SentinelOne

MONSTER CONNECT

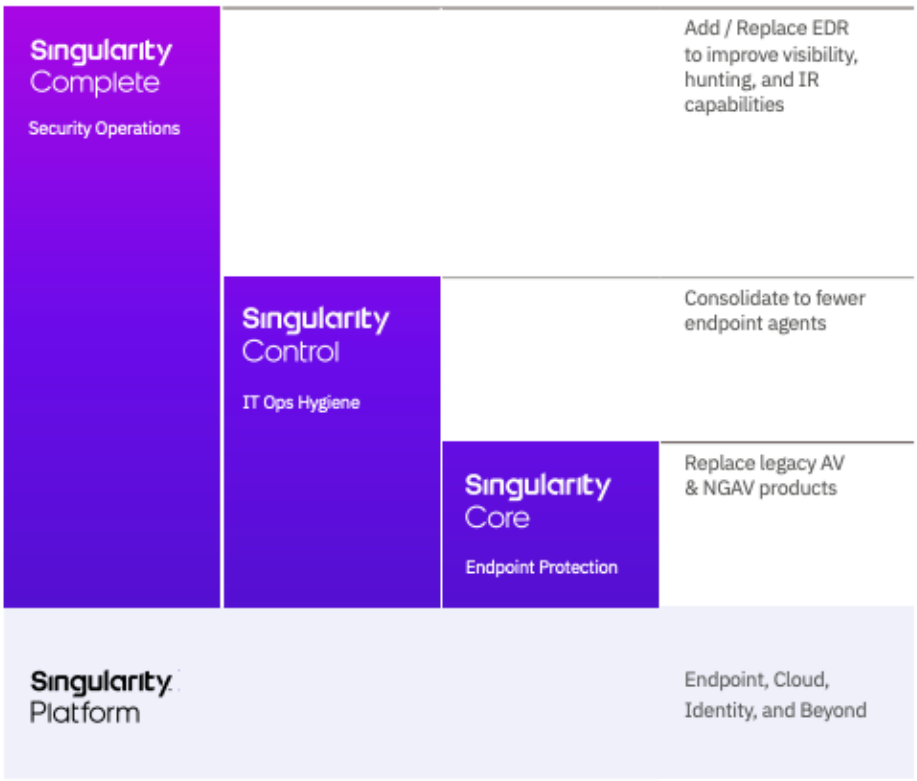
SentinelOne Singularity™

แพลตฟอร์ม โมดูล และบริการความปลอดภัยที่ครอบคลุม

SentinelOne Singularity : Platform ที่จะช่วยให้ทีม SOC และ ทีม IT Operation ปกป้องข้อมูลข้อมูลที่มีค่าขององค์กรจากภัยคุกคามที่มีความซับซ้อนในปัจจุบันอย่างมีประสิทธิภาพมากยิ่งขึ้น

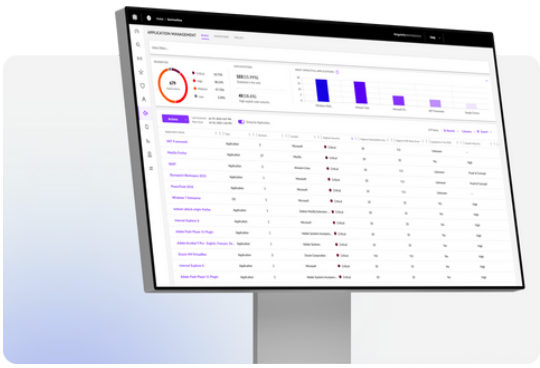
SentinelOne Singularity เป็นแพลตฟอร์มด้าน Cybersecurity ที่ ครอบคลุม ครบวงจร ช่วยให้ทีม SOC และ IT Operation สามารถมองเห็นภาพรวมของความเสี่ยงขององค์กรได้อย่างครบถ้วนและมีประสิทธิภาพมากยิ่งขึ้น SentinelOne Singularity ใช้ AI (Artificial intelligence)ในการวิเคราะห์ข้อมูลจาก Endpoint, Cloud workload, Network, identity และอุปกรณ์มือถือ เพื่อตรวจจับ ป้องกัน และตอบสนองภัยคุกคามได้อย่างรวดเร็วและแม่นยำ

SentinelOne Agents สามารถจัดการผ่านคอนโซล SaaS ของผู้เช่าหลายรายที่มีให้บริการทั่วโลก ออกแบบให้ใช้งาน จัดการได้ง่ายตามความต้องการ นอกจากนี้ยังมีบริการ Managed Detection & Response (MDR) จาก Monsterconnect เป็นบริการที่คอยตรวจจับและตอบสนองภัยคุกคามให้กับองค์กรตลอด 24 ชั่วโมง 7 วันต่อสัปดาห์



ทำไมต้องเลือก SentinelOne ?

- เพราะ SentinelOne นั้นดีที่สุดทั้งในด้านที่เป็น EPP+EDR
- 95% ของลูกค้าพึงพอใจ
- 96% ของผู้รีวิว Gartner Peer Insights แนะนำ SentinelOne
- คอนโซลที่ปรับแต่งได้ พร้อมworkfolwที่ช่วยประหยัดเวลา
- แก้ปัญหา ransomware ได้ด้วย AI ที่เหนือขั้น
- การตอบสนอง ป้องกันอัตโนมัติ เริ่มทำงานทันที
- ประหยัดเวลา ลดการทำงานหนักด้วย “Storyline” แพลตฟอร์มที่ออกแบบมาเพื่อผู้ที่ต้องเฝ้าระวังเหตุต่างๆ รวมไปถึงผู้ที่ทำการป้องกันภัยคุกคามในเชิงรุก
- มีการเก็บรักษาข้อมูล Event ต่างๆนานถึง 365 วัน สำหรับนำไปใช้วิเคราะห์ต่างๆ
- สามารถใช้งาน XDR กับ Vendor อื่นได้อย่างง่ายดาย

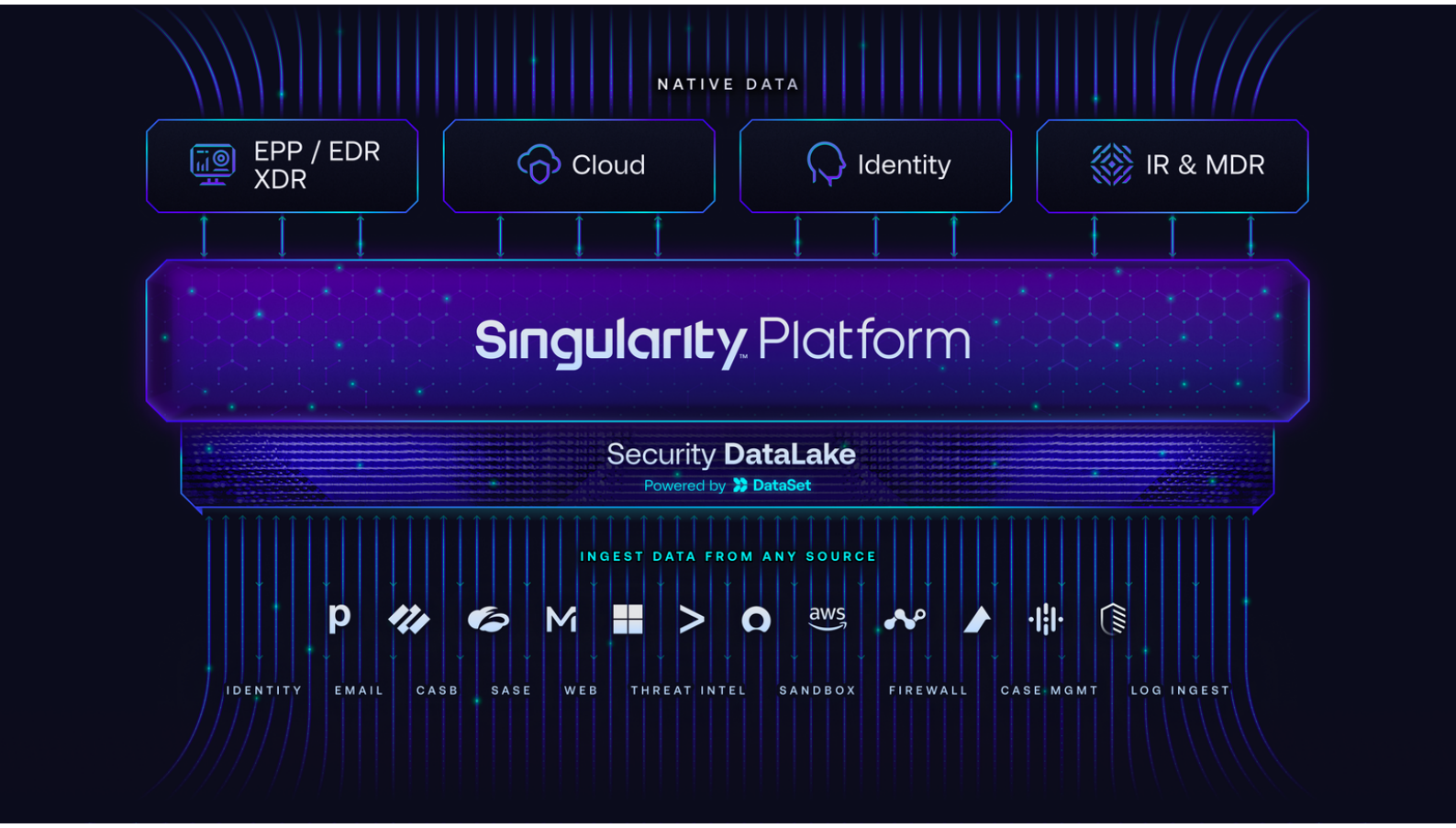


สอบถามเพิ่มเติม LINE: @monsterconnect Email: sales@mon.co.th โทร .02-026-6664

แพลตฟอร์ม Singularity ของ SentinelOne มีคุณสมบัติและข้อเสนอมากมาย

ลูกค้า SentinelOne ทุกคนสามารถเข้าถึงคุณสมบัติคอนโซลการจัดการ SaaS เหล่านี้ได้

- SentinelOne เป็น SaaS แบบ Global , High available สามารถเลือกใช้ Server ตามพื้นที่ ที่คุณต้องการ (US, EU, APAC)
- มีระบบ Authentication สำหรับ Admin หลากหลายรูปแบบ : SSO, MFA, RBAC
- ระบบ Administration ที่ปรับแต่งได้ให้เข้ากับโครงสร้างขององค์กร
- เก็บประวัติเหตุการณ์ภัยคุกคามนานถึง 3 ปี
- Single API มาพร้อมฟังก์ชันมากกว่า 340 ฟังก์ชัน
- รวมระบบ Threat intelligece กับ MITRE ATT&CK เข้าด้วยกันเพื่อบ่งชี้ รูปแบบ, ขั้นตอน ของภัยคุกคาม
- ขับเคลื่อนการทำงานด้วยข้อมูลที่เป็น Dashboard สำหรับการวิเคราะห์ด้าน Security
- สามารถตั้งต่าให้แจ้งเตือนด้วย E-mail และ syslog
- Singularity Marketplace ecosystem ใช้ร่วมกับแอปพลิเคชันอื่นๆได้ด้วยเพียง คลิกเดียว



องค์กรชั้นนำระดับโลกไว้วางใจ SentinelOne

SAMSUNG · EA · HITACHI Inspire the Next · AUTODESK · ASTON MARTIN · Sysco · NAVER · flex · POLITICO

Recommend Edition

Platform Features

	Singularity Core Cloud-Native NGAV	Singularity Control Security + Suite Features	Singularity Complete Enterprise Security
Singularity™ Platform Common Features			
Cloud-first multi-tenant SaaS	✓	✓	✓
Fully customizable management experience via multi-site, multi-group architecture	✓	✓	✓
Fully customizable role-based access control and MFA integration	✓	✓	✓
Patented Storyline™ correlation & context	✓	✓	✓
Skylight platform data analytics interface			✓
MITRE ATT&CK® Integration	✓	✓	✓
Data localization	Available	Available	Available
Singularity XDR Features			
Native data ingestion from SentinelOne surface agents (endpoint, cloud, identity, mobile, etc.) – Unmetered and does not decrement the Open XDR ingest quota.	✓	✓	✓
Open XDR data ingestion of 10 GB/day from any external, non-native, non-SentinelOne source. Upgradable to multi-terabyte/day.		✓	✓
Ingested data retention includes both Open XDR & Native data. 14 days default. Upgradable to 3 years.			✓
Singularity XDR Marketplace Apps		✓	✓
Storyline Active Response™ (STAR) Custom Detection Rules. 100 default. Upgradable.		Open XDR data only	✓
ENDPOINT SURFACES			
Endpoint security for Windows Workstation, macOS, and legacy Windows (XP, 7, 2003SP2+, 2008)	✓	✓	✓
Modern endpoint protection & NGAV utilizing static AI & behavioral AI	✓	✓	✓
Automated or one-click remediation & rollback	✓	✓	✓
Threat triage & investigation: 1 year lookback	✓	✓	✓
Rogue & unsecured device discovery. Requires Ranger Module for remote installation and other network functions.	✓	✓	✓
Mobile endpoint support: iOS, Android, Chrome OS	+	+	+
EPP Suite Control Features: Device Control, Firewall Control, Remote Shell		✓	✓
Application inventory and application CVEs		✓	✓
Built-in data collection scripts			✓
Native EDR data ingestion with Storyline™ and MITRE Engenuity ATT&CK® Mapping			✓
Native EDR threat hunting via Skylight			✓
Native EDR analytics			✓

Legend: ✓ Supported + Optional

Recommend Edition

Platform Features

	Singularity Core Cloud-Native NGAV	Singularity Control Security + Suite Features	Singularity Complete Enterprise Security
CLOUD SURFACES			
Realtime Cloud Workload Security for Linux VMs, Kubernetes clusters and Windows servers & VMs		✓	✓
Automated or one-click remediation & rollback. Remote shell.		✓	✓
Threat triage & investigation: 1 year lookback		✓	✓
Cloud service provider workload metadata sync		✓	✓
Automated App Control for Kubernetes and Linux VMs		✓	✓
Built-in data collection scripts			✓
Native EDR data ingestion with Storyline™ and MITRE Engenuity ATT&CK® Mapping			✓
Native EDR threat hunting via Skylight			✓
Native EDR analytics			✓
IDENTITY SURFACE			
Singularity Ranger AD Module: Real-time Active Directory and Azure AD attack surface monitoring and reduction.	+	+	+
Singularity Ranger AD Protect Module: Real-time Active Directory and Azure AD attack surface monitoring and reduction further supplemented with AD domain controller-based Identity Threat Detection and Response.	+	+	+
Singularity Identity Module: Identity Threat Detection & Response for Active Directory and Azure AD and AD domain-joined endpoints.	+	+	+
Singularity Hologram Module: Network-based threat deception that lures in-network and insider threat actors into engaging and revealing themselves.	+	+	+
PLATFORM MODULE OPTIONS			
Singularity Ranger® Attack Surface Management Module: Asset discovery, fingerprinting, and inventory. Automated agent deployment. Suspicious device isolation. Pivot to Skylight threat hunting.		+	+
RemoteOps Module: Orchestrated forensics, remote investigation, and rapid response at scale.			+
Cloud Funnel Data Lake Streaming Module: Replicate telemetry to any cloud for any purpose.			+
Binary Vault Module: Automated malicious and benign file upload for additional forensic analysis.			+

Legend: ✓ Supported + Optional

Service & Support

Recommend Edition

	Singularity Core	Singularity Control	Singularity Complete
Standard Support 5/9	✓	✓	✓
Enterprise Support 24/7/365	+	+	+
Enterprise Support + Technical Account Manager	+	+	+
SentinelOne Guided Onboarding ("GO") deployment service	+	+	+
Vigilance Respond Managed Detection & Response (MDR) subscription	Limited	Limited	+
Vigilance Respond Pro MDR + Digital Forensics & Incident Response (DFIR) subscription	Limited	Limited	+
WatchTower Active campaign threat hunting & intelligence reporting	+	+	+
WatchTower Pro Bespoke threat hunting & compromise assessment	+	+	+
Vigilance IR Retainer	+	+	+

Legend: ✓ Supported + Optional

Operating System Coverage

Windows + Legacy OSes

- Windows Server Core: 2022, 2019, 2016, 2012
- Windows Server 2003 SP2 or later, or R2 SP2 or later
- Windows: 11, 10, 8.1, 8, 7 SP1+ / 10 IoT Enterprise
- Windows Server: 2022, 2019, 2016, 2012 R2, 2012, 2008 R2 SP1
- Windows Storage Server: 2016, 2012 R2, 2012
- Windows "Legacy": XP SP3+, 2003, 2008
- Windows Embedded POSReady 2009

macOS

- macOS Ventura
- macOS Monterey
- macOS Big Sur

Linux Distributions

- Ubuntu 14.04, 16.04, 18.04, 19.04, 19.10,20.04, 22.04
- RHEL 6.4+, 7.0-7.9, 8.0-8.7, 9.0, 9.1
- CentOS 6.4+, 7.0-7.9, 8.0-8.4
- Oracle 6.9, 6.10, 7.0-7.9, 8.0-8.7, 9.0
- Amazon Linux 2, AMI 2018, AMI 2017
- SUSE Linux Enterprise Server 12.x, 15.x
- Fedora 25-30, 31 (kernel 5.5+) 32-36
- Debian 8, 9, 10, 11
- Virtuozzo 7
- Scientific Linux 6, 7
- RockyLinux 8.4, 8.5, 8.6, 8.7,9.0
- AlmaLinux 8.4, 8.5, 8.6,8.7, 9.0

Kubernetes &Container Runtimes

- Kubernetes v1.13+
- OpenShift 4.4 - 4.10
- Container Runtimes: Docker, containerd, cri-o
- Managed K8s Services: Amazon Elastic Kubernetes Service (EKS), Azure Kubernetes Service (AKS), Google Kubernetes Engine (GKE)
- Container Optimized Linux Distributions: Container-Optimized OS (Google), Red Hat Core OS (OpenShift), Flatcar Container Linux

Cloud Service Provider VMs

- Amazon EC2
- Azure VM
- Google Compute Engine

Virtualization/ VDI

- Citrix XenApp & XenDesktop
- Oracle VirtualBox
- VMware vSphere, Fusion, Horizon, Workstation
- Microsoft Hyper-V (requires the VHD file)

CONTACT ADDRESS

Monster Connect Co.,Ltd.
NASA STREET Building B, 99/1 Room L3-B02-B03, Floor 3rd,Ramkhamhaeng Road, Suan Luang Subdistrict, Suan Luang District, Bangkok 10250

Website : www.monsterconnect.co.th

Email : sales@mon.co.th