



ProVision Supported Vendor Technologies



Revised: October 30th, 2024

Version: 24.10.1

Classification: Public

Description: This document lists the supported technologies for the ProVision SIEM and should be used in conjunction with the Service Description located at <https://foresite.com/docs/sd/>. Use of Foresite services is subject to the Foresite Master Software License and Services Agreement available at: <https://foresite.com/docs/ma/>.

ProVision Portfolio	Monitor MA2	Manage MA3	Co-Manage MA4	Status	Ingestion Mode
Firewalls / Network & Security					
Palo Alto					
NGFW & VPN	Yes	Yes	Yes	Released	Syslog
NGFW Additional Functions	Yes	Yes	Yes	Released	Syslog
Prisma Access	Review	No	No	Review	Syslog(CEF)/API
Panorama	Yes	Yes	Yes	Released	Syslog
Fortinet					
FW & VPN	Yes	Yes	Yes	Released	Syslog
NGFW Additional Functions	Yes	Yes	Yes	Released	Syslog
FortiAnalyzer / FortiManager	Yes	Yes	Yes	Released	Syslog
FortiWeb	Yes	No	No	Parsing Only	Syslog
FortiClient (VPN)	Yes	No	No	Released	Syslog
SDWAN	Yes	No	No	Released	Syslog
CISCO					
ASA	Yes	Yes	Yes	Released	Syslog
Meraki (MX)	Yes	Yes	Yes	Released	Syslog
Meraki Switch	Yes	No	No	Released	Syslog
Meraki Access Points	Yes	No	No	Released	Syslog
Secure Firewall - FirePOWER / FTD	Yes	Yes	Yes	Released	Syslog
ASR / ISR (routing)	Yes	No	No	Released	Syslog
Catalyst/IOS (switching)	Yes	No	No	Released	Syslog
Nexus/XOS (switching)	Yes	No	No	Released	Syslog
WLC	Yes	No	No	Released	Syslog
Cisco Umbrella	Yes	No	No	Released	API
Cisco Netflow v9	Yes	No	No	Released	Syslog
Check Point					
NGFW & VPN	Yes	No	No	Released	Syslog(CEF)
Next Generation All Other Blades	Yes	No	No	On Req.	Syslog
SMB FW & IDS (700 Series)	No	No	No	Discontinued	Syslog
Juniper					
SRX	Yes	No	No	Released	Syslog
SSG	No	No	No	EOL	Syslog
SA / MAG (Pulse SSL VPN)	Yes	No	No	Released	Syslog
EX / MX (switching / routing)	Yes	No	No	Released	Syslog
Wireless (WLC)	Yes	No	No	Released	Syslog
Sonic Wall					
Firewall (TZ & NSA Series)	Yes	Yes	Yes	Released	Syslog
Sophos					
Firewall	Yes	No	No	Released	Syslog
WatchGuard					
FireBox (FW)	Yes	No	No	Released	Syslog

ProVision Portfolio	Monitor MA2	Manage MA3	Co-Manage MA4	Status	Ingestion Mode
Zscaler					
Zscaler ZIA	Yes	Yes	Yes	Released	Syslog(CEF)
Zscaler ZPA	No	No	No	On Req.	Syslog(CEF)
Zscaler ZDX	No	No	No	On Req.	Syslog(CEF)
Aruba					
Aruba Central	Yes	No	No	Released	API
Aruba Gateway	Yes	No	No	Released	API
ClearPass	Yes	No	No	Released	Syslog(CEF)
Airwave	Yes	No	No	Released	Syslog(CEF)
Mobility Master	Yes	No	No	Released	Syslog(CEF)
Aruba Wireless AP	Yes	No	No	Released	Syslog(CEF)
WLAN Controller	Yes	No	No	Released	Syslog(CEF)
Servers					
Windows Server	Yes	No	No	Released	Syslog (Winlogbeat)
Active Directory Server (Windows)	Yes	No	No	Released	Syslog (Winlogbeat)
Ubuntu	Yes	No	No	Released	Syslog
RHEL	Yes	No	No	Released	Syslog
Debian	Yes	No	No	Released	Syslog
Varonis DatAdvantage	Yes	No	No	Parsing Only	API
Standalone IDS					
SoureFire / Snort	Yes	No	No	Released	Syslog
EDR/AV - Anti-Virus					
Cylance	Yes	No	No	Released	API
CB Defense	Yes	Yes	Yes	Released	Syslog
SentinelOne	Yes	Yes	Yes	Released	API
Cisco Secure Endpoint- AMP	Yes	Yes	Yes	Released	API
Crowdstrike	Yes	Yes	Yes	Released	API
Eset	Yes	No	No	Released	Syslog(JSON)
McAfee EPO (On-Prem Only, not Cloud)	Yes	No	No	Released	Syslog(XML)
Palo Alto Cortex XDR	Yes	Yes	Yes	Released	Syslog(CEF)
Sophos Central	Yes	No	No	Released	API
Trend Micro Deep Security	Yes	No	No	Released	Syslog(CEF)
Windows Defender for Endpoint (E5 Licensing)	Yes	Yes	Yes	Released	API
Windows Defender Suite (P2 License)	Yes	No	No	Released	API
Webroot AV	Yes	No	No	Released	API
Authentication					
Duo	Yes	No	No	Released	API
Cisco TACACS	Yes	No	No	Released	Syslog
Cisco ISE (Identity Services Engine)	Yes	No	No	Released	Syslog
Microsoft MFA	Yes	No	No	Released	Syslog

ProVison Portfolio	Monitor MA2	Manage MA3	Co-Manage MA4	Status	Ingestion Mode
Auth0	Yes	No	No	Released	API
Okta	Yes	No	No	Released	API
SD-WAN					
VMWare VeloCloud	Yes	No	No	Released	Syslog
Versa Networks	Soon	No	No	On Req	Syslog
Palo Alto ION	Yes	No	No	Released	
Cisco Secure Firewall - Firepower SDWAN	Yes	No	No	Released	Syslog
Fortinet SDWAN	Yes	No	No	Released	Syslog
Hypervisors					
Vmware ESXi	Yes	No	No	Released	Syslog
VMWare vCenter	Yes	No	No	Released	Syslog
Nutanix	Yes	No	No	Released	Syslog
Load Balancers & Content Delivery					
Citrix Netscaler	Yes	No	No	Released	Syslog
F5 BIG-IP (LTM only)	Yes	No	No	Limited	Syslog
Cloudflare (Audit and WAF only)	Yes	No	No	Release	API
Managed Vulnerability Assessment					
ProVison Integrated solution	Yes	No	No	Released	N/A
Patch Management / Ivanti	Yes	No	No	Released	N/A
PAM / DNS / Access					
CyberArk PAM	Yes	No	No	Released	Syslog(CEF)
Infoblox	Yes	No	No	Released	Syslog
SecurEnvoy	Yes	No	No	Released	Syslog
Thycotic Secret Server	Yes	No	No	Parsing Only	Syslog
Cloud					
Azure AD	No	No	No	Roadmap	Tentative Q1-25
AWS	No	No	No	Roadmap	Tentative Q1-25
Google Cloud	No	No	No	Roadmap	Tentative Q1-25
Mail & Office Applications					
Office 365	Yes	No	No	Released	API
Barracuda Email Security	Yes	No	No	Released	Syslog
Proofpoint (SEG, TAP & TRAP)	Yes (TAP only)	Yes	Yes	Released	API. Only TAP monitored
SalesForce (B2C Commerce Platform)	Log fwd	No	No	Parsing Only	WebDAV

END.