

Service Overview

Your end users' machines and server infrastructure are top targets for modern day cyber-attacks. Attacks are happening every minute of every day regardless of organisation size, vertical or location. Active and consistent monitoring of your endpoint protection solution is a must to identify threats early.

With IT and Security teams under serious resource constraints HyperProtect provides an affordable and high integrity managed Advanced Endpoint (AEP). Our certified security staff assists in design, deployment, maintenance, and incident response for clients in addition to other security services clients typically have the SOC assist with. With HyperProtect managed AEP we can do more when security events are received including remediation of the event, root cause analysis, scope of breach detection and additional forensics.

More Than Just Anti-Virus

Anti-Virus on your endpoint is a core requirement but it is just the beginning. Modern day threats



and business demands require advanced detection engines for prevention of file and script-based threats. Additionally, efficient logging of all system activities for advanced forensics and threat hunting capabilities are an essential component.

Platform & Service Features

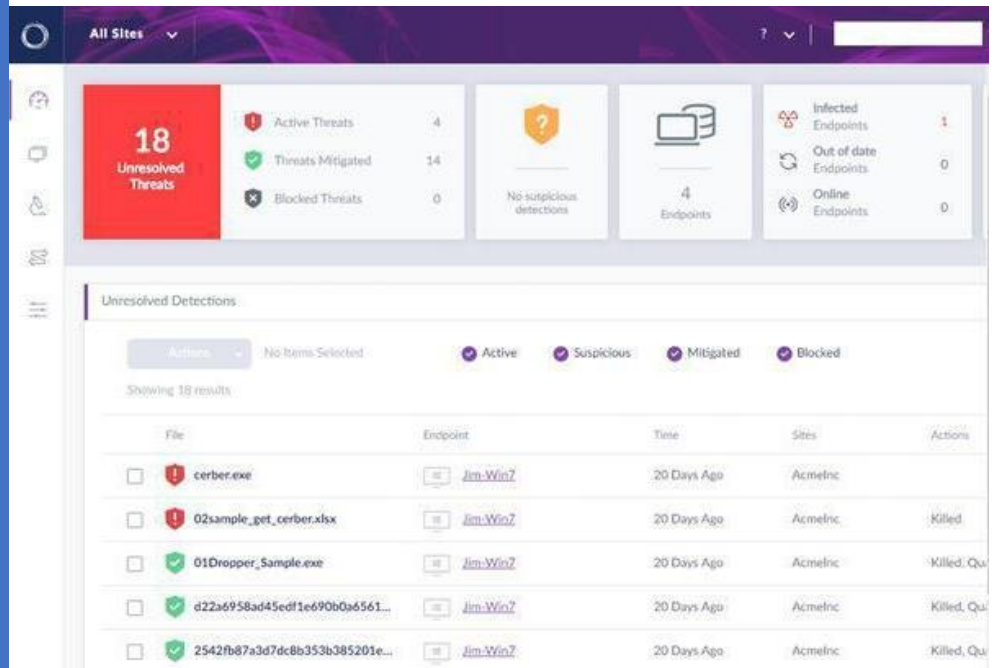
Platform & Service Features	Endpoint Detection Response (EDR)	Management	Service Features
Static AI	Threat Hunting	Device Control	Integrated with SOAR platform for extensible automation
Behaviour AI	IOC Search	API and SDK	24x7x365 Active SOC monitoring
Anti-Exploitation	Remediation	Application Inventory	Design, deployment, and maintenance resources
Lateral Movement	Encrypted Traffic Visibility	File Integrity Monitoring	Incident response and recommendations
Credential Theft Prevention	Containment and rollback	Vulnerability & Patch Management	Subject to SLA for predictable response

Shining a Light on Encrypted Traffic & Threats

With nearly 80% of enterprise web traffic encrypted and over 50% of modern malware threats leveraging encrypted traffic at some point in the process, having visibility and defence capabilities for encrypted traffic is an essential component of endpoint protection. If your current solution does not have the ability to inspect all encrypted communications, it is only a matter of time before a breach occurs.

\$1 Million Ransomware Guarantee per Infected Endpoint

HyperProtect ensures that both the policy settings and incident response procedure is executed and maintained to ensure that if a ransomware event does occur you are protected by Sentinel One's ransomware guarantee insurance policy.



Platform & Service Features

User Endpoint Clients	Server Endpoint Clients	Virtual Environments
Windows XP, 7, 8, 8.1, 10	Windows Server 2003, 2008, 2008 R2, 2012, 2012 R2, 2016 CentOS 6.5, 7.0, 7.2	Citrix XenApp
Mac OSX 10.9.x, 10.10.x, 10.11x, macOS 10.12x macOS 10.13 (High Sierra) CentOS 6.5, 7.0, 7.2	Red Hat Enterprise Linux 6.5, 7.0, 7.2 Ubuntu 12.04, 14.04, 16.04, 16.10	XenDesktop
Red Hat Enterprise Linux 6.5, 7.0, 7.2 Ubuntu 12.04, 14.04, 16.04, 16.10 openSUSE 42.2	SUSE Linux Enterprise Server 12SP1 Oracle Linux 6.5 - 6.9, 7.0+ Amazon Linux (AMI) 2016.09+, 2017.03+	Microsoft Hyper-V
		Oracle VirtualBox
		VMware vSphere
		VMware Workstation
		VMware Fusion
		VMware Horizon