endpoint (formerly AMP for Endpoints)
		  • Imperva WAF
		  • Microsoft Azure WAF
		  • Oracle Cloud Infrastructure Audit
		  • Oracle Cloud Guard
		  • Oracle Cloud WAF
		  • Trend Micro Cloud Integrity

5.2	02/05/24	• Reviewed and updated tiers for these data sources:
		  • Microsoft Entra ID Sign-in logs
		  • Snort
		  • VMware Carbon Black App Control (formerly CB protection)
		• Removed the following data sources:
		  • Cybereason Defense Platform (EDR)
		  • Trellix Endpoint Security (HX)
		• Updated the **About Trustwave**
		• Content and style improvements

5.1	01/12/24	• Updated the name of the list to **Supported Data Sources**
		• Removed the following data sources:
		  • Google Cloud Security Command Center
		  • Microsoft Intune
		  • Microsoft Azure Firewall
		  • Akamai Cloud Security
		  • Cisco Meraki MX
		  • Cisco Secure Endpoint (formerly AMP for Endpoints)
		  • Imperva WAF
		  • Microsoft Azure WAF
		  • Oracle Cloud Infrastructure Audit
		  • Oracle Cloud Guard
		  • Oracle Cloud WAF
		  • Trend Micro Cloud Integrity

Version	Date	Changes

5.0	12/21/23	• Content and style improvements
		• Updated acquisition methods for these devices:
		  • Cybereason EDR
		  • IBM Security QRadar
		  • Carbon Black EDR
		  • Carbon Black Endpoint
		  • BeyondTrust PAM via S3
		  • Microsoft Defender for IoT
		  • Trend Micro Control Manager/Apex One
		• Removed multiple data sources from the list as they have been deprecated (mostly Tier C data sources) and a few Tier B data sources:
		  • McAfee MVISION
		  • Mimecast Email Security
		  • pfSense Firewall
		  • Trustwave WebMarshal

4.9	10/19/23	• Review and update • Updated the names of the devices to reflect the current product naming used by vendors
4.8	07/28/23	• Review and update • Added **BeyondTrust PAM via S3** to the data sources list
4.7	07/10/23	• Review and update • Minor graphical and text fixes
4.6	05/15/23	• Review and update • Temporarily removed Microsoft 365 Defender from the **Data sources currently supported**
4.5	04/21/23	• Reviewed and updated the **Data sources ingested by Fusion for the MDR service** • Corrected a few graphical and text errors
4.4	03/21/23	• Reviewed and improved the **Content available** column • Upgraded **Trend Micro Control Manager** from Tier C to Tier B • Inverted the **Revision History** to show the latest versions at the top
4.3	03/01/23	• Added **Content available** column • Added quick introduction about the content and analytical rules in the **Data sources currently supported** section • Added **Trellix Endpoint Security (HX)** to the data sources list
4.2	01/20/23	• Minor graphical fixes, page numbering corrected

Version	Date	Changes
4.1	12/20/22	• Review and update • Added **AWS Security Hub, AWS VPC Flow,** and **Google Cloud Security Command Center** to Tier B value data sources
4.0	10/28/22	• Review and update • Modified introduction • Added **Trustwave Fusion Overview** and the **Definitions** sections • Added data sources in the **Data sources ingestion by Fusion** section into the table instead of the list • Changed the name of the **List of data sources** to **Data sources currently supported**
3.1	8/17/22	• Sorted items in the table by the Vendor names
3.0	8/9/22	• Review and update • Added the Acquisition column
2.0	6/10/22	• Review and update
1.0	2/15/22	• Initial Release