PROFICIO®

INTEGRATIONS GUIDE

Supported Log Sources and Devices

ProSOC MDR, ProSOC MDR for Microsoft Sentinel, ProSOC MDR for Splunk

Endpoint Security Products

Crowdstrike Falcon
Cisco Secure Endpoint
CylancePROTECT
Kaspersky Endpoint Security
McAfee Endpoint Protection
Microsoft Defender XDR
Microsoft Defender for Endpoint
Cortex XDR
SentinelOne Singularity for Endpoint
Sophos Central
Symantec Endpoint Protection
Trend Micro Apex One
Trend Micro Deep Security Agent
Trend Micro OfficeScan
VMware Carbon Black Cloud Endpoint™ Standard
VMware Carbon Black EDR

Next Generation Firewall Solutions

Check Point
Cisco ASA
Cisco Firepower
Cisco Meraki
Fortinet
Juniper SRX
Palo Alto NGFW
SonicWall
Sophos XG
WatchGuard

Web Application Firewalls

Cloudflare
F5
Imperva
Microsoft Defender for Cloud Apps
Reblaze

Intrusion Prevention / Detection Services

Check Point
Cisco Firepower
Cisco Meraki
Fortinet
Juniper IDP
McAfee NSM
Palo Alto

Vulnerability Scanning

Qualys
Nessus

Cloud Security

AWS CloudTrail
AWS GuardDuty
AWS VPC Flow
AWF WAF
Azure Firewall
GCP Projects
Microsoft Defender for Cloud

Content Filtering

Blue Coat
Check Point
Cisco Firepower
Cisco Meraki
Cisco Umbrella*
Fortinet FortiGuard
Juniper
McAfee Web Gateway
OpenDNS
Palo Alto
Websense
Zscaler NSSWeblog

*Requires Customer S3 Bucket

Email Security

Barracuda On Premise
Cisco IronPort Email Security Appliances
G Suite
McAfee Email Gateway On Premise
Microsoft Defender for Office 365
Mimecast
Office365
Proofpoint TAP

Identity Management

CyberArk
Duo
Microsoft Defender for Identity
Okta
Microsoft Entra ID Protection
OneLogin
RSA SecurID

PROFICIO®

INTEGRATIONS GUIDE

Supported Log Sources and Devices

Advanced Persistent Threat Analyzers

Cisco Stealthwatch
Darktrace
FireEye
FortiSandbox
Vectra AI

Network Access Control

Aruba ClearPass
Cisco ISE
Cisco ACS
Forescout

Virtual Private Networks (VPN)

Aventail
Check Point
Cisco
Cisco AnyConnect
Citrix NetScaler
Fortinet
Juniper
Palo Alto GlobalProtect
Pulse Secure

Domain Name Services

Infoblox
Windows

Networking Appliances

Cisco Router
Cisco Switch

Networking Wireless LAN Controllers

ADTRAN BlueSocket
Aruba
Cisco WLC

Workstation Operating Systems

Mac OS X
Windows

Windows Server Roles

Application Server
Database Server
Domain Controller
Domain Member

Server Operating Systems

AIX
BSD
CentOS
Debian
Fedora
HP-UX
Red Hat
Solaris
Ubuntu
Windows Servers

Specific Applications

Apache
Kiteworks
Broadcom CA Top Secret
IIS
Ipswitch MOVEit
LastPass
NGINX
Windows Application Logs

Specific Databases

Microsoft SQL Server
Oracle
PostgreSQL

SaaS Applications

Box
Menlo
Microsoft Defender for Cloud Apps
LastPass
Salesforce

Other Log Sources

F5 (Load Balancer)
KFSensor (Honeypot)
Microsoft Defender XDR
VMware ESXi
IBM Power Server i

PROFICIO®

INTEGRATIONS GUIDE

Supported Log Sources and Devices

Active Defense

Active Defense for Endpoint

Cisco Secure Endpoint
CrowdStrike
Microsoft Defender for Endpoint
SentinelOne
Trend Micro Apex One
VMware Carbon Black

Active Defense for Perimeter

AWS WAF
Check Point
Cisco ASA
Cisco Firepower
Fortinet FortiGate
Juniper SRX
Meraki
Microsoft Defender for Cloud
Palo Alto
SonicWall

Active Defense for Identity

Active Directory (on-premises)
Microsoft Entra ID
Okta

Managed Firewall

Check Point
Cisco ASA
Cisco Firepower
Fortinet FortiGate
Meraki
Palo Alto
SonicWall

Managed EDR

CrowdStrike
Cisco Secure Endpoint
Microsoft Defender for Endpoint
Sophos Intercept X
Trend Micro
VMware Carbon Black

Additional devices and log sources can be supported on request.