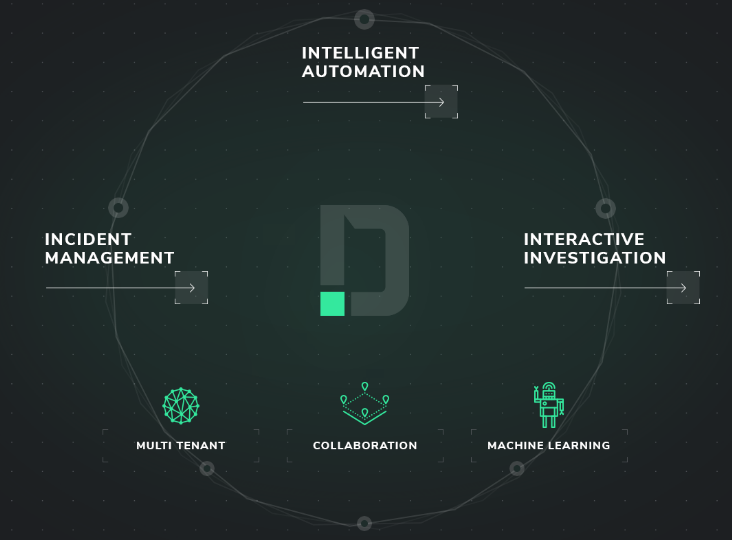
DEMISTO ENTERPRISE FOR MSSPs



The Connecting Fabric For Your Security Infrastructure And Teams

Full Multi Tenancy: Complete data segregation between customers in a single deployment

Primed for Collaboration: Master-tenant cooperation with isolated execution, master playbook design for multiple tenants, joint master investigations for reduced MTTR

Segmented Networks: Engine (proxy) for segmented networks, no firewall change needed for customer security device access

The SOC-as-a-Service Challenge

Organizations across the world are moving towards outsourcing their security services. This demand notwithstanding, MSSPs still grapple with multiple challenges that affect their ability to fully leverage this opportunity.

Reduced customer visibility: Most MSSPs offer customers little to no visibility into their security processes. This not only frustrates customers that want to be well-informed and demand more than standard post-incident reports, but also impacts MTTR due to lack of customer expertise and participation during incident response.

SLA anxiety: Managing security incidents across customers requires extensive coordination, consistency, patience, and foresight. There is often a disconnect between SLAs that an MSSP is willing to commit to and SLAs that a demanding customer would expect.

KEY BENEFITS

Maximized Analyst Productivity

- Intuitive playbooks that automate repetitive tasks.
- War Room discussions enable collaboration and cross-analyst learning.
- Single orchestration pane reduces alert fatigue.

Ironclad Security and Privacy

- Data isolation with master-tenant separation and role-based visibility.
- Execution isolation with each tenant running as a separate processs.
- Network isolation with engine (proxy) for segmented networks without firewall changes.

Consistent Results and SLA Confidence

- Master tenant has metric access to all tenants for accurate measurement and management.
- Playbooks, chat rooms, and flexible customer access reduce MTTR.
- Consistent processes and results tracking leads to increased SLA confidence.

Increased Customer Trust and Agility

- Collaborate in real-time with customers through War Room.
- Quick customer onboarding times and scalability.
- Joint investigations with MSSP and customers, leading to quicker response and increased trust/visibility.

Personnel shortage: Finding, training, and retaining skilled security personnel is an industry-wide issue, and MSSPs face it as well. Additionally, MSSPs need to employ a sizable number of non-security personnel, such as software developers and support. These challenges result in a lack of scalability and varying levels of output quality.

This is where Demisto Enterprise for MSSPs comes in – a natively multi-tenant Security Operations Platform that combines incident management, security orchestration and automation, and collaboration to improve analyst productivity, enable consistent processes, and increase SLA confidence.

Which MSSP Are You?

- If you are an MSSP that has customer-specific service tiers (full SOC service without customer involvement, sporadic customer assistance etc.), Demisto's master-child separation and data isolation will ensure that you provide tailored service to each customer.
- If you are an MSSP that only provides the platform as SaaS without touching the customer environment, Demisto's common playbook design across tenants and role-based access will lead to increased customer trust and agility.

What services can you provide?

- Handling phishing triage, enrichment, and response.
- Handling lost/stolen device instances.
- Responding to malware outbreaks.
- Identifying and remediating ransomware attacks.
- Responding to malware outbreaks.

These are just illustrative examples. You can offer endless other services using Demisto Enterprise features.

Complete Incident Management

Manage all aspects of the incident lifecycle to codify processes and achieve consistent results:

- Open and extensible platform of 140+ integrations with data enrichment tools, threat intelligence feeds, SIEMs, firewalls, EDRs, sandboxes, forensic tools, messaging systems, and more.
- Intuitive drag-and-drop playbooks to automate SOC processes and workflows.
- Auto-documentation of all incidents and investigations for comprehensive SLA tracking.
- Central indicator repository that enables pivoted searches around indicators and threat hunting exercises.
- Comprehensive dashboards and customizable reports to quantify performance and archive results.
- Windows/Mac/Linux OS dissolvable agents to collect data from endpoints.

Intelligent Automation and Orchestration

Improve analyst productivity and free up the need for non-security personnel:

- Playbook portfolio primed for automation with 140+ integrations and 400+ security actions.
- Custom integration builder (BYOI) to create bespoke connections beyond 140+ supported integrations.
- Portable playbooks and War Room documentation eschew the need for home grown solutions, external ticketing.
- Flexibility to create new playbook tasks/blocks and carry them over across playbooks.
- Playbooks have high availability and failover, easy to troubleshoot and start over from any point in the playbook.
- Machine-powered suggestions for related incidents and common indicators across incidents.

Interactive Investigation

Increase customer trust and agility by conducting joint investigations, improving process visibility:

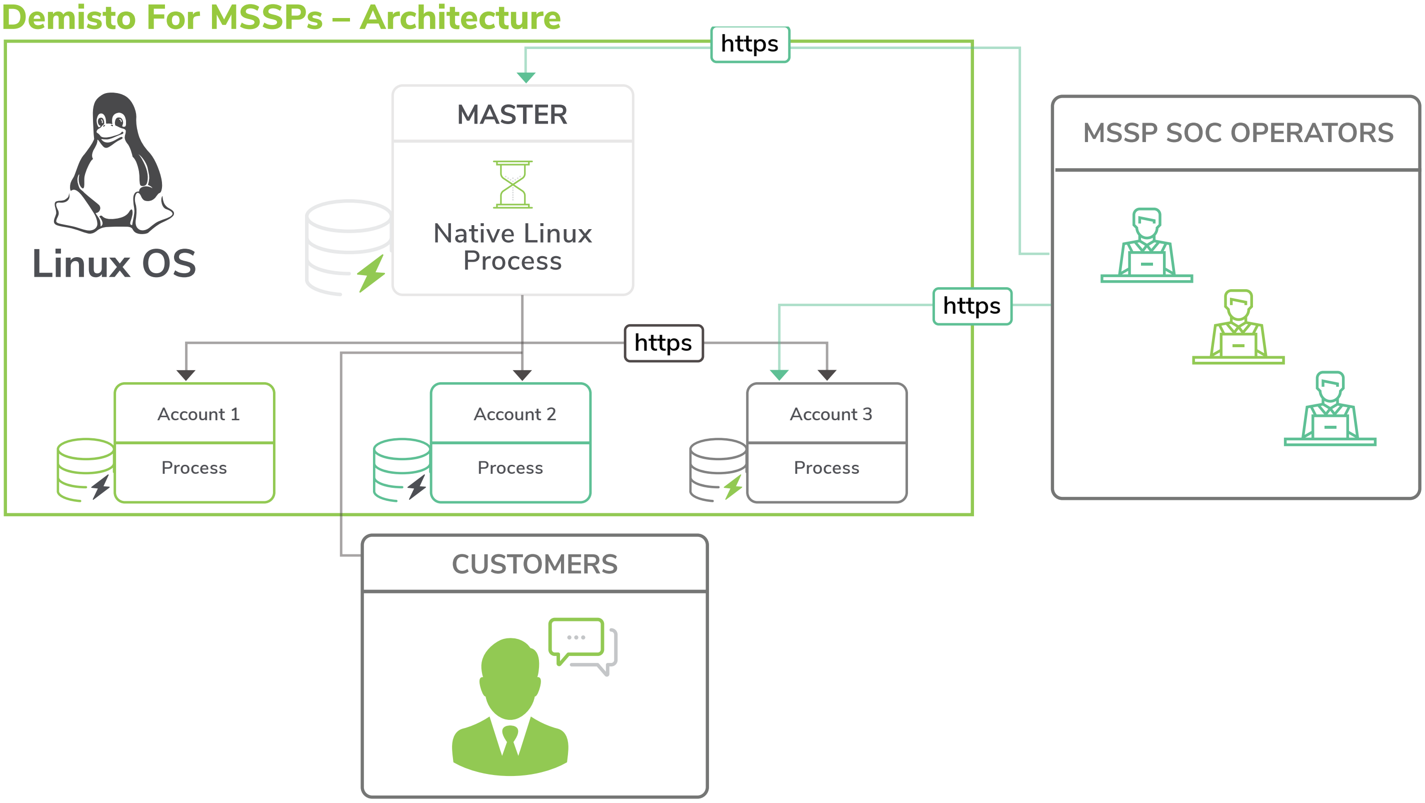
- ChatOps-powered virtual 'War Room' where analysts can collaborate in real-time and run security actions.
- Related Incidents investigative toolkit that provides customizable map of related incidents across time.
- In-house security bot (DBot) that helps run commands, suggests analyst ownership and future course of action.
- Externally installable chatbot that allows mirroring investigations on Slack.

Flexible Deployment

Cater to variety of customer environments and requirements with consistent output quality:

- Implement SaaS or on-premise deployment with full multi-tenant capabilities.
- Set up segmented networks through engine proxy for data privacy and compartmentalization.
- Account-based data segregation with isolated execution and scalability.
- Run playbooks/actions for specific accounts or across accounts depending on requirements.

Demisto For MSSPs – Architecture



System Requirements

Demisto Enterprise Server for MSSPs:

- Physical or virtual server
- Linux OS: Ubuntu 14.04 and 16.04, Centos 7 and up, RHEL 7 with Docker EE, Oracle Linux 7.3 with Docker EE (ask us about other distros and versions)
- 16GB RAM minimum (64GB desired)
- 8 CPU cores minimum (16 desired)

Demisto Engine:

- Linux OS: Ubuntu 14.04 and 16.04, Centos 7.x (ask us about other OSs, distros and versions), Windows
- 4GB RAM minimum
- Dual core CPU minimum

About Demisto

Demisto helps Security Operations Centers scale their resources, improve incident response times, and capture evidentiary support while working and solving problems the way humans are wired to – together. Demisto Enterprise is the first comprehensive, Security Operations Platform to combine intelligent automation with collaborative, human social learning and experience. Demisto's intelligent automation is provided by DBot which works with your team via a new concept, Security ChatOps, for fully automated, playbook-based workflows, cross-correlation, information sharing and curation from investigation-through-response and beyond. Demisto is backed by Accel with offices in Silicon Valley and Tel Aviv. For more information, visit www.demisto.com or email info@demisto.com.