Synycs' SynOps Ai Empowered Complete Cloud Management Tool



Run ML/AI Or Any Type Of Workload With Optimal Performance And Infrastructure Cost

FinOps and Cost Management



Forecast And Monitor An IT Infrastructure Cost



Identify Wastage And Optimize IT Expenses



Bring Resource / Application / Service Observability



IT Asset Management



Set TTL And Budget Constraints



Establish A Longterm Finops Process By Engaging Engineering Teams

Supported Platforms:



Microsoft Azure



C-J Alibaba Cloud



SynOps Unique Features over CSP

Cloud Resource Visibility And filtering Across All The Clouds, Accounts And Regions

Dozens Of Optimization Scenarios Not Supported By Clouds Incl. One Of The Best Rightsizing Engines

Cost Allocation Not Just By Tags But Other Properties

Geo And Network Traffic Map

TTL Rules And Budget Constraints

Finops: SynOps Is Built For Engineers To Be Responsible For Their Cloud Resources





Automated Run Of Several Experiments With Configurable Datasets, Hyperparameter Ranges And Model Versions



Optimal Hardware With Cost-efficient Usage Of Spot, Reserved Instances / Saving Plans



Configurable Experiment Goals And Success Criteria



Various Complete/Abort Conditions - Take first Successful, Complete All



Runsets

Runset overview AWS GPU Instances / #3_gentle_sky



ML R&D with Status Observability



List Of Models With Goals Status And Active Recommendations.

L.		L

Tracking The Number And Quality Of Experiments Run By A Team.



Cost Of An Overall Model And Individual Experiments.



ML/AI Profiling & Optimization



ML/AI Model Training Tracking And Profiling, Inside And Outside Metrics Collection



CPU/RAM/GPU/Disk IO Correlation Tracking



You Can Reduce Cloud Costs For ML/AI By Using Reserved Instances/Saving Plans And Optimization Scenarios.

Supported platforms:







Utilizing Reserved/Spot Instances And Saving Plans

Rightsizing And Instance Family Migration

Detecting CPU, GPU, RAM And IO Bottlenecks

Cross-regional Traffic

Spark Executor Idle State

Experiment/Run Comparison

ML/AI Profiling & Optimization

Application overv Applications / Shoes cat	iew regorizer							PROFILING INTEGRATION	CONFIGURE
OVERVIEW EXECU	ITORS								
Aborted Status	1 minute, 5 s	econds	\$284.25 Lifetime cost	\$8.48k Summary savings	19 Recommendatio	ins count			
Tracked parameters a Accuracy: • 1 out of 0.98 Data Loss: • 5 out of 10 Inference time: • 0.15 ou Data processed: • 132 ou Recommendations	a ut of 0.2 ut of 150		Applica Key: sho Runs: 9 Last succ Last run Owner: 0	ition summary es_categorizer cessful run: 3 months cost: \$14 Charlie Fisher	s ago		Last run executor i-3920fedd Cloud: i AWS HQ Name: sunflower-eu Region: us-west-2 Size: t3a.medium	ı-fra-1	
Executors upgrade See details		11 Count	Cross-region traffic See details	\$8 Sav	8.48k s	Spot/Preemptible instances usage See details	3 Count	Local storage bottleneck See details	1 Count
GPU memory See details		1 Count							

ML/AI Profiling & Optimization



IT Environment Management

- Manage A List Of IT Environments, Their Health And Availability 娿
- Book IT Environments And Organize Shared Usage
- \checkmark Track Deploy History, Review Software Versions
- Resource Planning Via Jira, Slack Or SynOps UI
- Power Management And Cost Optimization
- **Environment Performance Monitoring** C71



Integrations:













Environment Access Management

Traditional Environment Access Management Flow Company infrastructure Environment . . . A standard password or a public key which is not removed after workload usage Get access to environment User User Environment Grant or revoke access requests Job/ script

Environment Access Management flow With SynOps

Simple SynOps Onboarding



Resource Sharing and Lifecycle Management

|--|

Resource Grouping And Ownership





Tag Policies And Resource Auto-assignment





Cloud cost transparency and optimization

Budgets And Resource Auto-assignment

Track Every BU, Team, User Or App Expense And Cost Anomaly Detection

Spike Identification And Instant Alerts With In-depth Cost Analysis

Budget And Resource Expense History

Budget Forecasts, Thresholds & Insights

Get Analytics, Forecast And Optimization Insights



Concerns that are addressed by SynOps

- Engineers Are Not Engaged In Cost-saving Processes.
- Getting A Long List Of Optimization Scenarios Does Not Help As A Few DevOps Or Central IT folks Cannot fix All The Optimization Issues Without Reaching Resource Owners Who Have Other Priorities.
- As A Result, Only 20-30% of 'Low-Hanging Fruit' Recommendations Are Implemented.
- No Resource Lifecycle Management.
- Cloud Cost Management Tools Don't Give A Way To Manage Resource Lifecycle Management.
- No Transparency And flexibility.
- Cloud-native Tools Do Not Provide Enough Granularity And Transparency Across Budgets, Teams, Clusters And Applications.

Spot Instance Price Variation

	,					
Your instance type requiment	ts, budget requiments, and appl	ication design will determine he	ow to apply the following best pro	actices for your application. To learn more, see	e Spot Instan	ce Best Practices
iraph			Instance type			Platform
Availability Zones		•	c3.large			Linux/UNIX
© 0.0-Demand price \$0.105 sep 12 2020, 02:47 \$0.105 Average hearly cat \$0.120 30:100 \$0.100 \$0.080 \$0.060 \$0.060	Us-east-1b (0.0294 Sep 12 2030, 02:47 (0.0294 Average hourly cast 72.00% Average savings	Us-east-1C \$0.0299 Sep 12 2020, 02:67 \$0.0294 Average hourly cast 72.00% Average solvings		Us-east-1e (0.0294 Sep 12 2020, 02.87 (0.0294 Average hearly cost. 72.00% Average savings		
\$0.040	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~					
\$0.020						
					,	

SynOps' Cyber Protection

Complete Cyber Protection Platform

SynOps Cyber Protect Cloud



SynOps Cyber Protect Cloud



* One Solution Integrates Backup, Disaster Recovery, Ai-based Protection Against Malware And Ransomware, Remote Desktop, And Security Tools In A Single Agent

Full-image and file-level backups

Back up individual files or safeguard an entire business with a few clicks

- File-level backup: Use this option to protect specific data, reduce the backup size, and save storage space
- Full-image backup: Easily back up the entire system as a single file, ensuring bare metal restores
- In the event of data disaster, you can easily restore all information to new hardware



Why? Ensure Business Continuity With Flexible Backup Options And Avoid Downtime And Data Loss.

Vulnerability Assessments

Discover Issues Before They Happen

- Windows, Macos, Linux Support
- Continuous Daily Updates To Our Own Vulnerability And Patch Management Database
- Comprehensive Dashboard For Vulnerability Detection, Severity Assessments, And Patch Availability
 racking

270+ Third-party Applications And All Microsoft Applications Supported

vuniciabilities					Ų V
🔀 Install patches					4 items selected
- Name	Affected products	Machines	Severity 🕇	Patches	
CVE-2018-209654	Chrome, Firefox	12	CRITICAL	-	
CVE-2018-1000016	Office 2010	3	нібн	2	
CVE-2018-1003	Acrobat Reader	3	нібн	2	
CVE-2018-100047	Flash Player for Chrome, Flash Pl	7	MEDIUM	-	
CVE-2018-3223	Windows Server 2016	14	LOW	1	
CVE-2018-9800	Office 365 Client	9	NONE	3	
CVE-2018-337894	Firefox	3	NONE	1	

Why? Mitigate Potential Threats And Prevent Attacks.

Patch management

Ensure Workload Protection

Large Common Vulnerabilities And Exposures Database, With 250–300 New Cves Weekly

- All Windows Updates Including Microsoft Office And Windows 10 Apps
- Support For Patch Management Of Microsoft And Third-party Software On Windows
- Pre-update Backups And Apply Latest Patches As Part The Recovery Process.
- Patch Priority Visibility Based On Vulnerability Severity
- Prioritized Patching For Collaboration Apps: Zoom, Skype, Microsoft Teams, Cisco Webex, Etc.
- Staged Deployment For Patch Testing

Sources: CVE Program, The MITRE Corporation



Why? Mitigate Potential Threats And Prevent Attacks (E.G., Equifax, Wannacry).

Device control

Strengthen your security services and minimize the risk of data leaks for clients with essential data loss prevention (DLP)

- Controlled channels (local workloads) Endpoints (Windows PC, workstation, server), ports, peripheral and redirected devices, clipboard, virtualized sessions
- Capabilities:
 - · Selective access control per device/port type (deny, allow, read-only)
 - · Real-time alerts and notifications
 - a) On workloads on/off for all devices and ports
 - b) In console on/off per device/port type
 - · Control clipboard copy/paste operations
 - · Control screenshot captures (PrintScreen and any third party app)
 - Support of encrypted removable media
 - Allowlisting
 - a) Device type
 - b) USB granular, down to serial number
 - c) Clipboard operations within applications

vent data leaks by limiting user	access to device types and interfaces.	
Show OS notification to end us	ers if they try to use a blocked device type or port	с
Devices	Allow all	Deny all
Туре	Access	
Removable	🔒 Read-only 👻 🗹 Send ale	n
Printers		
Clipboard	Peripheral device access is t	blocked Jan 28, 2021, 06:50 PM
Mobile devices	Access to Removable device on '	W10x64-20H2-SAMSON' is blocked
Bluetooth	Device	W10x64-20H2-SAMSON
Optical drives	Plan name	SAMSON-test
Elopov drives	Source	Removable device
noppy annes	Action	Read
Ports	Name	E:\desktop.ini
Туре	Information	
USB	User	Cyber Protect Monitor ×
FireWire	Process	Access is denied
	Allow this USB device	You are not allowed to send F:\Sleep
Redirected devices ()		Away.mp3 to Removable device.
Туре	Access	Ask your IT staff for help.
Mapped drives	Allowed	
Clipboard incoming	Allowed ¥	

Why? Proactively prevent data leaks and control data flows between devices and peripherals.

Multi-layered protection



Seven layers of protection against modern email-borne threat

*Anti-evasion: Recursively Unpacks Embedded Files And URLs into Their Components To Identify Hidden Malicious Content

**Anti-spoofing: Catch Any Impersonation Attempt Or BEC With A Machine Learning-based Technology That Inspects All Relevant Data And Metadata (IP Reputation, SPF, DKIM, And DMARC Record Checks; Text And Metadata Analysis; Scoring Of Senders; Other Algorithms) To Detect Spoofing Attempts Well Before They Reach The End-user

***Next-generation Dynamic Detection: Unique CPU-level Technology That Acts Earlier In The Attack Chain (At The Exploit Stage, Before Malware Release) By Analyzing The Execution Flow During Runtime By reading the assembly code, we can catch and stop advanced threats such as appointments and zero days.

Why? Block Modern Email-borne Threat Before It Reaches End Users

Synycs' SynOps is An Al Empowered Cloud Management Tool that brings:

Cost Effectiveness

Resource Utilization

Best Practices Adherence

EndPoint Protection

CyberSecurity Posture

Ease in Integrations