REPORT REPRINT

# Tenable bets on converged IT/ OT vulnerability management with Indegy pickup

**DECEMBER 03 2019**

**By Patrick Daly**

The vendor has handed over $78m for Indegy to obtain tools for comprehensive IT/OT vulnerability and risk management. Consolidating visibility and control across these environments has the potential to offer organizations a more accurate understanding of their security posture and can highlight areas in need of improvement.

451 Research®

## Introduction

The ubiquity of computing and connectivity in industrial control systems (ICS) – and in operational technology (OT) broadly – has given rise to a market of vendors specializing in securing these critical systems. As it has become increasingly apparent that an organization's overall security posture depends on its level of visibility and control over both the IT and OT infrastructure, IT security incumbents increasingly see the value in consolidating security for converged IT/OT environments. With the acquisition of Indegy, Tenable is the first vulnerability and risk management provider to bet on the need for consolidated IT and OT security.

## Snapshot

| | |
|---|---|
| ACQUIRER | Tenable |
| TARGET | Indegy |
| SUBSECTOR | ICS security |
| DEAL VALUE | $78m |
| DATE ANNOUNCED | December 2, 2019 |
| CLOSING DATE | December 2, 2019 |

## 451 TAKE

Tenable has demonstrated a willingness to adjust its portfolio to meet the needs of modern organizations and counter criticism that previous prioritization methods based on common vulnerability scoring system (CVSS) scores were inadequate. The company's addition of cloud-based Tenable.io with container security and web application security and the introduction of Predictive Prioritization are good examples. The Indegy buy certainly bolsters Tenable's ICS security capabilities and would seem to fit well within its broader vulnerability management portfolio – the target was the first ICS security provider to develop an active query function to detect vulnerable or misconfigured assets. Indegy's findings, whether from an active query or passive traffic analysis in the ICS environment, should tie in well with Tenable's Predictive Prioritization offering, which prioritizes vulnerabilities for practitioners. Indegy should also offer valuable insights to Lumin, which measures enterprise-wide exposure based on vulnerability assessments and recommends fixes to reduce exposure.

## Deal details

Announcing just its second acquisition, Tenable says it will pay $78m for Indegy. (Subscribers to 451 Research's M&A KnowledgeBase can click on our deal record for our proprietary estimate of the transaction's valuation.) Tenable's purchase of Indegy is the latest security-focused IoT deal, a market that is – somewhat belatedly – only now taking off. As we noted in a related report, the M&A KnowledgeBase lists more IoT security acquisitions so far in 2019 than any other year.

## Deal rationale

IT and OT integration – partly driven by the expansion of connectivity and communications technologies in OT environments for remote monitoring and management, predictive maintenance and anomaly detection – has made security a leading cause for concern among industrial organizations. In a recent survey by 451 Research's Voice of the Enterprise, more than 40% of respondents cited security concerns as the leading impediment to implementing IoT initiatives. As a result, there is a significant market need for security tools capable of supplying visibility and control across both IT and OT environments. The Indegy pickup provides Tenable with many such tools, including vulnerability coverage across IT and OT environments and a more comprehensive understanding of an organization's exposure to risk by including OT exposure in enterprise measurements.

## Target profile

Since its founding in 2014, New York City-based Indegy has grown to 70 employees, raised $36m in venture funding and received a patent for its active query technology, Device Integrity. Device Integrity enables users to query industrial assets for full configuration and state information on a read-only basis. This information can be used to identify misconfigured assets and discover vulnerabilities, or as forensic evidence following a security incident. In addition to Device Integrity, Indegy passively discovers OT assets, detects threats using a combination of signature, policy and behavior-based methods, identifies misconfigured assets, and enables organizations to manage OT security across multiple sites.

Earlier this year, Indegy became the first ICS security vendor to offer a cloud-based version of its product, which it calls CIRRUS. CIRRUS includes a pure-cloud version that relies on Device Integrity's active scans, as well as a hybrid cloud version that leverages both passive and active methods. The company offers these services across a wide range of industries, notably electric and water utilities, oil and gas, transportation, building management, aerospace, wastewater treatment, discrete manufacturing and process manufacturing (including pharmaceuticals, food and beverage, and chemicals). Indegy says it has also noted a recent uptick in interest in securing datacenter building management systems.

## Acquirer profile

Tenable became one of the leading incumbents in vulnerability and risk management thanks in large part to the popularity of its scanning engine, Nessus, which itself gained recognition as an open source project before being rolled into Tenable. While Nessus remains the scanning engine that powers Tenable's portfolio, the company has introduced a range of functionality over the past year to address more salient needs in vulnerability and risk management than the discovery and cataloging of vulnerabilities.

The vendor's cloud-based Tenable.io product, for example, addresses some of the visibility-related requirements of modern organizations with the ability to scan web applications and cloud-native technologies like containers. Earlier this year, Tenable also launched its Predictive Prioritization offering to reduce the manual and time-consuming effort required to prioritize vulnerabilities. Predictive Prioritization combines asset data, vulnerability information like CVSS scores, and threat intelligence to identify the most critical vulnerabilities for security teams to focus on. Also earlier this year, the company unveiled Lumin, a risk management dashboard intended to provide CISOs with an enterprise-wide view of their exposure across business units or among industry peers and recommend changes that would reduce risk. Acquiring Indegy to augment its industrial security offering and consolidate visibility and control across IT and OT environments represents Tenable's latest effort to meet the needs of modern organizations.

The vendor has said that Indegy already integrates with its on-premises offering and expects integrations with cloud-based Tenable.io and risk management dashboard Lumin to be available by mid-2020. In the near term, it plans to apply Predictive Prioritization to OT vulnerabilities detected by Indegy, reducing the time and effort required for OT security practitioners to remediate or mitigate vulnerabilities.

## Competition

Tenable's primary competitors in the vulnerability and risk management arena include Qualys and Rapid7, neither of which offers an ICS-focused product that vies with Indegy. While acquiring Indegy may help Tenable differentiate its portfolio from those of its rivals, the most direct competition to its ICS security ambitions will come from the ICS security specialists Indegy was already running into – Claroty, Dragos and Nozomi Networks. Much like Indegy, all of these vendors provide organizations with visibility into their ICS assets, detect threats and offer tools to aid in incident response.

Although Cisco and ForeScout have also both purchased ICS security providers over the past year, neither are likely to significantly contend with Tenable given the angle they approach ICS security from. ForeScout has bundled SecurityMatters into its network access control offering, while Cisco is only using Sentryo to offer OT visibility in its IoT engagements.