Orchestrate
An any-to-any vendor agnostic orchestration platform for connecting and automating cyber, IT, and DevOps workflows across cloud, on-premise, and hybrid environments.

The ever-increasing complexity and number of cybersecurity tools have resulted in analysts needing to spend a lot of their time analyzing and responding to security events and incidents. This has led to analyst burnout and delayed threat responses. To counter this and improve the pace of threat response, organizations are adopting Cyware’s powerful Security Orchestration platform as a means to integrate, orchestrate and automate their security operations spanning across a wide variety of security tools from heterogeneous vendors deployed across different environments.

Orchestrate allows security teams to create customized low-code automation playbooks to execute various manual, repetitive tasks in a reliable machine-driven manner. Orchestrate 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.

Orchestrate helps organizations streamline and automate their security operations by enabling disparate tools and technologies from different vendors to talk to each other without having to rely on any manual effort for data normalization, enrichment, and analysis. By deploying Orchestrate, organizations can significantly reduce mean time to respond (MTTR) and increase operational efficiency along with overall return on investment (ROI) on security technologies.
**SUPERCHARGE YOUR SECURITY OPERATIONS WITH LOW-CODE SECURITY AUTOMATION**

- Build playbooks within minutes using out-of-the-box templates, custom integrations, drag-and-drop features, etc.
- Edit playbooks on the go using the user-friendly visual playbook editor.
- Eliminate dependency on developers for coding and building playbooks.
- Extend automation beyond security tools to automate workflows across IT/ITSM and DevOps workflows.

---

**PLAYBOOK USE CASE EXAMPLES**

- Automated phishing analysis and response
- Automated SOC event handling
- Malware detection and containment automation
- Automated SIEM incident case management

---

**CYWARE ORCHESTRATE ARCHITECTURE**

**OTA STYLE MARKETPLACE**

For Apps and Playbooks

- elasticsearch
- aws
- splunk
- Symantec
- mimecast
- slack
- Recorded Future
- FireEye
- CROWDSTRIKE
- Security Scorecard
- Cornerstone
- TANiUM

300+ Apps

150+ Playbook Library

**GUI-Based Playbook**

- Normalization
- Action Scheduling
- Data Aggregation
- Syslog Integration
- Drag & Drop

**AUTOMATED ACTIONS**

- Cyware Collaborate (CSAP)
- Cyware Agent
- Cyware Intel Exchange (CTIX)
- Cyware Enterprise Mobile App For Approval

**THREAT INTEL MANAGEMENT**

**INCIDENT MANAGEMENT**

**Holdable Playbook**

**Custom Script Support**

**Webhooks**

**Nested Playbooks**

**Data Enrichment**

**Open API Support**

**Cyware Respond (CFTR)**

**Cyware Collaborate (CSAP)**

**Cyware Agent**

**Cyware Intel Exchange (CTIX)**

**Cyware Enterprise Mobile App For Approval**

**PLAYBOOK USE CASE EXAMPLES**

- Automated phishing analysis and response
- Automated SOC event handling
- Malware detection and containment automation
- Automated SIEM incident case management
PERSONALIZED 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.

OUT-OF-THE-BOX AND CUSTOMIZABLE INTEGRATIONS

- Integrate and automate your workflows in and beyond the security domain using 250+ apps through Cyware’s integrations appstore.
- Build custom apps by creating apps from scratch or by cloning apps downloaded from our appstore and edit them based on your business use-cases.

CROSS-ENVIRONMENT ORCHESTRATION

- Create seamless automation interoperability between cloud and on-premise deployed technologies without exposing private networks or altering on-premise infrastructure setup with Cyware Agent.
- Accelerate security workflows by extending the machine-speed orchestration and automation capabilities to on-premise infrastructure.
- Gain greater control over assets, reduce infrastructure costs, enhance cloud security, resiliency, and flexibility to exchange data between third-party applications.
### A COMPLETE SECURITY, IT AND DEVOPS AUTOMATION PLATFORM

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Out-of-the-Box Playbooks</strong></td>
<td>Jumpstart automation and orchestration efforts by utilizing our vast library of pre-built Playbooks and customize them to your specific workflows.</td>
</tr>
<tr>
<td><strong>Nested Playbooks</strong></td>
<td>Deploy a nested Playbook methodology to create efficient subtask workflows and dynamic logic to address a plethora of use cases.</td>
</tr>
<tr>
<td><strong>Visual Editor</strong></td>
<td>Quickly and easily create powerful automation capabilities by developing logical workflows from the user-friendly visual playbook editor.</td>
</tr>
<tr>
<td><strong>Schedule Playbooks</strong></td>
<td>Make use of playbook scheduling features and take control of Playbook actioning by utilizing cron expression.</td>
</tr>
<tr>
<td><strong>Flexible Integrations</strong></td>
<td>Quickly build interoperable integrations with third-party tools, cloud-deployed resources, and on-premises technologies with Webhooks, Apps, and OpenAPI support.</td>
</tr>
<tr>
<td><strong>Application Extensibility</strong></td>
<td>Install applications built by third-parties to create technology integrations or create your own connectors and actions directly in the platform.</td>
</tr>
<tr>
<td><strong>Cyware Orchestrate Agent</strong></td>
<td>Leverage a lightweight integrator (less than 20MB) that automates process workflows between the cloud applications and on-premise deployed security solutions.</td>
</tr>
<tr>
<td><strong>App Marketplace</strong></td>
<td>Jumpstart integrations using our vast library with 300+ pre-built App integrations and customize them to your specific needs.</td>
</tr>
<tr>
<td><strong>Powerful Customization</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Data Synchronization</strong></td>
<td>Seamlessly orchestrate the voluminous data flow between disparate tools and technologies used by IT, ITSM, DevOps, and SecOps teams.</td>
</tr>
<tr>
<td><strong>Audit Playbook Executions</strong></td>
<td>Quickly review detailed runtime information to assist in Playbook debugging and enhancements.</td>
</tr>
<tr>
<td><strong>Multi-Instance Support</strong></td>
<td>Utilize our platform’s integration flexibility by creating multiple instances of each connector to address different use cases.</td>
</tr>
<tr>
<td><strong>Export and Import Logic</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Dedicated Mobile App</strong></td>
<td>Use our mobile app to approve workflow decisions and monitor the performance from anywhere.</td>
</tr>
<tr>
<td><strong>Persistent List</strong></td>
<td>Maintain, update, and quickly retrieve data while creating playbooks with an extensible and scalable system-failure proof datastore.</td>
</tr>
<tr>
<td><strong>Persistent Node</strong></td>
<td>Automatically update data in the datastore with help of an associated playbook.</td>
</tr>
</tbody>
</table>

### DOCKER-BASED DEPLOYMENTS

We provide Docker-based multiple deployment options for our products, giving our customers the flexibility to make use of all the product features by choosing the best model that suits their business needs.

- **PUBLIC & PRIVATE CLOUD**
- **ON-PREMISE**
- **HYBRID**

### ABOUT CYWARE

Cyware helps enterprise cybersecurity teams build platform-agnostic cyber fusion centers by delivering cyber threat intelligence and next-generation SOAR (security orchestration, automation, and response) solutions. As a result, organizations can increase speed and accuracy while reducing costs and analyst burnout.

Cyware’s Cyber Fusion solutions make secure collaboration, information sharing, and enhanced threat visibility a reality for MSSPs, enterprises, government agencies, and sharing communities (ISAC/ISAQ/CERTs and others) of all sizes and needs.