At-a-Glance

Service Benefits

- **Increase visibility** to cybersecurity, risk management and compliance throughout your business.
- **Tighten security** by streamlining access, reliably updating systems, detecting anomalies and monitoring compliance.
- **Boost productivity** through reduced downtime.
- **Control costs** with simpler management, less complexity, and greater consistency across sites.
- **More easily manage** cybersecurity and compliance on a site-by-site basis.

Cisco Secure Ops Solution

Gain Visibility and Control of ICS Networks

Throughout industry—in oil fields, power plants, factories, and more—the Internet of Things (IoT) is boosting production. It's speeding delivery of products. And it's helping companies like yours compete.

But while IoT is making you more efficient, the increased connectivity also makes your industrial control systems (ICSs) more vulnerable to cyberthreats.

Cisco® Secure Ops can help you address that challenge. The comprehensive, end-to-end system gives you a centralized view of what's happening at multiple, far-flung sites. It can detect and alert to anomalies, trigger the incident management process, and protect your most critical systems.

We designed Secure Ops to meet the needs of your risk-conscious executives and IT department, while streamlining operations.

How Secure Ops Works

Secure Ops is a combination of highly trained people, fully integrated operational support processes, and technology. The solution has a hub-and-spoke architecture, with a SecureCenter component as the hub, and SecureSites—made up of hardware and software located at each plant, oil rig, and so forth—as the spokes.

We built the solution to interface with asset discovery and inventory, secure access, and other functions from major automation companies. Some of these automation vendors are also joint delivery partners. Using a robust partner ecosystem, Secure Ops allows you to benefit from Cisco's network and security expertise and the automation suppliers' OT expertise.

Committed to market leading integration, the solution dramatically streamlines access to your systems for staff, vendors, and partners. It also organizes software maintenance and downloads, and it distributes patches and updates in a consistent manner across all your sites. Equally important, Secure Ops provides checks and balances at each step in the process to make sure your managers implement security policies appropriately and that sites are in compliance.

OT managers at the sites decide when to actually apply the updates—at an appropriate time in their maintenance cycle—to avoid unintentional downtime. Automated compliance reports let central management know whether site leadership has addressed vulnerabilities. Secure Ops flags sites that are out of compliance so that operators can more easily manage the exceptions. This reduces costs and improves operations.

"One of the things that is incredibly important… is our critical infrastructure. Whether that's refineries, wells, or lubricant plants, we need to protect that critical infrastructure… We asked Cisco to join with us in a comprehensive solution."

Executive Vice President and
Chief Information Officer,
Global Oil and Gas Customer

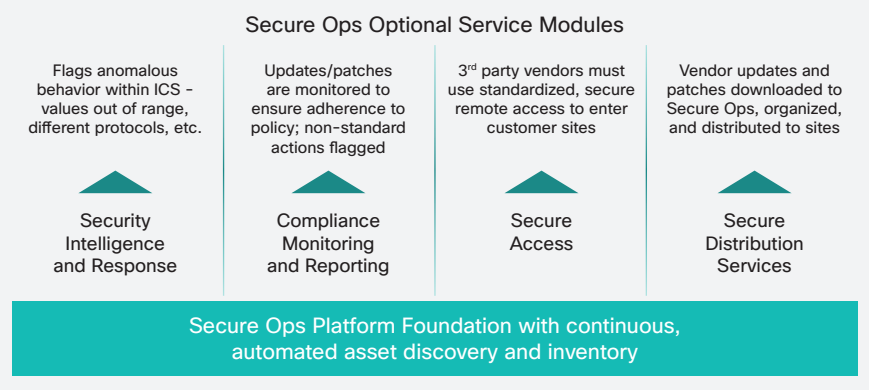
Oil Company Sees Significant Savings with Secure Ops

Secure Ops has had impressive results in the field. A major international oil and gas company is using it to help address challenges of growth and complexity in its facilities, along with new and evolving cyberthreats.

An ROI study performed by the company found Secure Ops reduced costs by $700,000 per site deployed over five years. And using the service delivery commercial model allowed the company to significantly reduce initial capital expenditures.

By more quickly managing risks and mitigating threats, the company has increased business agility, lowered operations and security costs, and significantly reduced downtime.

Figure 1. Secure Ops Provides Security and Control of Your Industrial Control Systems



Modular Approach Provides Flexibility

The Secure Ops modular approach lets you implement various controls based on your company's risks and needs (Figure 1). At the most basic level, we provide Foundational Services, which include automated and continuous asset discovery and inventory so you know exactly what devices are operating at each site.

Additional optional modules include:

- **Secure Access Services,** which provide secure, controlled remote access to underlying industrial networks and systems through centralized user management and role-based security profiles, file transfer, and file sharing. It uses an application tunnel (for TCP applications) to enable secure device-to-device connection.
- **Compliance Monitoring and Reporting Services,** which let you track whether sites are following policies for addressing vulnerabilities.
- **Security Intelligence and Response Services,** which allow you to detect and alert to system anomalies using deep packet inspection of IP, Industrial and Fieldbus protocols. This knowledge allows you to quickly respond to incidents.
- **Secure Distribution Services,** which provide controlled and centralized distribution of vendor-qualified operating system and application updates, upgrades, and patches as well as McAfee and Symantec antivirus updates.

Next Steps

For more information about the Cisco Secure Ops solution, visit http://www.cisco.com/go/secureops/.

C45-736243-00 12/15