CONTRAFORCE

Security Services Delivery Platform

# Streamline the time and security expertise you require to deliver an MDR service

## Your Challenge

In an era where cyber threats are increasingly sophisticated and pervasive, establishing a world-class Managed Detection and Response (MDR) service is crucial for managed service providers (MSPs) like you to keep your clients safe. Unfortunately, most MSPs have neither the security expertise nor the security services platform to be able to support an MDR service.

## How we can help

The ContraForce Security Service Delivery Platform decouples security services from the underlying software used to provide them, transforming how MDR services are delivered and allowing you to jumpstart a new line of business, improve your margins and deliver better client outcomes.

### ContraForce Spark

ContraForce Spark is a cloud-based managed service workbench for service providers that are looking to deploy or improve an in-house MDR offering. Spark harnesses AI and hyper-automation to standardize and simplify incident investigation and response workflows, streamlining the time and expertise required to deliver managed security services.

With Spark, you can onboard clients within a few minutes and easily manage multiple clients and multiple security tools simultaneously in a single dashboard. Spark is licensed based on the number of client workspaces under management, with no data or user-based fees, so your margins are protected.

### ContraForce Storm

ContraForce Storm is a commercial program that enables MSPs to have qualified providers deliver security services on their behalf. There is no need to incur the upfront costs of building a SOC and hiring security staff.

To reduce the potential for channel conflict and to standardize service delivery, both parties contract directly with ContraForce and co-manage client environments through the ContraForce platform. Storm providers must meet delivery requirements that include specified SLOs and SLAs. Storm is priced per endpoint with no upfront costs or long-term commitments.

| What you get with ContraForce | | Spark<br>*Per User* | Storm<br>*Per User* |
|---|---|---|---|
| **24/7 Threat Monitoring** | • Continuous incident status visibility. | ⚡ | ⚡ |
| **AI-Powered Detection Coverage** | • Potential threat activity mapped to MITRE ATT&CK and MITRE D3FEND to determine intent and the appropriate response.<br>• Incident context for associated assets and users, including incident graph and activity history. | ⚡ | ⚡ |
| **Response Automation** | • Automatic Gamebook recommendations.<br>• Actionable Gamebooks that disrupt, contain and/or resolve incidents. | ⚡ | ⚡ |
| **Universal Workbench** | • 24/7 access to ContraForce platform and real-time visibility for your staff and your clients.<br>• Ticketing integration.<br>• Security service delivery platform infrastructure and service uptime commitments. | ⚡ | ⚡ |
| **Support for Leading EDR and SIEM Tools** | • EDR: CrowdStrike Falcon XDR, Microsoft Defender, SentinelOne Singularity XDR.<br>• SIEM: IBM QRadar SIEM, Microsoft Sentinel, Splunk Enterprise Security. | ⚡ | ⚡ |
| **Microsoft Sentinel Automation** | • Automated detection rule updates and tuning.<br>• Email notification with recommended Gamebook within minutes of incident detection. | ⚡ | ⚡ |
| **Rapid Client Onboarding** | • Wizard-driven client onboarding, usually completed within minutes.<br>• API-based integration with existing client EDR and SIEM tools.<br>• No agents or network sensors required. | ⚡ | ⚡ |
| **ContraForce Account Management** | • Onboarding and ongoing service delivery support.<br>• Assigned resource for account management. | ⚡ | ⚡ |
| **Industry-Leading SLAs** | • Detection: Notification time of confirmed security incidents (critical/high 1 hour, medium 2 hours, low 18 hours).<br>• Response: response time for pre-approved, authorized actions (critical/high 1 hour, medium 2 hours, low 14 hours). | | ⚡ |
| **Incident Notification** | • Direct incident notifications including Gamebook (response playbook) recommendations via email and phone call. | | ⚡ |
| **Escalation Communication** | • Pre-defined escalation call process and procedure between you and the Storm Provider (MSSP). | | ⚡ |
| **Client Relationship Protection** | • Storm Provider will not share their name or trademark with client without your express prior written consent.<br>• Storm Provider will not solicit client for 12 months after termination of service. | | ⚡ |