Demisto Enterprise is a comprehensive Security Orchestration, Automation, and Response (SOAR) platform that combines full case management, intelligent automation, and real-time collaboration to serve security teams across the incident lifecycle.

- **Select Customers**
  - ~200 customers worldwide, spanning 10+ industry verticals
  - 25% of customers from the Fortune 500
  - Fortune 500 healthcare organization
  - Fortune 100 athletic-wear retailer
  - Online streaming and entertainment giant

- **Industry Recognition**
  - Top worldwide online payment system
  - Fortune 100 athletic-wear retailer
  - Fortune 50 healthcare organization
  - Online streaming and entertainment giant

- **Headquarters**
  - Santa Clara, CA | USA

- **Founded**
  - 2015

- **Platform**
  - 230+ integrations
  - Open & extensible platform

- **Partners**
  - 100% channel friendly
  - MSSP and cloud ready

- **Community**
  - 7000+ members (largest IR community in the industry)

---

**The Operating System for Enterprise Security**

- **Accelerate Response**
  - Respond to incidents with speed and scale
  - 100s of integrations
  - 1000s of security actions
  - Cross-correlations

- **Standardize Process**
  - Respond to incidents the same way every time
  - Task-based workflows
  - Visual playbook editor
  - SLA and metric tracking

- **Collaborate and Learn**
  - Improve investigation quality by working together
  - Virtual war room
  - Investigation canvas
  - Machine learning

- **Reduce Risk**
  - Reduce business and security risk
  - Dashboards and reports
  - Auto documentation
  - Improved ROI
Demisto for **Cloud Security**

Cloud security demands agility and flexibility in the face of an expanded threat surface and disparate teams. Demisto primes users for fast and standardized cloud security through multi-source ingestion of cloud data and playbooks that coordinate and automate incident response actions across cloud and on-premise environments.

**Cloud-Hosted**
- Cloud Security
- Cloud Services
- DevSecOps
- Threat Intelligence
- Malware Analysis

**On-Premise**
- SIEM
- EDR
- Firewall
- Email
- UEBA
- Ticketing

...and more!

**Automate Repeatable Steps**
Automate actions to standardize and scale incident response

**Unify Security Functions**
Coordinate enrichment and response for both on-premise and cloud environments from one console

**Orchestrate Cloud Security**
Ingest alerts from your cloud environment and trigger automated workflows that span across products
Case Study: The Pokemon Company International

Goals

- Keep pace with rapidly scaling cloud environment
- Automate everything that humans don’t need to do
- Provide value to other technology departments

Use Cases

- EC2 and account compromise
- Phishing enrichment and response
- Employee offboarding

Use Case Deep Dive

As part of the phishing response playbook that Pokémon deployed, Demisto automated extraction of IOCs before pushing those IOCs to blacklists across both cloud and on-premise environments.

IOCs → Demisto → Update SQS Queue → Update Lambda → Blacklist Bucket → Block on Palo Alto Networks Firewall

© 2019 Demisto, a Palo Alto Networks company | www.demisto.com
Demisto can be deployed both on-premise and as a cloud-hosted offering, adapting to customer requirements as the need arises. The platform is also primed with native multi-tenancy for MSSPs that scales horizontally, provides three layers of isolation, and maintains data integrity while simplifying communication across tenants.

**How Demisto Deploys**

Customer On-Premise Server | Customer Virtual or Cloud | Hosted SaaS
--- | --- | ---
![Demisto Logo] | ![Cloud Icon] | ![AWS Logo]

**Illustrative Integrations - Cloud Security**

- **100s of integrations**
- **1000s of actions**
- **Open and Extensible** platform

**RedLock**
Global Protect Cloud Service

**Microsoft**
- Microsoft Graph Security
- Microsoft Graph Mail
- Azure Active Directory
- Azure Security Center
- Microsoft Compute

**aws**
- GuardDuty
- SQS
- CloudTrail
- Route 53
- IAM
- CloudWatch Logs
- EC2
- S3
- Security Hub

**Other**
- Zscaler
- netskope
- Skyformation
- Cisco Stealthwatch
- Cisco Cloudlock

**Google**
- Big Query
- Google Cloud Platform
- Google Vault
- Google Cloud Resource Manager
- Google Cloud Compute

© 2019 Demisto, a Palo Alto Networks company | www.demisto.com