Trellix XDR Integrations

Introduction to XDR Integrations

Trellix XDR offers over 450 integrations for its cloud console, and when combined with the Enterprise Service Manager (ESM), it offers an additional 400 integrations, resulting in over 800 unique data ingestions. Additionally, Trellix XDR provides more than 120 integrations for response actions and playbooks, catering to both on-premise and cloud environments.

It's important to understand the capabilities and benefits of XDR integrations for your customers. XDR integrations refer to the ability to integrate third-party applications into your cybersecurity platform for improved security and threat detection capabilities.

Our platform supports up to 1,000 XDR integrations, encompassing both data ingestion and SOAR response actions that can function on-premise or in the cloud. This extensive integration capacity allows our platform to work seamlessly with a wide variety of applications, ensuring that your customers benefit from a more comprehensive and effective cybersecurity solution.

Using Cloud Connect for Easy Data Ingestion

One of the key features of our XDR integrations is the Cloud Connect tool, which enables easy data ingestion. This tool allows third-party SaaS applications to use webhooks, pull and push commands, and authenticate through API connections. As a result, your customers can quickly and easily integrate their existing applications into our platform without requiring complex custom development.

With Cloud Connect, customers can conveniently ingest data from a variety of sources, including endpoint devices, cloud applications, and network infrastructure. Our platform can then analyze this data to identify potential threats and security incidents.

The latest integrations can be obtained from the XDR console under the Cloud Connect menu selection. The below table outlines Trellix Cloud Connect integrations.

Table 1 - Cloud Connection Integrations

Vendor	Product/Service	Format	Category
Akamai	SIEM	Cloud Connect	Cloud Security
Alert Logic	Alert Logic Logs	Cloud Connect	SIEM
Amazon	AWS CloudTrail	Cloud Connect	Cloud Security
Amazon	AWS CloudWatch	Cloud Connect	Cloud Security
Amazon	AWS GuardDuty	Cloud Connect	Cloud Security
Amazon	AWS Route 53 (DNS)	Cloud Connect	Cloud Security
Amazon	AWS Network Firewall	Cloud Connect	Cloud Security
Amazon	Inspector	Cloud Connect	Cloud Security
Amazon	Web Application Firewall (WAF)	Cloud Connect	Cloud Security
Amazon	WorkSpace	Cloud Connect	Cloud Security
Atlassian	Jira	Cloud Connect	Notification
Bitdefender	Bitdefender	Cloud Connect	Endpoint
Bitglass	Bitglass	Cloud Connect	Cloud Access Security Broker (CASB)
Box	Box Events	Cloud Connect	Data Management System
Broadcom	Symantec CASB	Cloud Connect	Cloud Security
Broadcom	Symantec Endpoint Protection Mobile	Cloud Connect	Mobile
Broadcom	Symantec VIP Report	Cloud Connect	Security
Broadcom	Symantec Web Security Service	Cloud Connect	Firewall
Broadcom	Symantec Blue Coat	Cloud Connect	Firewall
Carbon Black	Carbon Black	Cloud Connect	Endpoint
Cato Networks	Cato Networks	Cloud Connect	Web Security
Check Point	Dome9	Cloud Connect	Cloud Computing
Check Point	Check Point Firewall Logs	Cloud Connect	Network Security
CipherCloud	CipherCloud CASB+	Cloud Connect	Cloud Access Security Broker (CASB)
CipherCloud	CipherCloud Logs	Cloud Connect	Security
Cisco	Cisco AMP Events	Cloud Connect	Endpoint

Vendor	Product/Service	Format	Category
Cisco	Meraki	Cloud Connect	Network
Cisco	Cisco Umbrella	Cloud Connect	Security
Cisco	Cisco Umbrella S3	Cloud Connect	Security
Cloudflare	Cloudflare Logs S3	Cloud Connect	Security
Cloudflare	Cloudflare Logs	Cloud Connect	Security
Cofense	Cofense	Cloud Connect	Email & Collaboration
Corelight	Corelight	Cloud Connect	Firewall
CrowdStrike	CrowdStrike FDR	Cloud Connect	Endpoint
CSC Global	CSC Global Domain Manager	Cloud Connect	Cloud Computing
CyberArk	Endpoint Privilege Manager	Cloud Connect	Authentication & Identity Management
Digital Guardian	Digital Guardian Events	Cloud Connect	Data Protection
DocuSign	DocuSign	Cloud Connect	Business
Druva	Druva Logs	Cloud Connect	Data Protection
Duo Security	Duo Auth	Cloud Connect	Authentication & Identity Management
Entrust	Entrust IntelliTrust Events	Cloud Connect	Authentication & Identity Management
Exabeam	Exabeam Alerts	Cloud Connect	Security
Facebook	Meta Workplace	Cloud Connect	Business
FireEye	Malware Analysis (AX)	Cloud Connect	Security
FireEye	FireEye Cloudvisory	Cloud Connect	Security
FireEye	FireEye Detection on Demand for AWS S3	Cloud Connect	Security
FireEye	File Security (FX)	Cloud Connect	Security
FireEye	FireEye Mandiant Validation	Cloud Connect	Security
FireEye	FireEye Messaging Security for Microsoft 365	Cloud Connect	Security
FireEye	FireEye Network Security	Cloud Connect	Security
FireEye	FireEye Detection On Demand for Microsoft SharePoint/OneDrive	Cloud Connect	Security
Forcepoint	Forcepoint Proxy	Cloud Connect	Web Security
Fortinet	FortiProxy	Cloud Connect	Network Security

Vendor	Product/Service	Format	Category
Gigya	Gigya Audit Logs	Cloud Connect	Authentication & Identity Management
Google	Google Cloud	Cloud Connect	Security Information & Event Management (SIEM)
Google	GSuite/Google Cloud Audit Events	Cloud Connect	Authentication & Identity Management
Google	GSuite Admin Logs	Cloud Connect	Authentication & Identity Management
H-ISAC	H-ISAC IOCs	Cloud Connect	Threat Intelligence
Iboss	Iboss secure cloud gateway	Cloud Connect	Cloud Security
Imperva	Imperva Attack Analytics	Cloud Connect	User & Entity Behavior Analytics
Imperva	Incapsula SIEM Integration	Cloud Connect	Security Information & Event Management (SIEM)
Infoblox	Infoblox	Cloud Connect	Network Security
IntSights	IntSights	Cloud Connect	Threat Intelligence
Ivanti	Ivanti	Cloud Connect	Endpoint Security
JFrog	JFrog	Cloud Connect	Application Development
Kentik	Kentik Events	Cloud Connect	Network Security
Lacework	Lacework	Cloud Connect	Cloud Security
LastPass	LastPass	Cloud Connect	Authentication & Identity Management
Lookout	Lookout	Cloud Connect	Endpoint Security
Malwarebytes	Malwarebytes	Cloud Connect	Endpoint Security
McAfee	McAfee ePolicy Orchestrator (ePO)	Cloud Connect	Security
McAfee	MVISION Insights	Cloud Connect	Enrichment
McAfee	McAfee Web Gateway Logs	Cloud Connect	Network Security
McAfee	McAfee MVISION Mobile	Cloud Connect	Endpoint Security
Menlo Security	Menlo Security Isolation Platform (MSIP)	Cloud Connect	Security
Microsoft	Azure Security Auditing	Cloud Connect	Cloud Security
Microsoft	Azure	Cloud Connect	Cloud Computing
Microsoft	Azure AD integration	Cloud Connect	Authentication & Identity Management
Microsoft	Defender	Cloud Connect	Endpoint Security
Microsoft	Microsoft Graph	Cloud Connect	Authentication & Identity Management

Vendor	Product/Service	Format	Category
Microsoft	Microsoft CASB	Cloud Connect	Cloud Access Security Broker (CASB)
Microsoft	Office 365	Cloud Connect	Cloud Computing
Microsoft	Windows Defender ATP	Cloud Connect	Endpoint Security
Mimecast	Mimecast Events	Cloud Connect	Email & Collaboration
Netra	Netra Syslogs	Cloud Connect	Log Management
Netskope	Netskope Events	Cloud Connect	Cloud Security
Okta	Okta Logs	Cloud Connect	Authentication & Identity Management
OnGuard Systems	Interactive Logs	Cloud Connect	Security
Palo Alto Networks	Cortex Data Lake	Cloud Connect	Log Management
Palo Alto Networks	PAN-OS	Cloud Connect	Network Security
Palo Alto Networks	Prisma Cloud	Cloud Connect	Cloud Security
Palo Alto Networks	Palo Alto Firewall Config	Cloud Connect	Network Security
Palo Alto Networks	Palo Alto Prisma Logs	Cloud Connect	Log Management
Palo Alto Networks	Palo Alto System Logs	Cloud Connect	Log Management
Palo Alto Networks	Palo Alto Threats	Cloud Connect	Network Security
Palo Alto Networks	Palo Alto Traffic	Cloud Connect	Network Security
PhishLabs	PhishLabs Incidents	Cloud Connect	Mail
PhishLabs	PhishLabs IOCs	Cloud Connect	Threat Intelligence
Proofpoint	Proofpoint CASB Integration	Cloud Connect	Cloud Access Security Broker (CASB)
Proofpoint	Proofpoint on Demand Logs	Cloud Connect	Mail
Proofpoint	Proofpoint SIEM Integration	Cloud Connect	Security Information & Event Management (SIEM)
Qualys	QualysGuard	Cloud Connect	Vulnerability Management
Qualys	Qualys File Integrity Monitoring	Cloud Connect	Data Protection
RSA	SecurID	Cloud Connect	Authentication & Identity Management
Salesforce	Salesforce Events	Cloud Connect	Business
ServiceNow	ServiceNow	Cloud Connect	IT Asset Management (ITAM)
Signal Sciences	Signal Sciences WAF	Cloud Connect	Web Security

Vendor	Product/Service	Format	Category
Slack	FireEye Message Security for Slack	Cloud Connect	Email & Collaboration
Sophos	Sophos Antivirus SIEM Integration	Cloud Connect	Security Information & Event Management (SIEM)
Squid	Squid Proxy Logs	Cloud Connect	Network Security
TeamViewer	TeamViewer Events	Cloud Connect	Remote Access & Support
Temenos	Infinity	Cloud Connect	Business
Tenable	Tenable	Cloud Connect	Vulnerability Management
Thales	SafeNet	Cloud Connect	Authentication & Identity Management
Thinkst	Canary	Cloud Connect	Security
Trend Micro	Trend Micro Apex Central	Cloud Connect	Security
Trend Micro	Trend Micro Deep Security Manager	Cloud Connect	Security
Trend Micro	Trend Micro Deep Security Agent	Cloud Connect	Endpoint Security
Verizon	Verizon WAF	Cloud Connect	Web Security
Webroot	Webroot	Cloud Connect	Security
Zimperium	Zimperium Logs	Cloud Connect	Mobile
Zscaler	Zscaler Proxy Logs	Cloud Connect	Firewall

On-Premise Connectors for Maximum Flexibility

In addition to Cloud Connect, our platform also offers on-premise connectors for maximum flexibility. These message brokers are called CommBrokers. The CommBroker will allow customers to integrate third-party applications using features such as event forwarding or message brokers. For example, Trellix's CommBroker can be run on a Linux virtual instance to enable integration with our platform.

On-premise connectors are particularly useful for customers who have unique requirements or need to integrate with applications that are not available in the cloud. With our on-premise connectors, customers can integrate any application into our platform, regardless of where it's hosted.

The table below highlights the vendors and services that allow your application's event forwarding feature or Trellix's CommBroker to send data directly into the Trellix XDR Platform.

Table 2 - Cloud Connection Integrations

Vendor	Product/Service	Format	Category
Adtran	NetVanta	Syslog	Network Security
Aerohive	Access Point	Syslog	Network
Akamai	Kona WAF	Syslog	Cloud Security
Alcatel-Lucent	OmniSwitch	Syslog	Network
Alcatel-Lucent	Lucent Firewall	Syslog	Network Security
Apache	Cassandra	Syslog	Database Management System
Apache	HTTP Server	Syslog	Web Server
Apache	ModSecurity	Syslog	Firewall
Apereo Foundation	CAS	Syslog	Authentication & Identity Management
Apple	Mac OS	Syslog	Operating System
Arista	Airtight/Mojo Networks Access Point	Syslog	Network
Aruba	ClearPass	CEF	Network Security
Atlassian	Jira	JSON	Notification
Attivo Networks	BOTsink	CEF	Network
Avaya	Nortel VPN	CEF	Network
AWS	SSM Agent	Syslog	Cloud Security
AWS	CloudFront	Syslog	Cloud Security
AWS	ELB	Syslog	Cloud Security
AWS	S3	Syslog	Cloud Security
AWS	VPC Flow	Syslog	Cloud Security
Barracuda Networks	NextGen Firewall	Syslog	Network Security
Barracuda Networks	SSL VPN	Syslog	Network Security
Barracuda Networks	Web Application Firewall	LEEF	Network Security
Belden	Tofino Xenon	CEF	Firewall
BeyondTrust	BeyondInsight	Syslog	Authentication & Identity Management
Bitglass	Cloud CSAB	Syslog	Cloud Access Security Broker (CASB)

Vendor	Product/Service	Format	Category
Broadcom	Brocade VTM	Syslog	Network
Broadcom	Brocade Vyatta Vrouter	Syslog	Network
Broadcom	Brightmail	Syslog	Mail
Broadcom	Data Center Security (DCS)	Syslog	Security
Broadcom	DLP	Syslog	Data Protection
Broadcom	Endpoint Protection	CEF	Endpoint Security
Broadcom	SDCS:S	Syslog	Security
Broadcom	Server	Syslog	Security
Bromium	vSentry	CEF	Endpoint
Carbon Black	AW	Syslog	Endpoint
Carbon Black	Defense	CEF	Endpoint
Carbon Black	ER	JSON, CEF	Endpoint
Centrify	Centrify Suite	Syslog	Authentication & Identity Management
Check Point	Check Point	CEF	Network Security
Check Point	Firewall	Syslog	Network Security
Check Point	HTTP Proxy	Syslog	Firewall
Check Point	Next Generation Firewall	CEF	Network Security
Check Point	SmartDefense	Syslog	Security
Cisco	ACS	CEF	Authentication & Identity Management
Cisco	ASA	CEF	Network Security
Cisco	ASA CWS	Syslog	Network Security
Cisco	Firepower	Syslog	Network Security
Cisco	Firepower IPS	Syslog	Network Security
Cisco	Firewall	Syslog	Network Security
Cisco	Flow	Syslog	Network Security
Cisco	Firepower Threat Defense	Syslog	Firewall
Cisco	FWSM	Syslog	Firewall

Vendor	Product/Service	Format	Category
Cisco	HSRP	Syslog	Network
Cisco	IDS	Syslog	Firewall
Cisco	IOS	Syslog	Network
Cisco	IPS	Syslog	Firewall
Cisco	IronPort Email	Syslog	Mail
Cisco	IronPort HTTP Proxy	Syslog	Mail
Cisco	IronPort Management	Syslog	Mail
Cisco	ISE	CEF	Authentication & Identity Management
Cisco	Nexus	Syslog	Network
Cisco	PIX	CEF	Network
Cisco	Prime	Syslog	Network
Cisco	Routing Ace	Syslog	Network
Cisco	VCS	Syslog	Email & Collaboration
Cisco	VPN	CEF	Network
Cisco	WLC	Syslog	Network
Cisco	Cloudlock API	LEEF	Cloud Access Security Broker (CASB)
Cisco	DUO Authentication	JSON	Authentication & Identity Management
Cisco	FireSIGHT System Event Streamer (eStreamer)	Syslog	Security
Cisco	Meraki CMS	Syslog	Network
Cisco	NetFlow	CEF	Network
Cisco	OpenDNS	Syslog	Network
Cisco	Sourcefire	Syslog	Network Security
Citrix	IMA	Syslog	Network
Citrix	NetScaler	CEF	Network
ClamAV	AntiVirus	Syslog	Endpoint
Claroty	CTD	CEF	Industrial OT
Claroty	Ranger	CEF	Industrial OT

Vendor	Product/Service	Format	Category
Claroty (Medigate)	Medical Device Security Platform	CEF	Industrial OT
Cofense	Triage	CEF	Log Management
Corelight	DNS	Syslog	Network
Corelight	HTTP	Syslog	Firewall
CrowdStrike	Falcon	CEF, LEEF	Endpoint
CyberArk	PTA	CEF, LEEF	Authentication & Identity Management
CyberArk	Vault	CEF, LEEF	Data Management System
CyberArk	Viewfinity	Syslog	Authentication & Identity Management
Cylance	Protect IPS	Syslog	Endpoint
Darktrace	DCIP	CEF	Security
Dell EMC	Data Domain	Syslog	Data Management System
Digital Arts	i-FILTER HTTP Proxy	Syslog	Network Security
Digital Guardian	Code Green Networks DLP	Syslog	Data Protection
Dovecot	Email Server	Syslog	Mail
Epic	Security-SIEM	CEF	SIEM
Epic Systems	Epic Healthcare	Syslog	Business
ESET	Antivirus	LEEF	Endpoint
ESET	Remote Administrator	Syslog	Endpoint
ExtraHop	ExtraHop	Syslog	Firewall
F5	Load Balancer	CEF	Security
F5	ASM	Syslog	Security
F5	Big-IP	JSON	Security
F5	Big-IP APM	Syslog	Security
F5	Big-IP ASM	Syslog	Security
F5	VPN	Syslog	Firewall
FairWarning	Patient Privacy Monitoring (PPM)	Syslog	Security
Fidelis Cybersecurity	Fidelis Cybersecurity	Syslog	Security

Vendor	Product/Service	Format	Category
FireEye	FireEye	JSON	Security
FireEye	Email Security (ETP)	JSON	Security
FireEye	Email Security (EX)	JSON	Security
FireEye	Email Security (EX)	JSON	Security
FireEye	Email Security (HX)	JSON	Security
FireEye	FireEye Endpoint Agent	JSON	Security
FireEye	FireEye HX Controller	JSON	Security
FireEye	Localsig	JSON	Security
FireEye	Network Security (NX)	JSON	Security
FireEye	Network Security (NX)	JSON	Security
FireEye	Packet Capture (PX)	JSON	Security
FireEye	Network Security (NX), Email Security (EX), Malware Analysis (AX)	JSON	Security
FireEye	Network Security (NX), Email Security (EX), Malware Analysis (AX)	JSON	Security
Forcepoint	DLP	CEF	Data Protection
Forcepoint	Email	CEF	Email & Collaboration
Forcepoint	Firewall	CEF	Network Security
Forcepoint	HTTP Proxy	CEF, LEEF	Web Security
Forcepoint	Websense HTTP Proxy	CEF, LEEF	Web Security
ForgeRock	ForgeRock	Syslog	Authentication & Identity Management
ForgeRock	Tomcat	Syslog	Authentication & Identity Management
Forescout	CounterACT	JSON, CEF, LEEF	Network Security
Forescout	NAC	Syslog	Network Security
Forescout	SecurityMatters SilentDefense	CEF	Industrial OT
Fortinet	Bradford Network Sentry	CEF	Network Security
Fortinet	FortiAnalyzer	Syslog	Network Security
Fortinet	FortiGate	CEF	Network Security
Fortinet	FortiMail	Syslog	Email & Collaboration

Vendor	Product/Service	Format	Category
GitHub	GitHub	Syslog	Content Management
GitHub	Auth	Syslog	Content Management
GTB Technologies	Inspector	CEF	Threat Intelligence
Guardicore	Centra	CEF	Threat Intelligence
HAProxy Technologies	HTTP	Syslog	Network Security
HelpSystems	Powertech Interact	CEF	Privileged Access Management
HP Enterprise	MicroFocus ArcSight	CEF	Security Information & Event Management (SIEM)
HP Enterprise	Aruba Networks	Syslog	Network
HP Enterprise	HP-UX	Syslog	Infrastructure & Server Management
IBM	AIX	Syslog	Infrastructure & Server Management
IBM	BigFix	Syslog	Endpoint Security
IBM	Guardiant	Syslog	User & Entity Behavior Analytics
IBM	OS/390	CEF	Infrastructure & Server Management
IBM	Proventia	CEF, LEEF	Intrustion Detection & Prevention
IBM	QRadar	LEEF	Security Information & Event Management (SIEM)
IBM	WebSEAL	CEF	Authentication & Identity Management
IBM	WebSphere	Syslog	Cloud Security
IBM	WinCollect	Syslog	Log Management
IBM	XGS	Syslog	Network Security
iBoss	Secure Web Gateway	Syslog	Web Security
Imperva	Incapsula	CEF, LEEF	Web Security
Imperva	Runtime Application Self-Protection (RASP)	JSON	Data Protection
Imperva	SecureSphere	CEF	Data Protection
Imperva	SecureSphere Data Security	Syslog	Data Protection
Imperva	SecureSphere WAF	Syslog	Web Security
Imperva	JSonar	CEF	Vulnerability Management
Infoblox	IntSights	CEF	Authentication & Identity Management

Vendor	Product/Service	Format	Category
Infoblox	Ivanti	Syslog	Authentication & Identity Management
Ivanti	Lookout	Syslog	Endpoint Security
Juniper Networks	OSSEC	Syslog	Web Security
Juniper Networks	PowerDNS	Syslog	Network Security
Juniper Networks	ServiceNow	Syslog	Network Security
Juniper Networks	Silverfort	Syslog	Intrustion Detection & Prevention
Juniper Networks	SonicWall	CEF	Network Security
Juniper Networks	Sophos	Syslog	Infrastructure & Server Management
Juniper Networks	Tenable	CEF	Authentication & Identity Management
Juniper Networks	Vectra AI	Syslog	Security Information & Event Management (SIEM)
Juniper Networks	Webroot	Syslog	Remote Access & Support
Kaspersky	Security Center	CEF	Endpoint Security
Kiteworks	Secure File Sharing	JSON	Data Protection
Lancope	StealthWatch	CEF	Network Security
Lastline	Enterprise	CEF	Intrustion Detection & Prevention
ManageEngine	ADAudit Plus	CEF	Log Management
Mandiant	MCA	CEF	Security
Mandiant	MIR	CEF	Security
Mandiant	MSO	CEF	Security
McAfee	Ma	JSON	Security
McAfee	McAfee ePolicy Orchestrator (ePO)	CEF	Security Information & Event Management (SIEM)
McAfee	IPS	CEF	Network Security
McAfee	Network Security Platform (NSP)	CEF	Network Security
Men&Mice	DNS	Syslog	Network
Microsoft	Hexadite AIRS	CEF	Threat Intelligence & Response
Microsoft	Advanced Threat Analytics (ATA)	CEF	Authentication & Identity Management
Microsoft	System Center	Syslog	Infrastructure & Server Management

Vendor	Product/Service	Format	Category
Microsoft	ADFS	JSON	Authentication & Identity Management
Microsoft	DHCP	JSON, Syslog	Network
Microsoft	DNS	JSON, Syslog	Network
Microsoft	Exchange	CEF, Syslog	Email & Collaboration
Microsoft	IIS	JSON	Web Security
Microsoft	ISA Server	Syslog	Web Security
Microsoft	Cloud App Security SIEM Agent	CEF	Cloud Access Security Broker (CASB)
Microsoft	Netlogon	JSON	Authentication & Identity Management
Microsoft	Software Asset Management	Syslog	IT Asset Management (ITAM)
Microsoft	System Center Operations Manager	Syslog	Infrastructure & Server Management
Microsoft	SharePoint	Syslog	Content Management
Microsoft	TMG Firewall	Syslog	Network Security
Microsoft	TMG HTTP Proxy	Syslog	Web Security
Microsoft	Windows Cluster	Syslog	Infrastructure & Server Management
Microsoft	Windows Event	JSON, Syslog	Log Management
Microsoft	Windows Performance Monitor (perfmon)	Syslog	Log Management
Microsoft	Windows PowerShell	Syslog	Automation & Orchestration
Nagios	Core	Syslog	Network
Nessus	Network Monitor	CEF	Vulnerability Management
NETSCOUT	Arbor Networks Peakflow	CEF	Network
NEXUS	PAS Card	CEF	Authentication & Identity Management
OCLC	EZproxy	Syslog	Remote Access & Support
One Identity	Safeguard	CEF	Privileged Access Management
Open Systems	SD-WAN	JSON	Network
Oracle	Oracle Auditing	Syslog	Data Management System
Oracle	Cloud Infrastructure (OCI)	JSON	Infrastructure & Server Management
Oracle	Sun One LDAP	CEF	Authentication & Identity Management

Vendor	Product/Service	Format	Category
Oracle	Sun Solaris	Syslog	Operating System
Osirium	PAM	CEF	Privileged Access Management
OSSEC	OSSEC	CEF	Network Security
Palo Alto Networks	Config	CEF	Network Security
Palo Alto Networks	Correlation	CEF	Security Information & Event Management (SIEM)
Palo Alto Networks	Decryption	CEF	Network Security
Palo Alto Networks	Firewall	CEF	Network Security
Palo Alto Networks	GlobalProtect	CEF	Remote Access & Support
Palo Alto Networks	GTP	CEF	Network Security
Palo Alto Networks	HIP Match	CEF	Threat Intelligence & Response
Palo Alto Networks	HTTP Proxy	Syslog	Web Security
Palo Alto Networks	LightCyber	Syslog	Network
Palo Alto Networks	System	CEF	Operating System
Palo Alto Networks	Threat Data	Syslog	Threat Intelligence & Response
Palo Alto Networks	Threat File	CEF	Threat Intelligence & Response
Palo Alto Networks	Threat Flood	CEF	Threat Intelligence & Response
Palo Alto Networks	Threat Packet	CEF	Threat Intelligence & Response
Palo Alto Networks	Threat Scan	CEF	Threat Intelligence & Response
Palo Alto Networks	Threat Spyware	CEF	Threat Intelligence & Response
Palo Alto Networks	Threat URL	CEF, LEEF	Threat Intelligence & Response
Palo Alto Networks	Threat Virus	CEF	Threat Intelligence & Response
Palo Alto Networks	Threat Vulnerability	CEF	Vulnerability Management
Palo Alto Networks	Threat WildFire	CEF	Security
Palo Alto Networks	Traffic	CEF, LEEF	Network Security
Palo Alto Networks	Traps	CEF	Endpoint Security
Palo Alto Networks	User-ID	CEF	Authentication & Identity Management
pfSense	Filterlog	Syslog	Network Security

Vendor	Product/Service	Format	Category
Ping Identity	Ping Identity	CEF	Authentication & Identity Management
Postgres	PostgreSQL	Syslog	Data Management System
PowerDNS	PowerDNS	Syslog	Network
Proofpoint	ObserveIT	CEF	Threat Intelligence
Proofpoint	Sendmail	Syslog	Mail
Proofpoint	SIEM API	Syslog	Security Information & Event Management (SIEM)
Pulse Secure	VPN	Syslog	Network
PwC	Bit	Syslog	Security
Quality Open Software (QOS)	Logback	Syslog	Log Management
RedSeal	Cap	Syslog	Network Security
Reservoir Labs	R-Scope Conn	Syslog	Network Security
Reservoir Labs	R-Scope DNS	Syslog	Network Security
Reservoir Labs	R-Scope Files	Syslog	Network Security
Reservoir Labs	R-Scope HTTP	Syslog	Network Security
Reservoir Labs	R-Scope SMTP	Syslog	Network Security
Reservoir Labs	R-Scope SSL	Syslog	Network Security
Reservoir Labs	R-Scope Syslog	Syslog	Network Security
Reservoir Labs	R-Scope Weird	Syslog	Network Security
Riverbed	Network Monitoring	Syslog	Log Management
RSA	Fortscale UBA	Syslog	User & Entity Behavior Analytics
RSA	Authentication Manager	Syslog	Authentication & Identity Management
RSA	NetWitness	CEF	Network
SecureAuth	IdP	Syslog	Authentication & Identity Management
Silverfort	Silverfort	CEF	Security
SonicWall	SonicWall	CEF	Network Security
SonicWall	NSA	Syslog	Web Security
SonicWall	SRA	Syslog	Network Security

Vendor	Product/Service	Format	Category
Sophos	Sophos	Syslog	Endpoint Security
Sophos	UTM	Syslog	Endpoint Security
Splunk	Ops	Syslog	Security Information & Event Management (SIEM)
Splunk	Stream	JSON	Log Management
Splunk	Stream DNS	CEF	Network
Squid	Squid HTTP Proxy	Syslog	Network Security
Stealthbits Technologies	StealthINTERCEPT	CEF, LEEF	Security
Suricata	Suricata HTTP Proxy	Syslog	Network Security
Symantec	Blue Coat HTTP Proxy	CEF	Network Security
Symantec	Blue Coat Ops	Syslog	Network
Tenable	Nessus	CEF	Vulnerability Management
Thales eSecurity	Vormetric DSM	CEF, LEEF	Security
Thales eSecurity	Vormetric VFS	CEF, LEEF	Data Protection
The National Institute of Open Schooling (NIOS)	Mobile App	Syslog	Endpoint Security
Thycotic	Secret Server	CEF	Authentication & Identity Management
Trend Micro	Tipping Point IPS	CEF	Network Security
Trend Micro	Control Manager	CEF	Security
Trend Micro	Deep Discover Analyzer	CEF, LEEF	Threat Intelligence
Trend Micro	Deep Discover Inspector	LEEF	Network
Trend Micro	HTTP Proxy	Syslog	Network Security
Trend Micro	InterScan Messaging Security (IMSVA)	Syslog	Email & Collaboration
Tripwire	Enterprise	CEF	Network Security
Tripwire	IDS	CEF	Network Security
Trustwave	HTTP Proxy	CEF	Network Security
Unix Service	Bind DNS	Syslog	Operating System
Unix Service	collectd	Syslog	Operating System
Unix Service	Dhclient DHCP	Syslog	Operating System

Vendor	Product/Service	Format	Category
Unix Service	DHCPD DHCP	Syslog	Operating System
Unix Service	DNSMasq	Syslog	Operating System
Unix Service	Docker	JSON	Operating System
Unix Service	Inetd	Syslog	Operating System
Unix Service	Jboss App Server	Syslog	Operating System
Unix Service	nscd	Syslog	Operating System
Unix Service	nginx	Syslog	Operating System
Unix Service	ntpd	Syslog	Operating System
Unix Service	OpenSFTP	Syslog	Operating System
Unix Service	OpenLDAP	Syslog	Operating System
Unix Service	OpenPGP	Syslog	Operating System
Unix Service	OpenVPN	Syslog	Operating System
Unix Service	PHP	Syslog	Operating System
Unix Service	Postfix Mail TA	Syslog	Operating System
Unix Service	Puppet	Syslog	Operating System
Unix Service	Python	Syslog	Operating System
Unix Service	qmail MTA	Syslog	Operating System
Unix Service	rsyslog	Syslog	Operating System
Unix Service	Salt Minion	Syslog	Operating System
Unix Service	Sendmail	Syslog	Operating System
Unix Service	snmpd	Syslog	Operating System
Unix Service	Snort	CEF	Operating System
Unix Service	stunnel	Syslog	Operating System
Unix Service	Unix	CEF	Operating System
Unix Service	Automatic Bug Reporting Tool (ABRT)	Syslog	Operating System
Unix Service	anacron	Syslog	Operating System
Unix Service	atd	Syslog	Operating System

Vendor	Product/Service	Format	Category
Unix Service	audit	Syslog	Operating System
Unix Service	cron	Syslog	Operating System
Unix Service	cxtracker	Syslog	Operating System
Unix Service	FTP	Syslog	Operating System
Unix Service	Health Check	Syslog	Operating System
Unix Service	impi	Syslog	Operating System
Unix Service	init	Syslog	Operating System
Unix Service	kernel	Syslog	Operating System
Unix Service	kprop	Syslog	Operating System
Unix Service	mgmtd	Syslog	Operating System
Unix Service	mon	Syslog	Operating System
Unix Service	multipath	Syslog	Operating System
Unix Service	Nagios Remote Plugin Executor (NRPE)	Syslog	Operating System
Unix Service	OSSEC	Syslog	Operating System
Unix Service	Pluggable Authentication Module (PAM)	Syslog	Operating System
Unix Service	RGP	Syslog	Operating System
Unix Service	SCSI	Syslog	Operating System
Unix Service	SSH	Syslog	Operating System
Unix Service	statsd	Syslog	Operating System
Unix Service	syslog	Syslog	Operating System
Unix Service	xntpd (NTP)	Syslog	Operating System
Unix Service	Xecutor	Syslog	Operating System
Unix Service	xinetd	Syslog	Operating System
Varonis	DataPrivilege	CEF	Network Security
Vectra AI	Vectra AI	JSON	Data Management System
Verdasys	Digital Guardian	CEF	Data Protection
VMware	ESX	Syslog	Operating System

VMware	ESXi	CEF	Operating System
VMware	Horizon	Syslog	Virtual
VMware	Management	Syslog	Virtual
VMware	Unified Access Gateway	Syslog	Remote Access & Support
VMware	vSphere	Syslog	Cloud Computing
Voya	Voya SSO	CEF	Authentication & Identity Management
WatchGuard	Firewall	Syslog	Network Security
Waterfall	Logger	Syslog	Industrial OT
Waterfall	Unidirectional Security Gateway	Syslog	Industrial OT
WTI	DSM Server	Syslog	Network
ZeroFox	Threat Feed	Syslog	Threat Intelligence
Zscaler	Firewall & Web Proxy	LEEF	Firewall

Trellix Automated Response (TAuR) within XDR

Trellix Automated Response is our Security Orchestration and Response capability that brings response actions to your XDR console for both Trellix and third-party applications. These actions are generated automatically from a rule created within the XDR console or manually from an alert within the XDR console. The application under control is triggered through their API capabilities and will perform actions, such as create incident tickets, triage an event, or even quarantine a system. This feature of TAuR within XDR does not have customized playbooks, rather skip to the next section to customized your response actions.

The following TAuR response actions are available.

Table 3 - TAuR Response Actions

Vendor	Solution	TAuR Version
Microsoft	Azure	TAuR Cloud
Microsoft	User Enrichment	TAuR Cloud
ServiceNow	ServiceNow	TAuR Cloud
Trellix	Cloudvisory	TAuR Cloud
Trellix	EDR (Mvision EDR)	TAuR Cloud
Trellix	ePO	TAuR Cloud
Trellix	IVX	TAuR Cloud
VirusTotal	VirusTotal Plug-in	TAuR Cloud

Trellix Automated Response (TAuR) On-Premise

Trellix Automated Response is our Security Orchestration and Response capability that brings response actions to your XDR console for both Trellix and third-party applications. This version of TAuR (also named FSO) can be installed locally on a virtual machine or in a cloud environment as a virtual image. TAuR On-Premise is a full SOAR solution that allows customizations and light case management on your response actions.

The following TAuR response actions are available.

Table 4 - TAuR Response Actions – On-Premise

Vendor	Solution	TAuR Version
AbuseIPDB	AbuseIPDB	TAuR Virtual
AlienVault	AlienVault OTX	TAuR Virtual
Anomali	Anomali ThreatStream Plug-in	TAuR Virtual
AOL Moloch	AOL Moloch Plug-in	TAuR Virtual
Apache	Apache Kafka Plug-in	TAuR Virtual
Apility.io	Apility.io Plug-in	TAuR Virtual
AWS	Amazon CloudTrail	TAuR Virtual
AWS	Amazon WAF	TAuR Virtual
AWS	Amazon GuardDuty	TAuR Virtual
AWS	Amazon VPC Plug-in	TAuR Virtual
AWS	Amazon S3 Plug-in	TAuR Virtual
AWS	Amazon SNS Plug-in	TAuR Virtual
AWS	Amazon Lambda Plug-in	TAuR Virtual
AWS	Amazon IAM Plug-in	TAuR Virtual
AWS	Amazon EC2 Plug-in	TAuR Virtual
AWS	Amazon Athena Plug-in	TAuR Virtual
AWS	Alexa AWIS	TAuR Virtual
Axonius	Axonius Plug-in	TAuR Virtual
Best Practical	Best Practical Request Tracker Plug-in	TAuR Virtual
BlacklistMaster	BlacklistMaster Plug-in	TAuR Virtual
BMC	BMC Remedy Plug-in	TAuR Virtual
BMC	BMC Remedy AR System	TAuR Virtual

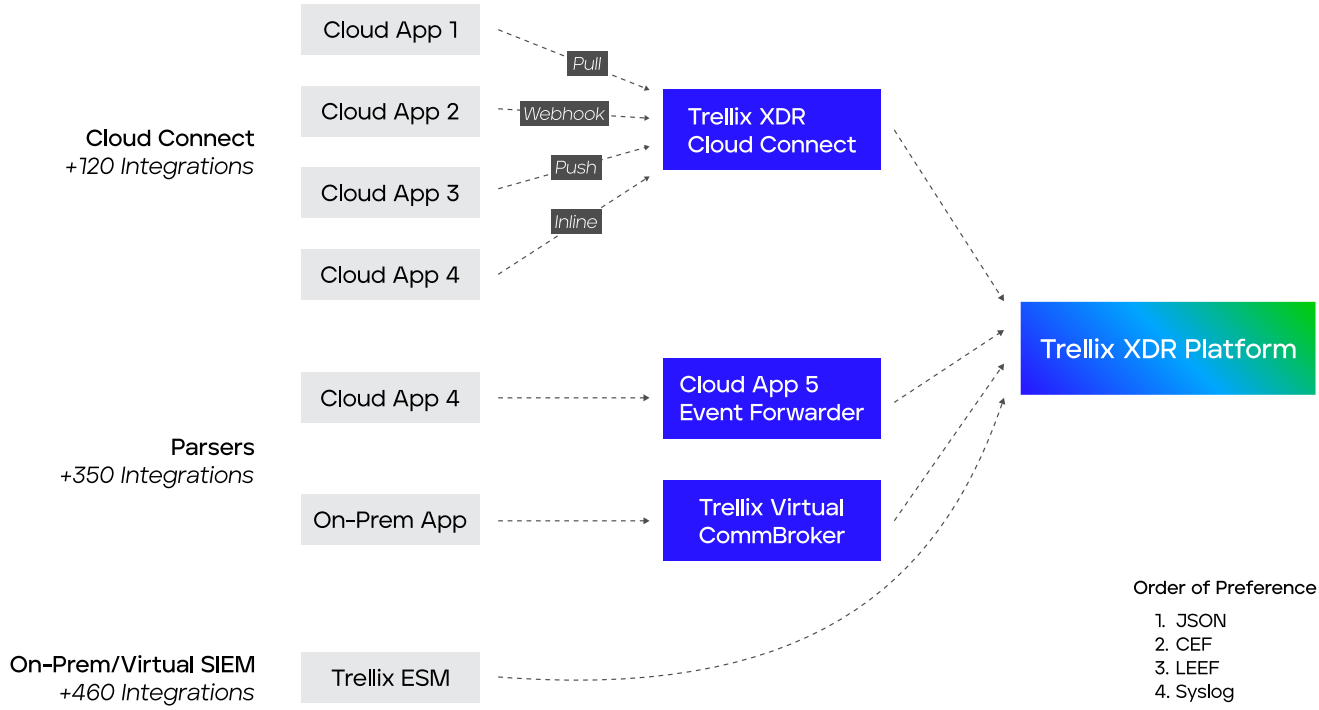
Vendor	Solution	TAuR Version
Broadcom	Broadcom/Symantec Security Analytics Plug-in	TAuR Virtual
Broadcom	Broadcom/Symantec Data Loss Prevention (DLP) Plug-in	TAuR Virtual
Censys	Censys Plug-in	TAuR Virtual
Check Point	Check Point Management	TAuR Virtual
Cherwell	Cherwell Plug-in	TAuR Virtual
Cisco	Cisco Threat Grid Plug-in	TAuR Virtual
Cisco	Cisco ISE Plug-in	TAuR Virtual
Cuckoo	Cuckoo Sandbox Plug-in	TAuR Virtual
Darktrace	Darktrace Threat Visualizer	TAuR Virtual
DNS	DNS	TAuR Virtual
DomainTools	DomainTools Plug-in	TAuR Virtual
DomainTools	DomainTools Iris Investigate Plug-in	TAuR Virtual
Elastic	Elasticsearch Plug-in	TAuR Virtual
Elastic	Elastic Endgame Plug-in	TAuR Virtual
Farsight	Farsight DNSDB Plug-in	TAuR Virtual
Forcepoint	Forcepoint Web Security Plug-in	TAuR Virtual
Fortinet	Fortinet FortiSIEM Plug-in	TAuR Virtual
Freshworks	Freshworks Freshservice Plug-in	TAuR Virtual
Google	Google Safe Browsing Plug-in	TAuR Virtual
Google	Google Gmail Plug-in	TAuR Virtual
Google	Google Geolocation Plug-in	TAuR Virtual
Hack I Been Pwned	Have I Been Pwned Plug-in	TAuR Virtual
HackerTarget	HackerTarget Plug-in	TAuR Virtual
HCL	HCL BigFix Plug-in	TAuR Virtual
IBM	IBM X-Force Plug-in	TAuR Virtual
IBM	IBM Domino Plug-in	TAuR Virtual
IFTT	IFTTT Plug-in	TAuR Virtual

Vendor	Solution	TAuR Version
Infoblox	Infoblox Plug-in	TAuR Virtual
IntSights	IntSights	TAuR Virtual
IPHub	IPHub Plug-in	TAuR Virtual
IPQualityScore	IPQualityScore Plug-in	TAuR Virtual
Joe Sandbox	Joe Sandbox Cloud	TAuR Virtual
Juniper	Juniper Cyphort Plug-in	TAuR Virtual
Kaseya	Kaseya Vorex	TAuR Virtual
KnowBe4	KnowBe4 Plug-in	TAuR Virtual
Koodous	Koodous Plug-in	TAuR Virtual
LogRhythm	LogRhythm Platform Manager Plug-in	TAuR Virtual
MAC	MAC Vendors Lookup Plug-in	TAuR Virtual
malboxlayer	mailboxlayer Plug-in	TAuR Virtual
MalShare	MalShare Plug-in	TAuR Virtual
malware.com	malware.com Plug-in	TAuR Virtual
ManageEngine ServiceDesk	ManageEngine ServiceDesk Plug-in	TAuR Virtual
Mandiant	Mandiant Threat Intelligence Plug-in	TAuR Virtual
Mandiant	Mandiant Advantage	TAuR Virtual
Micro Focus	Micro Focus Universal CMDB Plug-in	TAuR Virtual
Micro Focus	Micro Focus ArcSight Logger Plug-in	TAuR Virtual
Micro Focus	Micro Focus ArcSight ESM Plug-in	TAuR Virtual
Micro Focus	Micro Focus ArcSight CEF Plug-in	TAuR Virtual
Microsoft	Microsoft Teams Plug-in	TAuR Virtual
Microsoft	Microsoft SMB Share Plug-in	TAuR Virtual
Microsoft	Microsoft SCCM Plug-in	TAuR Virtual
Microsoft	Microsoft NetBIOS Plug-in	TAuR Virtual
MISP	MISP Plug-in	TAuR Virtual
Mnemonic	Mnemonic Plug-in	TAuR Virtual

Vendor	Solution	TAuR Version
MobileIron	MobileIron MDM Plug-in	TAuR Virtual
MxToolbox	MxToolbox Plug-in	TAuR Virtual
MyIP	MyIP Plug-in	TAuR Virtual
Neutrino	Neutrino API Plug-in	TAuR Virtual
Nmap	Nmap Plug-in	TAuR Virtual
Pastebin	Pastebin Plug-in	TAuR Virtual
PhishTank	PhishTank Plug-in	TAuR Virtual
Proofpoint	Proofpoint URLDefense Plug-in	TAuR Virtual
Proofpoint	Proofpoint Threat Insight	TAuR Virtual
Proxycheck.io	Proxycheck.io Plug-in	TAuR Virtual
Qualys	Qualys Vulnerability Management	TAuR Virtual
Rapid7	Rapid7 InsightVM Plug-in	TAuR Virtual
Recorded Future	Recorded Future Plug-in	TAuR Virtual
Restpack	Restpack.io Screenshot Plug-in	TAuR Virtual
ReversingLabs	ReversingLabs TitaniumCloud Plug-in	TAuR Virtual
RiskIQ	RiskIQ PassiveTotal Plug-in	TAuR Virtual
RocketChat	RocketChat Plug-in	TAuR Virtual
RSA	RSA Security Analytics Plug-in	TAuR Virtual
ServiceNow	ServiceNow	TAuR Virtual
SFTP	SFTP Rapid	TAuR Virtual
Shodan	Shodan Plug-in	TAuR Virtual
Slack	FireEye Message Security for Slack	TAuR Virtual
SolarWinds	SolarWinds Plug-in	TAuR Virtual
SSH	SSH Plug-in	TAuR Virtual
Symantec	Symantec Blue Coat ProxySG Plug-in	TAuR Virtual
SysAid	SysAid	TAuR Virtual
Tanium	Tanium Plug-in	TAuR Virtual

Vendor	Solution	TAuR Version
Telegram	Telegram Plug-in	TAuR Virtual
Tenable	Tenable SecurityCenter Plug-in	TAuR Virtual
TheHive	TheHive Plug-in	TAuR Virtual
ThreatConnect	ThreatConnect Plug-in	TAuR Virtual
ThreatCrowd	ThreatCrowd	TAuR Virtual
ThreatCrowd	ThreatCrowd	TAuR Virtual
Tor	Tor Plug-in	TAuR Virtual
Twilio	Twilio Messaging Plug-in	TAuR Virtual
Twitter	Twitter Plug-in	TAuR Virtual
Unshorten.me	Unshorten.me Plug-in	TAuR Virtual
URLScan	URLScan.io Plug-In	TAuR Virtual
URLVoid	URLVoid APIVoid Plug-in	TAuR Virtual
Vade	Vade Secure IsItPhishing Plug-In	TAuR Virtual
VirusTotal	VirusTotal Plug-in	TAuR Virtual
Vulners	Vulners Plug-in	TAuR Virtual
Wayback Machine	Internet Archive Wayback Machine Plug-in	TAuR Virtual
Web of Turst	Web of Trust Plug-in	TAuR Virtual
WhoAPI	WhoAPI Plug-in	TAuR Virtual
Whois	WhoisXML API Plug-in	TAuR Virtual
Wireshark	Wireshark Plug-in	TAuR Virtual
Zscaler	Zscaler Internet Access SSE Plugin	TAuR Virtual

Visual of XDR Integrations



Conclusion

XDR integrations are a powerful tool for improving cybersecurity and threat detection capabilities. With over 1,000 integrations available, Cloud Connect for easy data ingestion, and on-premise connectors for maximum flexibility, the Trellix XDR platform offers a comprehensive and effective solution for your customers.

Visit Trellix.com to learn more.