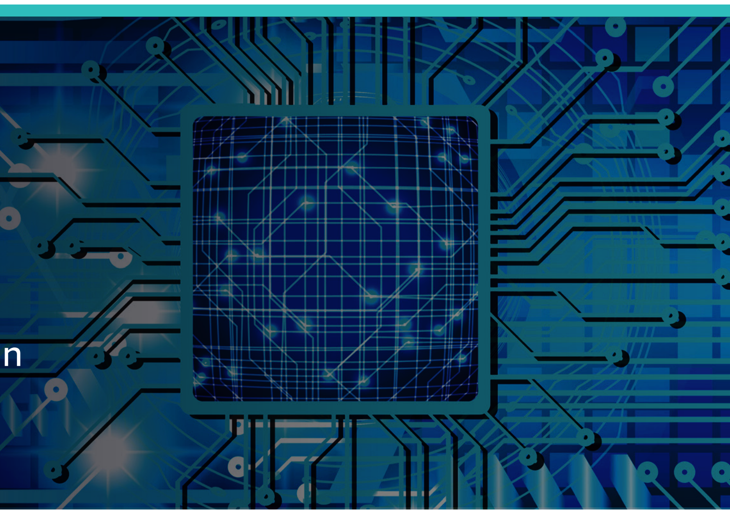


Cyware Security Orchestration Layer (CSOL)

A Universal Any-to-Any Security Orchestration Gateway

The ever-increasing complexity and variety of cybersecurity tools has resulted in analyst burnout and slowed threat response for organizations. Security operations teams are often burdened due to a large number of repetitive processes in their daily workflow. To counter this and improve the pace of threat response, organizations are adopting Cyware's security automation and orchestration platform as a means to automate their security operations leveraging security tools deployed across different environments.

Cyware Security Orchestration Layer (CSOL) is a universal and dedicated security orchestration gateway for executing on-demand or event-triggered tasks across deployment environments at machine speeds. CSOL allows security teams to create customized automation playbooks to execute various manual, repetitive tasks in a reliable machine-driven manner. CSOL enables machine-to-machine (M2M), human-to-machine (H2M), and machine-to-human (M2H) security orchestration through integrations with a wide range of deployed security tools and technologies.

CSOL helps organizations streamline and automate their security operations by enabling disparate tools and technologies to talk to each other without having to rely on any manual effort for data normalization, enrichment, and analysis. By deploying CSOL, organizations can significantly reduce mean time to respond (MTTR) and increase operational efficiency along with overall return on investment (ROI) in cybersecurity.

Capabilities and Benefits

Seamless Security Orchestration

- Cross-Environment Orchestration
- Custom Security Playbooks
- Flexible RESTful API
- Third-party Integrations
- Visual Playbook Editor
- On-Demand and Scheduled Orchestration

Process Automation and Standardization

- Automated Standard Security Processes
- Consistent Repeatable Results
- Fine-tuned Logical Workflows
- High Service Availability

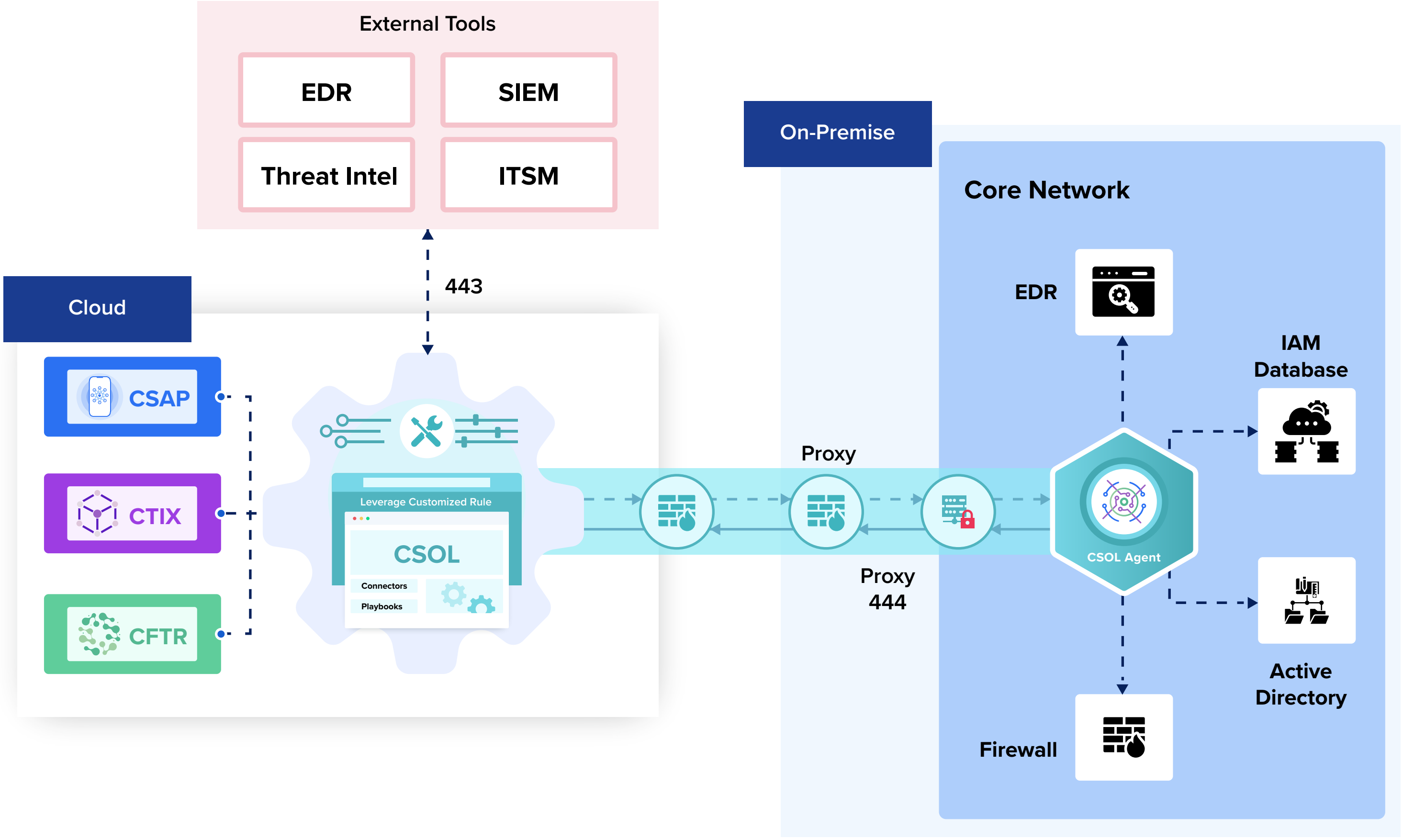
Save Time and Increase Efficiency

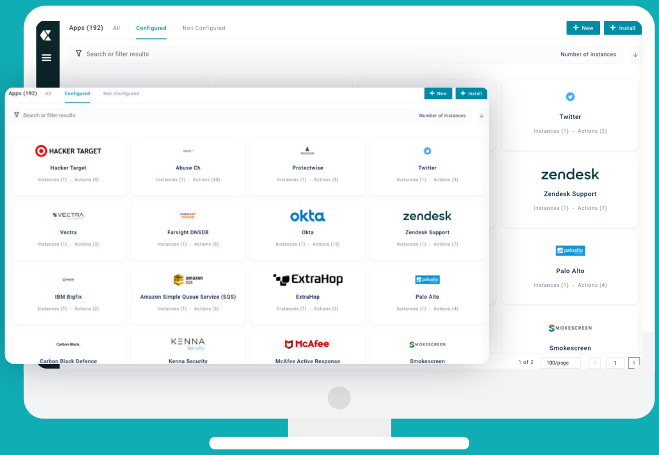
- Increased Efficiency through Custom Playbooks
- Reduced Analyst Burnout by Automating Manual Tasks
- Dashboards and KPI Tracking
- Respond Faster and With More Accuracy

Playbook Use Case Examples

- Automated Phishing Analysis & Response
- Malware Detection and Containment Automation
- Automated SOC Event Handling
- Automated SIEM Incident Case Management

CSOL Architecture




Apps (192) All Configured Non Configured
+ New + Install
Search or filter results
Number of Instances

Hacker Target Instances (1) · Actions (9)	Abuse Ch Instances (1) · Actions (40)	Protectwise Instances (1) · Actions (9)	Twitter Instances (1) · Actions (3)
Vectra Instances (1) · Actions (3)	Farsight DNSDB Instances (1) · Actions (8)	Okta Instances (1) · Actions (18)	Zendesk Support Instances (1) · Actions (7)
IBM Bigfix Instances (1) · Actions (2)	Amazon Simple Queue Service (SQS) Instances (1) · Actions (6)	ExtraHop Instances (1) · Actions (3)	Palo Alto Instances (1) · Actions (4)
Carbon Black Defence	Kenna Security	McAfee Active Response	Smokescreen

Twitter
Instances (1) · Actions (3)

Zendesk Support
Instances (1) · Actions (7)

Palo Alto
Instances (1) · Actions (4)

Smokescreen

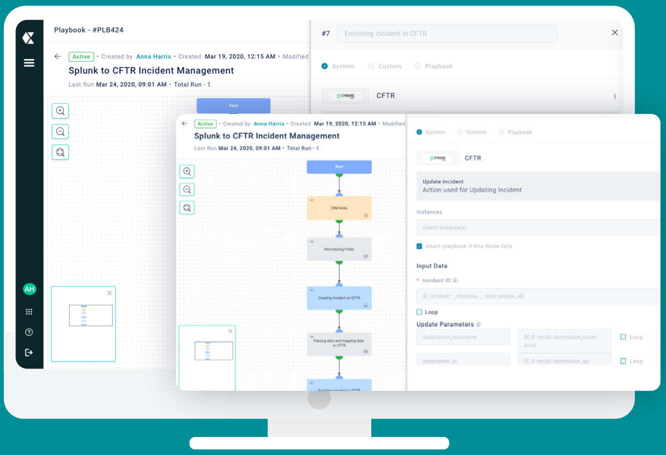
1 of 2 100/page 1

Cross-Environment Automation with CSOL Agent

- Create seamless automation interoperability between cloud and on-premise deployed technologies without exposing private networks or altering on-premise infrastructure setup.
- Accelerate security workflows by extending the machine-speed orchestration and automation capabilities to on-premise infrastructure.
- Accrue extended benefits such as greater control over assets, reduction in infrastructure cost, enhanced cloud security, resiliency, and flexibility to exchange data between third-party applications.
- Integrate CSOL with existing technology stack by utilizing over 250 pre-built application integrations and RESTful API.

Custom Automation Playbooks

- Leverage manual as well as fully-automated playbooks to dynamically meet process and procedure-specific demands.
- Gain access to hundreds of easily click-and-drag, customizable, out-of-the-box playbooks with multiple integrations and custom embedded code.
- Create nested playbooks with dynamic logic to address a wide variety of use cases.


Playbook - #PLB424

Active • Created by Anna Harris • Created Mar 19, 2020, 12:15 AM • Modified

Splunk to CFTR Incident Management

Last Run Mar 24, 2020, 09:01 AM • Total Run - 1

#7 Enriching incident in CFTR

● System ○ Custom ○ Playbook

CFTR

Update Incident
Action used for Updating Incident

Instances
Select Instance(s)

☑ Abort playbook if this Node fails

Input Data
* Incident ID
$(_3::result::__instance__::data::unique_id)

☐ Loop

Update Parameters

destination_hostname	$(_8::result::destination_hostname)	☐ Loop
destination_ip	$(_8::result::destination_ip)	☐ Loop

Start
CIM fields
Normalizing Fields
Creating Incident on CFTR
Parsing data and mapping data to CFTR
Enriching incident in CFTR

The Complete Security Automation Platform

CSOL Agent
A lightweight integrator (less than 20MB) that automates process workflows between the cloud applications and on-premise deployed security solutions.

Flexible API
Utilize a rich, RESTful API to easily build interoperable integrations with custom or third-party tools, cloud-deployed resources, or on-premises technologies.

Pre-Built Playbooks
Jumpstart automation and orchestration efforts by utilizing our vast library of pre-built playbooks and customize them to your specific workflows.

Powerful Customization
Harness the power of a secure development environment built upon and supporting Python 3, to manipulate and normalize data by easily and efficiently creating custom functions directly in the visual playbook editor.

Audit Playbook Executions
Quickly review detailed runtime information to assist in playbook debugging and enhancements.

Export and Import Logic
Maintain version control and harness the ability to move playbooks between instances by importing and exporting playbooks directly in the interface or automate the process by leveraging our API.

Nested Playbooks
Deploy a nested playbook methodology to create efficient subtask workflows and dynamic logic to address a plethora of use cases.

Application Extensibility
Install applications built by third-parties to create technology integrations or create your own connectors and actions directly in the platform.

Schedule Playbooks
Make use of playbook scheduling features and take control of playbook actioning by utilizing cron expression.

Visual Editor
Quickly and easily create powerful automation capabilities by developing logical workflows from the user-friendly visual playbook editor.

Multi-Instance Support
Utilize our platform's integration flexibility by creating multiple instances of each connector to address different use cases.

Deployment Environments

We provide multiple deployment options for our products, giving our customers the flexibility to utilize all our product features by choosing the model that best suits their business needs.

- Public and Private Cloud
- On-Premise
- Hybrid
- Air Gapped

System Requirements

System requirements will change based on the considerations of high availability and backups

	16	32 GB	100 GB
Operating System	CPU Cores	Memory	Storage

About Cyware

Cyware provides threat intelligence sharing and cyber fusion products to security teams across the world. Cyware's innovative solutions include capabilities for strategic and tactical threat intelligence sharing, cyber fusion, security orchestration, and incident response. Cyware's solutions make secure collaboration, cyber resiliency, and enhanced threat visibility a reality for customers.

CYWARE™

Cyware®
1460 Broadway New York NY 10036

cyware.com | sales@cyware.com
☎ 855-MY-CYWARE