

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

Web Application Firewalls

Cloudflare	Microsoft Defender for
F5	Cloud Apps
Imperva	Reblaze

Intrusion Prevention / Detection Services

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

Vulnerability Scanning

Qualys
Nessus

Cloud Security

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

Content Filtering

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

*Requires Customer S3 Bucket

Email Security

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

Identity Management

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

Supported Log Sources and Devices

Advanced Persistent Threat Analyzers

Cisco Stealthwatch FortiSandbox
Darktrace Vectra AI
FireEye

Network Access Control

Aruba ClearPass Cisco ACS
Cisco ISE Forescout

Virtual Private Networks (VPN)

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

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 Domain Controller
Database Server Domain Member

Server Operating Systems

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

Specific Applications

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

Specific Databases

Microsoft SQL Server
Oracle
PostgreSQL

SaaS Applications

Box LastPass
Menlo Salesforce
Microsoft Defender for
Cloud Apps

Other Log Sources

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

Supported Log Sources and Devices

Active Defense

Active Defense for Endpoint

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

Active Defense for Identity

Active Directory (on-premises)
Microsoft Entra ID
Okta

Managed Firewall

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

Additional devices and log sources can be supported on request.



Proficio is an award-winning managed security services provider (MSSP) delivering 24/7 security monitoring and managed detection and response (MDR) services. Proficio has Security Operations Centers (SOCs) in San Diego, Singapore, and Barcelona where our security teams monitor security events, investigate suspicious behavior, and hunt for targeted attacks.

US | Headquarters
San Diego, CA

APAC
Singapore

EMEA
Barcelona, Spain

Copyright © 2024 Proficio, Inc. All rights reserved. ProSOC is a registered trademark of Proficio Inc. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Proficio assumes no responsibility for any inaccuracies in this document. Proficio reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Active Defense for Perimeter

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

Managed EDR

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

Ready To Get Started? Request a Demo

GET STARTED

proficio.com | info@proficio.com | +1 800.779.5042