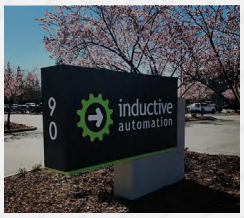
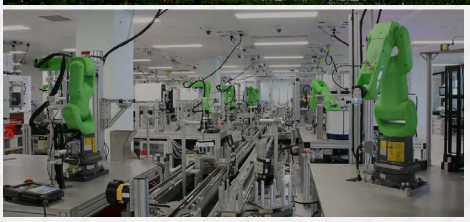
voices

CrowdStrike Customer Case Study





inductive automation®

CrowdStrike Helps Inductive Automation Ensure Business Continuity for Critical Industry and Public Services

When you develop software systems that sit at the heart of most of the world's essential industrial operations — healthcare, energy, utilities, pharmaceuticals and food production — ensuring the security of these systems is mission critical. And that task gets harder all the time as those industries increasingly embrace new ways of working such as the manufacturing sector's "Industry 4.0" and the internet of things (IoT) that drive greater efficiency, but also increase vulnerability.

It is a challenge that California-based Inductive Automation faces every day. The company develops industrial supervisory control and data acquisition (SCADA) software for many global brands including Airbus, Coca-Cola, GlaxoSmithKline, Johnson & Johnson, Kraft, Shell and Unilever, as well as hundreds of public sector utilities. Its flagship product Ignition was the first universal industrial automation application platform. As one process manufacturing customer said, "Pretty much whatever we think of doing, we do it in Ignition."

Inductive Automation helps customers manage industrial operations such as manufacturing, wastewater and nuclear power with applications that integrate multiple systems into a single point of monitoring and control. The goal is to provide solutions that integrate with whatever ecosystem is adopted by a customer. Therefore, it is critical for Inductive Automation that the way it develops, hosts and manages licensing and authentication of these systems is highly secure.

Protecting Critical Industry and Infrastructure

"We consider ourselves a crucial part of the supply chain for customers that are in the world's most critical sectors," said Inductive Automation Director of Cyber Security Jason Waits. "So, we must invest, and invest early, to ensure that we are never the cause of a security issue."

As a software house, Inductive Automation has a complex IT environment, with a large percentage of its employees in skilled technical roles, making the enforcement of security mandates challenging at times. While most servers are Linux, the company also has Microsoft Windows and Apple Mac systems. Most applications are run on premises but there is a sizable and growing AWS-based cloud environment used for customer-facing functions like product activation, ticketing and licensing.

Inductive Automation had a world-class security infrastructure in place, but there were some challenges with one of the key legacy packages that protected the company's endpoints. The security application offered a comprehensive range of capabilities, but the tool was comprised of

INDUSTRY

Technology

LOCATION/HQ

Folsom, California

CHALLENGES

- Ensuring software used in critical industry operations was robust and secure
- Increasing vulnerabilities from changes like Industry 4.0 and internet of things (IoT)
- Complex, developer-dominated IT systems and infrastructure
- Fragmented endpoint security imposed a burden on system resources

SOLUTION

Inductive Automation is using a portfolio of CrowdStrike solutions to protect and secure the data, systems and software used to monitor and control many of the world's most critical industries and public infrastructure services

"The bottom line is that we've elevated security for the whole company and, despite it being a premium solution, we saved money by deploying CrowdStrike."

Jason Waits
Director of Cyber Security
Inductive Automation

voices

CrowdStrike Customer Case Study

an amalgamation of previously separate products that had been pulled together as a single offering following acquisitions by the well-known parent company.

Another challenge was the demands created by the endpoint protection software on computer resources. The work that Inductive Automation does — developing sophisticated SCADA applications — requires a lot of processing power and developers could not tolerate slow-running systems. The package also was producing many false positives, resulting in wasted time and effort for the security team.

The issues were further magnified by Inductive Automation's explosive growth over the last few years. This necessitated that any security solution needed to be able to flex, adapt and scale to support the company's impressive growth and constantly evolving business model.

Streamlining the Process

Inductive Automation started looking for an alternative solution for the incumbent endpoint protection product and did a market evaluation. "We were pretty much blown away by the performance of CrowdStrike," Waits said. "There was minimal CPU demand and negligible impact on system performance. To confirm our findings in a real-world scenario, we decided to get one of our more outspoken developers to participate in a beta test. It was hilarious because the engineer quickly forgot that CrowdStrike was even running on his system."

Inductive Automation replaced several of its existing products with comprehensive security protection utilizing the CrowdStrike Falcon® platform for both on-premises and cloud environments. CrowdStrike Falcon OverWatch™ managed threat hunting service was selected to augment the in-house security team and overcome the challenge of attracting additional suitably skilled staff.

Low Profile, High Impact

"We consider CrowdStrike to be one of the most valuable elements in our security stack — we love it because it's completely out of the way, doesn't slow anyone down, but still gives us eyes on everything that is occurring," Waits said. "If something does get flagged, we can step in and interject in a really slick way. CrowdStrike lets us catch things early on without friction or impact on performance."

The comprehensive nature of the Falcon platform brings additional benefits. "There's a very measurable operational cost to individually picking and managing every discrete piece of an endpoint solution, but when you consolidate onto a single platform you reduce overhead," Waits said. "With CrowdStrike we just needed to install a single agent — it's lightweight, doesn't impact performance and can deliver a host of capabilities, including USB and firewall control, vulnerability management, antivirus and forensics."

Tools like CrowdStrike Falcon Intelligence™ are leveraged for tasks such as detecting and managing suspicious links or files. "It's really nice to have the capability to safely 'detonate' suspects in the Falcon Intelligence sandbox to quickly gain insight into any malicious intentions and, if needed, use that context to optimize our remediation strategies," Waits said.

RESULTS

Reduced costs from deploying a premium security solution

Lessened demand on development computing power

Enhanced speed, accuracy and high-fidelity detection

ENDPOINTS

CROWDSTRIKE PRODUCTS

- Falcon Device Control for cloud-delivered device control
- Falcon Discover™ IT hygiene
- Falcon Firewall Management™ centralized firewall management
- Falcon Horizon™ cloud security posture management
- Falcon Insight™ endpoint detection and response
- Falcon OverWatch™ managed threat hunting
- Falcon Prevent™ next-generation antivirus
- Falcon Spotlight™ vulnerability management
- Falcon Intelligence™ automated intelligence

voices

CrowdStrike Customer Case Study

Setting the Pace

Waits has been impressed by what he describes as the "aggressive" pace of CrowdStrike update releases. Unlike other vendors where not much changes over the course of a year, he applauds CrowdStrike's cadence of regularly rolling out new capabilities and enhancements.

Because CrowdStrike supports multiple platforms like Linux, Windows and Mac OS, Inductive Automation was able to replace other OS-specific security applications and reduce costs through the consolidation of agents. "CrowdStrike delivers speed, accuracy and high-fidelity detection," Waits said. "We don't waste our time chasing red herrings and achieving this with a single agent lowers operational costs. The bottom line is that we've elevated security for the whole company and, despite it being a premium solution, we saved money by deploying CrowdStrike."