USM Anywhere AlienApps List

The AT&T Alien Labs™ Security Research Team regularly updates the data source library to increase the extensibility of USM Anywhere. These AlienApps enable your USM Anywhere Sensor to process and analyze logs produced by your existing devices and applications.

Note: This table shows the AlienApps that ship with USM Anywhere as of *April 05, 2023*. If you cannot find the AlienApp that you are looking for, submit a request so we can build one for you.

List of AlienApps Available in USM Anywhere

Data Source	AlienApp	Log Format	Auto-discovered
AdminbyRequest NXLog	AdminbyRequest NXLog	JSON	Yes
AdTran Switch	AdTran Switch	RegEx	No
Aerohive WAP	Aerohive Networks Aerohive WAP	RegEx	No
AIX Audit	IBM AIX Audit	RegEx	No
Akamai EAA	Akamai EAA	JSON	No
Akamai ETP	Akamai ETP	JSON	No
Alibaba Cloud	Alibaba Cloud	Key-Value	Yes
AlienVault Agent	None. Data received through AlienVault Agent	JSON	No
AlienVault Agent - Windows EventLog	None. Data received through AlienVault Agent	JSON	No
AlienVault Cluster Management Application	AlienVault Cluster Management Application	RegEx	No
AlienVault Internal API	AT&T Cybersecurity Forensics and Response	JSON	No
AlienVault NIDS	None. Data received through a deployed sensor	JSON	Yes

List of AlienApps Available in USM Anywhere (Continued)

Data Source	AlienApp	Log Format	Auto-discovered
Amazon Aurora	AWS Aurora	CSV	No
Amazon Aurora PostgrestSQL	AWS Aurora PostgrestSQL	RegEx	No
Amazon AWS CloudTrail	AWS CloudTrail	JSON	No
Amazon CloudFront Real Time Logs W3C	AWS CloudFront Real Time Logs W3C	W3C	No
Amazon EKS API Server	AWS EKS API Server	RegEx	No
Amazon EKS API Server Audit	AWS EKS API Server Audit	JSON	No
Amazon EKS Authenticator	AWS EKS Authenticator	Key-Value	No
Amazon Elasticsearch Service	AWS Elasticsearch Service	JSON	No
Amazon GuardDuty	AWS GuardDuty	JSON	No
Amazon Macie	AWS Macie	JSON	No
Amazon MSK	AWS MSK	JSON	Yes
Amazon Redshift	AWS Redshift	CSV	No
Amazon Redshift User Activity	AWS Redshift User Activity	RegEx	No
Amazon VPC Flow Logs	AWS VPC Flow Logs	CSV	No
Apache	Apache Web Server CLF	CLF	Yes
Apache Server	Apache Web Server	RegEx	No
Apple Airport Extreme	Apple Airport Extreme	RegEx	No
Arbor Networks Pravail APS	Arbor Networks Pravail APS	RegEx	Yes
Arista Networks Platform	Arista Networks Platform	RegEx	Yes
Armis Endpoint Security	Armis	JSON	No
Arpwatch	LBNL Arpwatch	RegEx	Yes
Array Networks APV Series	Array Networks APV Series	Key-Value	No
ArticaProxy	ArticaProxy	RegEx	No

List of AlienApps Available in USM Anywhere (Continued)

Data Source	AlienApp	Log Format	Auto-discovered
Aruba	Aruba Networks Wireless	RegEx	No
Aruba ClearPass	Aruba Networks ClearPass	RegEx	No
Aruba ClearPass CEF	Aruba Networks ClearPass	CEF	Yes
Aruba Mobility Master	Aruba Networks Mobility Master	CEF	Yes
Aruba Switch	Aruba Networks Switch	RegEx	No
Asterisk VoIP	Asterisk VoIP	RegEx	No
AT&T Network Based Firewall	AT&T Network Based Firewall	JSON	No
AT&T VPN-RAS-GW	AT&T VPN-RAS-GW	Key-Value	No
Aunt Bertha Website Acitvity Plugin	Aunt Bertha Website Acitvity	JSON	No
Auth0	Auth0	JSON	Yes
Auth0 - EventBridge	Auth0 - EventBridge	JSON	Yes
Avanan Email Security	Avanan Email Security	JSON	No
Avaya Media Gateway	Avaya Media Gateway	RegEx	Yes
Avaya VSP Switches	Avaya VSP Switches	RegEx	No
Avaya Wireless LAN	Avaya Wireless LAN	RegEx	No
Aviatrix Cloud Gateway	Aviatrix Cloud Gateway	Key-Value	Yes
AWS API Gateway	AWS API Gateway	JSON	No
AWS Application Load Balancer	AWS Application Load Balancer	CSV	No
AWS Client VPN Endpoint	AWS Client VPN Endpoint	JSON	No
AWS Config	AWS Config	JSON	No
AWS Directory Service	AWS Directory Service	XML	No
AWS ECS	AWS ECS	JSON	No
AWS Health	AWS Health	JSON	Yes

List of AlienApps Available in USM Anywhere (Continued)

Data Source	AlienApp	Log Format	Auto-discovered
AWS IoT	AWS IoT	JSON	No
AWS Kubernetes	AWS Kubernetes	RegEx	No
AWS Lambda	AWS Lambda	JSON	No
AWS Lambda@edge	AWS Lambda@edge	JSON	No
AWS Neptune	AWS Neptune	CSV	No
AWS Network Firewall	AWS Network Firewall	JSON	No
AWS RDS	AWS RDS	XML	No
AWS RDS MySQL	AWS RDS MySQL	RegEx	No
AWS RDS PostgreSQL	AWS RDS PostgreSQL	RegEx	No
AWS Route 53 Resolver Query Logs	AWS Route 53 Resolver Query Logs	JSON	No
AWS Step Functions	AWS Step Functions	JSON	No
AWS Storage Gateway	AWS Storage Gateway	JSON	No
AWS VPC Flow Logs	AWS VPC Flow Logs	JSON	No
AWS Web Application Firewall (WAF)	AWS Web Application Firewall	JSON	No
AWS Windows	AWS Windows	Split	No
Azure AD Audit Logs	Microsoft Azure AD Audit Logs	JSON	No
Azure AD Monitoring	Microsoft Azure AD Monitoring	JSON	No
Azure AD Sign In	Microsoft Azure AD Sign In	JSON	No
Azure AKS BLOB storage	Microsoft Azure AKS BLOB storage	JSON	No
Azure App Service	Microsoft Azure App Service	JSON	No
Azure Application Gateway	Microsoft Azure Application Gateway	JSON	Yes

List of AlienApps Available in USM Anywhere (Continued)

Data Source	AlienApp	Log Format	Auto-discovered
Azure IIS	Microsoft Azure IIS	W3C	No
Azure Insight	Microsoft Azure Insight	JSON	No
Azure Multifactor Authentication	Microsoft Azure Multifactor Authentication	RegEx	No
Azure Security Center	Microsoft Azure Security Center	JSON	No
Azure SQL Database	Microsoft Azure SQL Database	JSON	No
Azure SQL Server	Microsoft Azure SQL Server	JSON	No
Azure VPN Gateway	Azure VPN Gateway	JSON	No
Azure Web App	Microsoft Azure Web App	W3C	No
Azure Windows Events	Microsoft Azure Windows Events	JSON	No
Barracuda CloudGen Firewall	Barracuda CloudGen Firewall	RegEx	Yes
Barracuda Content Shield	Barracuda Content Shield	RegEx	Yes
Barracuda Email Security Service	Barracuda Email Security Service	JSON	No
Barracuda Load Balancer ADC	Barracuda Load Balancer ADC	Key-Value	No
Barracuda NextGen Firewall	Barracuda NextGen Firewall	RegEx	Yes
Barracuda NextGen Firewall Traffic	Barracuda NextGen Firewall	Traffic Key-Value	Yes
Barracuda Spam Firewall	Barracuda Spam Firewall	CSV	Yes
Barracuda Web Application Firewall	Barracuda Web Application Firewall	RegEx	Yes
Barracuda Web Application Firewall CEF	Barracuda Web Application Firewall	CEF	Yes
Barracuda Web Filter	Barracuda Web Filter	RegEx	Yes
Bayshore	Bayshore	Key-Value	No
BeyondTrust BeyondInsight	BeyondTrust BeyondInsight	Key-Value	No

List of AlienApps Available in USM Anywhere (Continued)

Data Source	AlienApp	Log Format	Auto-discovered
BeyondTrust Privilege Management Console	BeyondTrust Privilege Management Console	JSONbeyond	No
Bitdefender GravityZone	Bitdefender GravityZone	JSON	Yes
Bitvise SSH Server NXLog	Bitvise SSH Server NXLog	JSON	Yes
BlackBerry UEM	BlackBerry UEM	RegEx	No
Bluecoat W3C	Bluecoat	W3C	No
Box Events	Box	JSON	No
Bricata	Bricata	LEEF	Yes
Bro IDS	Bro IDS	JSON	Yes
Brocade	Brocade	RegEx	No
Buffalo TeraStation	Buffalo TeraStation	RegEx	Yes
Business Intelligence Analytics	Looker Business Intelligence Analytics	RegEx	No
Cambium Networks Xirrus	Cambium Networks Xirrus	RegEx	No
Capsule8 Linux Detection	Capsule8 Linux Detection	JSON	No
Cato Networks Cloud-based NGFW	Cato Networks Cloud-based NGFW	CEF	Yes
Carbon Black Defense	Carbon Black Endpoint Standard	CEF	Yes
Carbon Black Defense JSON	Carbon Black Endpoint Standard	JSON	No
Carbon Black Protection	Carbon Black App Control	Key-Value	No
Carbon Black Protection CEF	Carbon Black App Control	CEF	Yes
Carbon Black EDR JSON	Carbon Black EDR	JSON	No
Carbon Black EDR LEEF	Carbon Black EDR	Key-Value	No
Centrify Cloud IdM	Centrify Cloud IdM	Key-Value	Yes
Centrify Server Suite	Centrify Server Suite	RegEx	Yes

List of AlienApps Available in USM Anywhere (Continued)

Data Source	AlienApp	Log Format	Auto-discovered
Check Point CloudGuard Dome9	Check Point CloudGuard Dome9	JSON	Yes
Check Point FW1	Check Point	Key-Value	No
Check Point FW1 Generic	Check Point FW1	RegEx	No
Check Point FW1 Loggrabber	Check Point FW1	Loggrabber	Yes
Check Point FW1 R77.30	Check Point FW1	R77.30 Key-Value	No
Check Point FW1 R80 CEF	Check Point FW1	R80 CEF	Yes
Check Point SandBlast Agent	Check Point SandBlast Agent	Key-Value	No
Cisco ACE	Cisco ACE	RegEx	Yes
Cisco ACS	Cisco ACS	Key-Value	Yes
Cisco AMP for Endpoints	Cisco Secure Endpoint	JSON	No
Cisco ASA	Cisco Secure Firewall ASA	RegEx	Yes
Cisco ASR	Cisco ASR	RegEx	Yes
Cisco Email Security	Cisco Secure Email	CEF	Yes
Cisco ESA	Cisco ESA	Key-Value	No
Cisco Expressway	Cisco Expressway	RegEx	No
Cisco Firepower Management Center	Cisco Secure Firewall Threat Defense Manager	RegEx	Yes
Cisco Firepower NGIPS	Cisco Firepower NGIPS	RegEx	Yes
Cisco Firepower NGFW	Cisco Firepower NGFW	Key-Value	No
Cisco Firepower Threat Defense	Cisco Firepower Threat Defense	RegEx	Yes
Cisco HyperFlex	Cisco HyperFlex	RegEx	No
Cisco Ironport	Cisco Ironport	RegEx	No
Cisco ISE	Cisco ISE	Key-Value	Yes

List of AlienApps Available in USM Anywhere (Continued)

Data Source	AlienApp	Log Format	Auto-discovered
Cisco Lancope StealthWatch	Cisco Lancope StealthWatch	CEF	Yes
Cisco Meraki	Cisco Meraki	Key-Value	No
Cisco Nexus	Cisco Nexus	RegEx	Yes
Cisco Pix	Cisco Pix	RegEx	Yes
Cisco Router	Cisco Router	RegEx	Yes
Cisco RV Series Router	Cisco RV Series Router	RegEx	No
Cisco SD-WAN by Viptela	Cisco SD-WAN by Viptela	RegEx	Yes
Cisco Stealth Watch Cloud	Cisco Stealth Watch Cloud	JSON	No
Cisco UCS Manager	Cisco UCS Manager	RegEx	Yes
Cisco Umbrella	Cisco Umbrella	CSV	No
Cisco Umbrella Proxy	Cisco Umbrella Proxy	CSV	No
Cisco Unified Communications Manager	Cisco Unified Communications Manager	Key-Value	No
Cisco VPN	Cisco VPN	RegEx	No
Cisco WLC	Cisco WLC	RegEx	No
Citrix NetScaler	Citrix NetScaler	Key-Value	No
Citrix NetScaler Application Firewall CEF	Citrix NetScaler Application Firewall	CEF	Yes
Citrix XenServer	Citrix XenServer	RegEx	Yes
Clarity	Clarity	CSV	No
Claroty	Claroty	CEF	Yes
Clavister Firewall	Clavister Firewall	Key-Value	No
Clearswift SECURE Email Gateway	Clearswift SECURE Email Gateway	RegEx	No

List of AlienApps Available in USM Anywhere (Continued)

Data Source	AlienApp	Log Format	Auto-discovered
Clearswift SECURE Web Gateway	Clearswift SECURE Web Gateway	Split	No
Cloudflare Enterprise Log Share	Cloudflare	JSON	No
Cloudflare Enterprise Log Share Audit	Cloudflare	JSON	No
Cloudflare Enterprise Log Share Received	Cloudflare	JSON	No
CloudFront RTMP distribution W3C	AWS CloudFront RTMP distribution W3C	W3C	No
CloudFront Web distribution W3C	AWS CloudFront Web distribution W3C	W3C	No
CloudPassage CEF	CloudPassage	CEF	Yes
ConnectWise API	ConnectWise	JSON	No
Corelight	Corelight	JSON	No
Cowrite Honeypot	Cowrite Honeypot	JSON	Yes
Cradlepoint AER	Cradlepoint AER	RegEx	No
CrowdStrike	CrowdStrike	JSON	No
CrowdStrike Falcon	CrowdStrike Falcon	CEF	Yes
CyberArk Enterprise Password Vault	CyberArk Enterprise Password Vault	CEF	Yes
CyberHound	CyberHound	RegEx	No
CyberX Platform	CyberX Platform	CEF	Yes
Cylance CylancePROTECT	Cylance CylancePROTECT	Key-Value	Yes
Cylance CylancePROTECT - Logstash	Cylance CylancePROTECT	JSON	Yes
Cylance CylanceSVC	Cylance CylanceSVC	Key-Value	Yes

List of AlienApps Available in USM Anywhere (Continued)

Data Source	AlienApp	Log Format	Auto-discovered
Cylance Optics	Cylance Optics	Key-Value	Yes
Cynet 360	Cyphort 360	CEF	Yes
Cyphort CEF	Cyphort	CEF	Yes
D-Link UTM Firewall	D-Link UTM Firewall	Key-Value	Yes
Darktrace Cyber Intelligence Platform	Darktrace Cyber Intelligence Platform	CEF	Yes
Darktrace Cyber Intelligence Platform - JSON	Darktrace Cyber Intelligence Platform	JSON	Yes
DataSunrise Database Firewall	DataSunrise Database Firewall	CEF	Yes
DB CyberTech	DB CyberTech	CEF	Yes
Deep Instinct Advanced Endpoint Security	Deep Instinct Advanced Endpoint Security	CEF	Yes
Dell Boomi Atom	Dell Boomi Atom	JSON	Yes
Dell Compellent SC	Dell Compellent SC	RegEx	No
Dell EMC DNOS	Dell EMC DNOS	RegEx	No
Dell EMC Isilon	Dell EMC Isilon	RegEx	No
Dell Force10 Switch	Dell Force10 Switch	RegEx	No
Dell IDRAC	Dell IDRAC	RegEx	No
Dell Networking X-Series	Dell X-Series	RegEx	No
Dell SecureWorks	Dell SecureWorks	RegEx	No
Dell SonicWall UTM	SonicWall UTM	Key-Value	No
Dell SonicWall UTM - Logstash	Dell SonicWall UTM	JSON	Yes
DenyAll WAF	DenyAll WAF	CSV	No
DenyAll WAF JSON	DenyAll WAF	JSON	No
Devolutions Password Server	Devolutions Password Server	RegEx	No

List of AlienApps Available in USM Anywhere (Continued)

Data Source	AlienApp	Log Format	Auto-discovered
Digital Guardian DLP	Digital Guardian DLP	CEF	Yes
Digital Shadows Searchlight	Digital Shadows Searchlight	JSON	No
Docker	Docker	JSON	No
Docker Dockerd	Docker Dockerd	Key-Value	Yes
DrayTek Vigor	DrayTek Vigor	RegEx	No
Dropbox	Dropbox	JSON	No
Dtex	Dtex Systems	CEF	Yes
Duo Authentication Proxy NXLog	Duo Authentication Proxy NXLog	JSON	Yes
Duo Log Sync	Duo Log Sync	JSON	No
Duo Security - Logstash	Duo Security	JSON	Yes
Duo Two-Factor Authentication CEF	Duo Two-Factor Authentication	CEF	Yes
EclecticIQ Endpoint Response	EclecticIQ Endpoint Response	JSON	No
EdgeWave	EdgeWave	RegEx	No
Egnyte Audits	Egnyte Audits	Key-Value	Yes
Elastic Packetbeat - Logstash	Elastic Packetbeat	JSON	Yes
Elastic Winlogbeat - Logstash	Elastic Winlogbeat	JSON	Yes
ELBAccess	AWS ELBAccess	CSV	No
Endpoint Protector	CoSoSys Endpoint Protector	Key-Value	Yes
Epic EHR	Epic EHR	CEF	Yes
Eset	Eset	JSON	Yes
ExtraHop Reveal	ExtraHop Reveal	Key-Value	No
ExtraHop Reveal CEF	ExtraHop Reveal	CEF	Yes
ExtraHop Reveal JSON	ExtraHop Reveal	JSON	No

List of AlienApps Available in USM Anywhere (Continued)

Data Source	AlienApp	Log Format	Auto-discovered
Extreme Networks SummitX and Black Diamond Switches	Extreme Networks SummitX/Black Diamond Switches	RegEx	No
F-Secure Policy Manager	F-Secure Policy Manager	Key-Value	No
F5 Application Security Manager CEF	F5 BIG-IP ASM	CEF	No
F5 BIG-IP	F5 BIG-IP	RegEx	No
F5 BIG-IP Access Policy Manager	F5 BIG-IP Access Policy Manager	RegEx	No
F5 BIG-IP ASM	F5 BIG-IP ASM	CSV	Yes
Fail2ban	Fail2ban	Rgex	Yes
FiberStore Switches	FiberStore Switches	RegEx	No
FireEye Central Management System	FireEye Central Management	CEF	Yes
FireEye Endpoint Security HX Series	FireEye Endpoint Security	CEF	Yes
FireEye Malware Protection Systems	FireEye Malware Protection	CEF	Yes
Fluentd	Fluentd	RegEx	Yes
Forcepoint CASB	Forcepoint CASB	CEF	Yes
Forcepoint DLP	Forcepoint DLP	CEF	Yes
Forcepoint Email Security	Forcepoint Email Security	CEF	Yes
Forcepoint NGFW	Forcepoint NGFW	CEF	Yes
Forcepoint Triton AP-Web	Forcepoint Triton AP-Web	CEF	Yes
Forcepoint Web Security Cloud NXLog	Forcepoint Web Security Cloud	JSON	Yes
ForeScout NAC	ForeScout NAC	RegEx	Yes

List of AlienApps Available in USM Anywhere (Continued)

Data Source	AlienApp	Log Format	Auto-discovered
FortiGate Single Sign-On	FortiGate Single Sign-On	RegEx	No
Fortinet FortiAnalyzer - Logstash	Fortinet FortiAnalyzer	JSON	Yes
Fortinet FortiClient	Fortinet FortiClient	Key-Value	Yes
Fortinet FortiClient CEF	Fortinet FortiClient	CEF	Yes
Fortinet FortiDDoS	Fortinet FortiDDoS	Key-Value	No
Fortinet FortiGate	Fortinet FortiGate	Key-Value	Yes
Fortinet FortiManager	Fortinet FortiManager	Key-Value	Yes
Fortinet FortiNAC	Fortinet FortiNAC	CSV	No
Fortinet FortiWAN	Fortinet FortiWAN	RegEx	No
Fortinet FortiWeb	Fortinet FortiWeb	Key-Value	Yes
Fortinet Menu Networks MC	Fortinet Menu Networks MC	RegEx	No
FreeRadius	FreeRADIUS	RegEx	Yes
FutureX Guardian	FutureX Guardian	Split	No
G Suite Audit	Google G Suite	JSON	No
G Suite Drive	Google G Suite	JSON	No
G Suite Mail	Google G Suite	JSON	No
GitHub	GitHub	JSON	No
GitLab	GitLab	RegEx	Yes
Google Cloud Audit	Google Cloud Audit	JSON	No
Google Cloud Firewall Logs	Google Cloud Firewall Logs	JSON	No
Google Cloud Kubernetes Engine	Google Cloud Kubernetes Engine	JSON	No
Google Cloud Platform - Compute Engine	Google Cloud Platform - Compute Engine	JSON	No

List of AlienApps Available in USM Anywhere (Continued)

Data Source	AlienApp	Log Format	Auto-discovered
Google Cloud Platform Audit	Google Cloud Platform Audit	JSON	No
Google Cloud VPC FlowLogs	Google Cloud VPC FlowLogs	JSON	No
Graphus	Graphus	JSON	Yes
GTA Firewall	GTA Firewall	Key-Value	No
GTB Technologies	GTB Technologies	CEF	Yes
H3C Switch	H3C Switch	RegEx	No
HAProxy	HAProxy	CSV	Yes
HelpSystems GoAnywhere	HelpSystems GoAnywhere	Key-Value	Yes
Heroku Dynos	Heroku Dynos	RegEx	No
HP Storage Area Network Switch	HP SAN Switch	RegEx	No
HP Switch	HP Switch	RegEx	No
HPE Integrated Lights Out	HPE Integrated Lights Out	RegEx	No
HPE MSM Controller	HPE MSM Controller	RegEx	No
HPE OfficeConnect	HPE OfficeConnect	RegEx	No
HPE StoreOnce	HPE StoreOnce	RegEx	Yes
Huawei NGFW	Huawei NGFW	Key-Value	No
IBM IHS	IBM IHS	RegEx	No
IBM Maximo	IBM Maximo	RegEx	Yes
IBM QRadar Network Security	IBM QRadar	LEEF	Yes
IBM QRadar WinCollect	IBM QRadar WinCollect	Key-Value	Yes
IBM Security Directory	IBM Security Directory	Key-Value	Yes
IBM Security Guardium	IBM Security Guardium	CEF	Yes
IBM Tivoli Access Manager WebSEAL	IBM Tivoli Access Manager WebSEAL	CSV	Yes

List of AlienApps Available in USM Anywhere (Continued)

Data Source	AlienApp	Log Format	Auto-discovered
iboss Cloud Platform	iboss Cloud Platform	JSON	No
Illumio Policy Compute Engine	Illumio Policy Compute Engine	RegEx	Yes
Illusive Networks Honeypot	Illusive Networks Honeypot	CEF	Yes
Imperva SecureSphere	Imperva SecureSphere	Key-Value	No
Imperva SecureSphere CEF	Imperva SecureSphere	CEF	Yes
Incapsula CEF	Incapsula	CEF	Yes
Infoblox Data Connector	Infoblox Data Connector	CEF	Yes
Infoblox DDI	Infoblox	RegEx	No
Infocyte	Infocyte	CEF	Yes
Ipswitch WS_FTP	Ipswitch	RegEx	No
Ironscales IronTraps	Ironscales IronTraps	CEF	Yes
JAMF Protect	JAMF Protect	JSON	No
Jenkins	Jenkins	RegEx	Yes
Jira API	Jira	JSON	No
JSCAPE MFT Server	JSCAPE MFT Server	CSV	No
JumpCloudAPI	JumpCloud	JSON	No
Juniper EX Series	Juniper EX Series	RegEx	Yes
Juniper MX Series	Juniper MX Series	RegEx	Yes
Juniper NetScreen ScreenOS	Juniper NetScreen ScreenOS	RegEx	No
Juniper NetScreen ScreenOS Traffic	Juniper NetScreen ScreenOS	Traffic Key-Value	Yes
Juniper Network Security Manager	Juniper Network Security	CSV	No
Juniper QFX Series	Juniper QFX Series	RegEx	No
Juniper Secure Access VPN	Juniper Secure Access VPN	RegEx	No

List of AlienApps Available in USM Anywhere (Continued)

Data Source	AlienApp	Log Format	Auto-discovered
Juniper SRX - Logstash	Juniper SRX	JSON	Yes
Juniper SRX Junos	Juniper SRX	RegEx	No
Kaspersky Security	Kaspersky Security Center	JSON	No
Kaspersky Security Center	Kaspersky Security Center	RegEx	Yes
Kaspersky Security Center CEF	Kaspersky Security Center	CEF	Yes
Kerio Connect	GFI Software Kerio Connect	RegEx	Yes
Keycloak	Keycloak	Key-Value	Yes
Keycloak JSON	Keycloak	JSON	Yes
Keyfactor Cloud PKlaaS	Keyfactor Cloud PKlaaS	RegEx	No
KeyFocus KFSensor	KeyFocus KFSensor	Key-Value	Yes
Kiteworks Accellion	Kiteworks Accellion	JSON	Yes
Lacework Cloud Security	Lacework Cloud Security	JSON	No
Libra Esva Email Security	Libra Esva Email Security	RegEx	No
Lightning ADC	A10 Networks Lightning ADC	RegEx	No
Linux Auditd	Linux Auditd	Fullmessage	Yes
Linux BIND	ISC Linux BIND	RegEx	Yes
Linux ClamAV	Linux ClamAV	Fullmessage	Yes
Linux CRON	Linux CRON	RegEx	Yes
Linux DHCP Client	Linux DHCP Client	RegEx	Yes
Linux DHCPD	Linux DHCPD	RegEx	Yes
Linux DNSMASQ	Linux DNSMASQ	RegEx	Yes
Linux IPTables	Linux IPTables	Key-Value	No
Linux Kernel	Linux Kernel	RegEx	Yes
Linux NXLog	Linux NXLog	JSON	Yes

List of AlienApps Available in USM Anywhere (Continued)

Data Source	AlienApp	Log Format	Auto-discovered
Linux Process	Linux Process	RegEx	Yes
Linux Services	Linux Services	RegEx	No
Linux SSH	Linux SSH	RegEx	Yes
Linux SUDO	Linux SUDO	RegEx	Yes
Linux Systemd	Linux Systemd	RegEx	Yes
Linux Useradd/Groupadd	Linux Useradd/Groupadd	RegEx	Yes
LogMeIn LastPass	LogMeIn LastPass	JSON	Yes
Lookout JSON	Lookout	JSON	No
Lookout	Lookout	Key-Value	Yes
Malwarebytes Breach Remediation	Malwarebytes Breach Remediation	CEF	Yes
Malwarebytes Endpoint Protection	Malwarebytes Endpoint Protection	CEF	Yes
Malwarebytes Endpoint Security	Malwarebytes Endpoint Security	JSON	Yes
Malwarebytes Management Console	Malwarebytes Management Console	CEF	Yes
ManageEngine ADAudit Plus	ManageEngine	Key-Value	Yes
ManageEngine Data Security	ManageEngine Data Security	Key-Value	No
ManageEngine PAM360	ManageEngine	RegEx	No
ManageEngine Password Manager Pro	ManageEngine Password Manager Pro	CSV	No
McAfee Database Security	McAfee Database Security	CEF	Yes
McAfee EPO	McAfee	JSON	No
McAfee EPO - Logstash	McAfee EPO Logstash	JSON	Yes

List of AlienApps Available in USM Anywhere (Continued)

Data Source	AlienApp	Log Format	Auto-discovered
McAfee Network Security Platform	McAfee Network Security Platform	RegEx	Yes
McAfee Web Gateway	McAfee Web Gateway	CEF	Yes
McAfee Web Gateway Cloud	McAfee Web Gateway Cloud	CSV	No
Medigate	Medigate	JSON	No
Microsoft Advanced Threat Analytics	Microsoft Advanced Threat Analytics	CEF	Yes
Microsoft Advanced Threat Protection CEF	Microsoft Advanced Threat Protection	CEF	Yes
Microsoft Advanced Threat Protection JSON	Azure Log Collection	JSON	No
Microsoft Azure Automation	Microsoft Azure Automation	JSON	Yes
Microsoft Azure Firewall	Microsoft Azure Firewall	JSON	Yes
Microsoft Azure Network Security Group	Microsoft Azure Network Security Group	JSON	Yes
Microsoft Cloud App Security	Microsoft Cloud App Security	CEF	Yes
Microsoft Defender for Cloud	Microsoft Defender for Cloud	CSV	No
Microsoft HTTP API 2.0 NXLog	Microsoft HTTP API 2.0 NXLog	CSV	Yes
Microsoft IIS 8.0+ Plugin	Microsoft IIS	Pre-8.0 CSV	No
Microsoft IIS pre-8.0 Plugin	Microsoft IIS	8.0+ CSV	No
Microsoft IIS Regex	Microsoft IIS	RegEx	No
Microsoft Intune	Microsoft Intune	JSON	No
Microsoft OmiServer	Microsoft OmiServer	RegEx	Yes
MikroTik Router	MikroTik Router	RegEx	No
Mimecast	Mimecast	Key-Value	No
MNP LLP Web App	MNP LLP Web App	RegEx	No

List of AlienApps Available in USM Anywhere (Continued)

Data Source	AlienApp	Log Format	Auto-discovered
MobileIron Core	MobileIron Core	RegEx	No
MobileIron Threat Defense	MobileIron Threat Defense	JSON	No
ModSecurity Nginx	ModSecurity Nginx	RegEx	No
MySQL Community Edition	System Software MySQL Community Edition	RegEx	No
Nasuni Edge Appliance	Nasuni Edge Appliance	JSON	No
Nasuni Edge Appliance Audit	Nasuni Edge Appliance Audit	RegEx	Yes
NetApp Hybrid-Flash Storage System	NetApp Hybrid-Flash Storage System	RegEx	No
Netgate	Linux Netgate	Key-Value	Yes
Netgear Access Point	Netgear Access Point	RegEx	No
Netgear Firewall	Netgear Firewall	RegEx	No
Netgear Switch	Netgear Switch	RegEx	No
NetMotion Mobility Server	NetMotion Mobility Server	RegEx	No
Netskope	Netskope	JSON	No
Netskope CEF	Netskope	CEF	Yes
Netskope - Logstash	Netskope	JSON	Yes
Netwrix Auditor NXLog	Netwrix Auditor	JSON	Yes
NGINX	NGINX	CLF	Yes
NGINX Error	NGINX Error	RegEx	Yes
NGINX NAXSI	NBS NGINX NAXSI	RegEx	Yes
Nimble Storage	Nimble Storage	RegEx	Yes
NLnet Labs Unbound	NLnet Labs Unbound	Split	Yes
Northwave Gateway	Northwave Gateway	Key-Value	No
ObserveIT	ObserveIT	CEF	Yes

List of AlienApps Available in USM Anywhere (Continued)

Data Source	AlienApp	Log Format	Auto-discovered
Office 365 Audit	Microsoft Office 365 Audit	JSON	No
Office 365 Azure AD	Microsoft Office 365 Azure AD	JSON	No
Office 365 Exchange	Microsoft Office 365 Exchange	JSON	No
Office 365 SharePoint	Microsoft Office 365 SharePoint	JSON	No
Office 365 SharePoint NXLog	Office 365 SharePoint NXLog	JSON	Yes
Okta	Okta	JSON	No
Olfeo Proxy	Olfeo Proxy	RegEx	Yes
OneLogin	OneLogin	Key-Value	No
OpenGear Out-of-Band Management	OpenGear Out-of-Band Management	RegEx	No
OpenVPN Syslog	OpenVPN Technologies	RegEx	Yes
Oracle Audit Syslog	Oracle Audit Syslog	RegEx	Yes
Oracle BART	Oracle BART	RegEx	Yes
Oracle Cloud Infrastructure Audit	Oracle Cloud Infrastructure Audit	JSON	Yes
Oracle DB	Oracle DB	JSON	No
Oracle MySQL Enterprise	Oracle MySQL Enterprise	JSON	Yes
Oracle Unified Audit Trail	Oracle Unified Audit Trail	CEF	Yes
Osquery	Osquery	JSON	Yes
Osquery Error	Osquery Error	Key-Value	Yes
OSSEC Daemon	Trend Micro OSSEC Daemon	RegEx	Yes
OSSEC JSON	Trend Micro OSSEC	JSON	Yes
OSSEC v2.5	Trend Micro OSSEC	Key-Value	Yes
PA File Sight	Power Admin PA File Sight	RegEx	No
Packet Viper	Packet Viper	Key-Value	No

List of AlienApps Available in USM Anywhere (Continued)

Data Source	AlienApp	Log Format	Auto-discovered
PacketFence	Inverse PacketFence	RegEx	No
Palo Alto Cortex Data Lake	Palo Alto Cortex Data Lake	CEF	Yes
Palo Alto Cortex XDR	Palo Alto Cortex XDR	CEF	Yes
Palo Alto Networks CloudGenix ION	Palo Alto Networks CloudGenix ION	CSV	Yes
Palo Alto Traps	Palo Alto Networks Traps	CEF	Yes
Palo Alto Traps Management Service	Palo Alto Networks Traps Management	CSV	Yes
Palo Alto PAN-OS	Palo Alto Networks PAN-OS	CSV	Yes
Palo Alto PAN-OS - Logstash	Palo Alto Networks PAN-OS	JSON	Yes
Palo Alto PAN-OS CEF	Palo Alto Networks PAN-OS	CEF	Yes
Panda SIEM Feeder	Panda SIEM Feeder	Key-Value	Yes
Passwordstate	Click Studios Passwordstate	CSV	No
Passwordstate Syslog	Click Studios Passwordstate Syslog	RegEx	No
Percona Audit Log	Percona Audit Log	JSON	Yes
Perimeter81	Perimeter81	RegEx	Yes
pfSense Filter	pfSense Filter	CSV	Yes
pfSense System	pfSense System	RegEx	No
pfSense VPN	pfSense VPN	RegEx	Yes
phpIPAM	phpIPAM	RegEx	Yes
Pleasant Password Server	Pleasant Password Server	RegEx	Yes
Plixer Scrutinizer	Plixer Scrutinizer	JSON	Yes
Postfix	Postfix	RegEx	Yes
PostgreSQL	PostgreSQL	RegEx	No

List of AlienApps Available in USM Anywhere (Continued)

Data Source	AlienApp	Log Format	Auto-discovered
Power Admin PA File Sight	Power Admin PA File Sight	RegEx	No
Power Admin PA Sever Monitor	Power Admin PA Sever Monitor	JSON	Yes
PowerDNS	Open-XChange PowerDNS	RegEx	Yes
Preempt Security Behavioral Firewall	Preempt Security Behavioral Firewall	CEF	Yes
Preempt Security Behavioral Firewall - Logstash	Preempt Security Behavioral Firewall	JSON	Yes
ProFTPD	ProFTPD	RegEx	Yes
Proofpoint PhishAlarm	Proofpoint PhishAlarm	JSON	Yes
Proofpoint Targeted Attack Protection (TAP)	Proofpoint Targeted Attack Protection	Key-Value	No
Proofpoint Targeted Attack Protection - Logstash	Proofpoint Targeted Attack Protection	JSON	Yes
Proofpoint Targeted Attack Protection Syslog	Proofpoint Targeted Attack Protection Syslog	Key-Value	No
Proxmox Virtual Environment	Proxmox Virtual Environment	RegEx	Yes
PRTG Network Monitor	Paessler PRTG Network Monitor	RegEx	Yes
Pulse Connect Secure	Pulse Connect Secure	RegEx	Yes
Pure-FTPd	Pure-FTPd	RegEx	Yes
Qnap NAS	Qnap NAS	RegEx	Yes
Radware AppWall	Radware Cloud Services	Key-Value	No
Radware Cloud Services	Radware Cloud Services	Key-Value	No
Radware Defense Pro	Radware Defense Pro	RegEx	No
Raritan Dominion KX II KVM	Raritan Dominion KX II KVM	RegEx	No
Red Hat Ansible	Red Hat Ansible	Key-Value	Yes
Red Hat Directory Server	Red Hat Directory Server	RegEx	Yes

List of AlienApps Available in USM Anywhere (Continued)

Data Source	AlienApp	Log Format	Auto-discovered
Red Hat Single Sign-On	Red Hat Single Sign-On	RegEx	Yes
Red Hat WildFly	Red Hat WildFly	JSON	No
Riverbed SteelCentral	Riverbed SteelCentral	RegEx	No
Riverbed SteelConnect	Riverbed SteelConnect	RegEx	No
Riverbed STM	Riverbed STM	CLF	No
Route 53 DNS Queries	AWS Route 53 DNS Queries	CSV	No
RSA Authentication Manager	RSA Authentication Manager	CSV	No
Ruckus SmartCell Gateway	Ruckus SmartCell Gateway	Key-Value	No
Ruckus Virtual SmartZone	Ruckus Virtual SmartZone	RegEx	No
Ruckus Wireless ZoneDirector	Ruckus Wireless ZoneDirector	RegEx	No
Rumble Network Discovery	Rumble Network Discovery	Key-Value	Yes
Salesforce Activity	Salesforce	JSON	No
Salesforce LoginHistory	Salesforce	JSON	No
Salesforce Mulesoft	Salesforce Mulesoft	JSON	No
Salesforce SetupAuditTrail	Salesforce SetupAuditTrail	JSON	No
Samba	Samba	Split	Yes
Sangfor Next-Generation Firewall	Sangfor Next-Generation Firewall	Key-Value	Yes
SAST Security Radar	SAST Security Radar	CEF	Yes
SecureAuth	SecureAuth	XML	Yes
SEL-3620	SEL-3620	RegEx	No
SEL RTAC	SEL RTAC	CSV	Yes
SendMail	SendMail	Key-Value	Yes
SentinelOne	SentinelOne Syslog	CEF	Yes

List of AlienApps Available in USM Anywhere (Continued)

Data Source	AlienApp	Log Format	Auto-discovered
SentinelOneAPI	SentinelOne	JSON	No
SentinelOneSTAR	SentinelOne	JSON	No
SentryWire Packet Capture	Alliance SentryWire Packet Capture	RegEx	Yes
ServerAccess	AWS ServerAccess	CSV	No
ServiceNow API	ServiceNow	JSON	No
Shrubbery Tacacs	Shrubbery Networks Tacacs	RegEx	No
Signal Sciences Cloud WAF	Signal Sciences Cloud WAF	JSON	No
Silver Peak Unity Orchestrator	Silver Peak Unity Orchestrator	Key-Value	No
Silver Peak Unity Orchestrator RegEx	Silver Peak Unity Orchestrator	RegEx	No
Silver Peak WAN Optimization	Silver Peak WAN Optimization	RegEx	No
SinfoniaRx RxCompanion	SinfoniaRx RxCompanion	RegEx	Yes
Slack	Slack	JSON	No
Slapd	OpenLDAP Slapd	RegEx	Yes
Smoothwall Express	Smoothwall Express	RegEx	No
Snort Syslog	Cisco Snort	RegEx	Yes
Snowflake	Snowflake Snowflake	JSON	No
SoftEther VPN	SoftEther VPN	RegEx	No
SonicWall SSL VPN	SonicWall SSL VPN	Key-Value	Yes
Sophos Central	Sophos	CEF	Yes
Sophos Central JSON	Sophos	JSON	No
Sophos Cyberoam	Sophos Cyberoam	Key-Value	No
Sophos Email Appliance	Sophos Email Appliance	RegEx	No
Sophos Enterprise Console	Sophos Enterprise Console	Key-Value	Yes

List of AlienApps Available in USM Anywhere (Continued)

Data Source	AlienApp	Log Format	Auto-discovered
Sophos UTM	Sophos UTM	Key-Value	No
Sophos UTM & UTM VPN - Logstash	Sophos UTM & UTM VPN	JSON	Yes
Sophos UTM WAF	Sophos UTM WAF	RegEx	Yes
Sophos Web Security	Sophos Web Security	Key-Value	Yes
Sophos XG	Sophos XG	Key-Value	Yes
SourceFire IDS	Cisco SourceFire IDS	RegEx	No
South River Technologies Titan FTP Server	South River Technologies Titan FTP Server	W3C	No
SpyCloud API	SpyCloud Dark Web Monitoring	JSON	No
Squid	Squid	RegEx	Yes
SSH.COM PrivX	SSH.COM PrivX	JSON	No
STEALTHbits File Activity Monitor	STEALTHbits	CEF	Yes
Stormshield SN	Stormshield SN	Key-Value	No
StrongSwan VPN	StrongSwan VPN	RegEx	Yes
SWIFT NXLog	SWIFT NXLog	JSON	Yes
Symantec ATP	Symantec ATP	CEF	Yes
Symantec DLP	Symantec DLP	CEF	Yes
Symantec Encryption	Symantec Encryption	RegEx	No
Symantec Endpoint Threat Defense for Active Directory	Symantec Endpoint Threat Defense for Active Directory	Key-Value	Yes
Symantec EPM	Symantec EPM	RegEx	No
Syncplify.me	Syncplify	RegEx	No
Synology NAS	Synology NAS	RegEx	No

List of AlienApps Available in USM Anywhere (Continued)

Data Source	AlienApp	Log Format	Auto-discovered
Tanium Threat Response	Tanium Threat Response	JSON	No
Tenable Nessus Network Monitor	Tenable Nessus Network Monitor	Split	Yes
Tenable Tenable.io	Tenable Tenable.io	JSON	No
Tesserent Next Gen Firewall	Tesserent Next Gen Firewall	Key-Value	No
Thinkst Canary	Thinkst Canary	Key-Value	Yes
Thycotic Secret Server	Thycotic Secret Server	CEF	Yes
Trend Micro Control Manager	Trend Micro Control Manager	Key-Value	Yes
Trend Micro Control Manager CEF	Trend Micro Apex Central	CEF	Yes
Trend Micro Deep Discovery Inspector	Trend Micro Deep Discovery Inspector	CEF	Yes
Trend Micro Deep Security	Trend Micro Deep Security	CEF	Yes
Trend Micro InterScan	Trend Micro InterScan Messaging Security Virtual Appliance	RegEx	No
Trend Micro InterScan Web Security Virtual Appliance	Trend Micro InterScan Web Security Virtual Appliance	RegEx	No
Trend Micro TippingPoint	Trend Micro TippingPoint	RegEx	No
Trend Micro TippingPoint CEF	Trend Micro TippingPoint	CEF	Yes
Trend Micro Vulnerability Protection	Trend Micro Vulnerability Protection	CEF	Yes
Trend Micro Worry-Free Business Security Services	Trend Micro Worry-Free Business Security Services	Key-Value	Yes
Trustwave ModSecurity	Trustwave ModSecurity	Key-Value	No
Trustwave Secure Web Gateway	Trustwave Secure Web Gateway	RegEx	Yes

List of AlienApps Available in USM Anywhere (Continued)

Data Source	AlienApp	Log Format	Auto-discovered
Trustwave Secure Web Gateway Traffic	Trustwave Secure Web Gateway	Key-Value	Yes
Twistlock	Twistlock	Key-Value	Yes
Ubiquiti airMAX CPE	Ubiquiti airMAX CPE	RegEx	No
Ubiquiti EdgeRouter	Ubiquiti EdgeRouter	RegEx	No
Ubiquiti Unifi	Ubiquiti Unifi	RegEx	No
UFW	Linux UFW	Key-Value	Yes
Untangle NGFW	Untangle NGFW	JSON	No
User and Entity Behavior Analytics	User and Entity Behavior Analytics	JSON	Yes
Varonis DatAdvantage	Varonis DatAdvantage	CEF	Yes
Vectra	Vectra	CEF	Yes
VeloCloud VCO API	VeloCloud VCO API	Key-Value	Yes
Venafi Trust Protection Platform	Venafi Trust Protection Platform	JSON	No
Versa Director	Versa Director	RegEx	No
Versa FlexVNF	Versa FlexVNF	Key-Value	No
Virtual LoadMaster	KEMP Virtual LoadMaster	RegEx	No
VMRay Analyzer	VMRay Analyzer	CEF	Yes
VMware AirWatch	VMware AirWatch	RegEx	Yes
VMware ESXi	VMware ESXi	RegEx	No
VMware ESXi Agent Manager	VMware ESXi Agent Manager	CSV	No
VMware Horizon 7	VMware Horizon 7	Key-Value	No
VMware NSX	VMware NSX	RegEx	No
VMware SD-WAN by VeloCloud	VMware SD-WAN by VeloCloud	RegEx	Yes

List of AlienApps Available in USM Anywhere (Continued)

Data Source	AlienApp	Log Format	Auto-discovered
VMware SSO	VMware SSO	RegEx	No
VMware vCenter	VMware vCenter	RegEx	No
VMware vCenter Server Appliance	VMware vCenter Server Appliance	RegEx	No
VMware vRealize	VMware vRealize	RegEx	No
VMware vSAN	VMware vSAN	RegEx	No
VMware vShield	VMware vShield	Key-Value	No
VMwareAPI	VMware Sensor	JSON	No
Vormetric Data Security Manager	Vormetric Data Security Manager	CEF	Yes
Wallix Baston	Wallis Baston	Key-Value	No
Watchguard Firebox	Watchguard Firebox	RegEx	No
Watchguard Firebox - Logstash	Watchguard Firebox	Logstash	Yes
Watchguard XTM	Watchguard XTM	Key-Value	No
Wazuh	Wazuh	JSON	No
Webmin	Webmin	RegEx	No
Webroot FlowScape	Webroot FlowScape	CEF	Yes
Websense Email Security Gateway	Websense Email Security	CEF	Yes
Websense Web Security Gateway	Websense Web Security	Key-Value	No
Windows DHCP NXLog	Microsoft Windows DHCP NXLog	CSV	Yes
Windows DNS Server	Microsoft Windows DNS Server	RegEx	Yes
Windows Exchange NXLog	Microsoft Windows Exchange NXLog	JSON	Yes

List of AlienApps Available in USM Anywhere (Continued)

Data Source	AlienApp	Log Format	Auto-discovered
Windows Firewall NXLog	Microsoft Windows Firewall NXLog	JSON	Yes
Windows FTP Server NXLog	Microsoft Windows FTP Server NXLog	JSON	Yes
Windows IIS NXLog	Microsoft Windows IIS	NXLog JSON	Yes
Windows NPS NXLog	Microsoft Windows NPS NXLog	JSON	Yes
Windows NXLog	Microsoft Windows NXLog	JSON	Yes
Windows PowerShell NXLog	Microsoft Windows PowerShell NXLog	JSON	Yes
Windows SMTP NXLog	Microsoft Windows SMTP NXLog	JSON	Yes
Windows Snare	Microsoft Windows Snare	RegEx	No
Windows SQL NXLog	Microsoft Windows SQL NXLog	JSON	Yes
Windows Winlogbeat	Microsoft Windows Winlogbeat	JSON	Yes
Wireguard-go	Wireguard-go	RegEx	No
ZenDesk CRM	ZenDesk CRM	JSON	No
ZeroFOX	ZeroFOX	JSON	Yes
Zimbra Collaboration	Zimbra Collaboration	RegEx	No
Zimperium Mobile Device Security - zIPS	Zimperium Mobile Device Security - zIPS	JSON	No
ZingBox IoT Guardian	ZingBox	CEF	Yes
Zscaler NSS	Zscaler	CSV	No
Zscaler NSS Firewall Logs	Zscaler NSS Firewall Logs	CEF	Yes
Zscaler NSS Web Logs CEF	Zscaler NSS Web Logs	CEF	Yes
Zscaler ZPA	Zscaler ZPA	CSV	No
ZyXEL Wireless LAN Controller	ZyXEL Wireless LAN Controller	CEF	Yes
ZyXEL ZyWALL	ZyXEL ZyWALL	CEF	Yes