



## The Channel Company Modernizes Cybersecurity, Begins Zero Trust Journey Amidst Global Expansion

THE **CHANNELCO.**

### Overview

Over the past few years, The Channel Company (TCC), a leading marketing services, events and media company, has aggressively expanded, making several acquisitions to further diversify its global marketing portfolio for technology channel partners. These acquisitions have significantly increased its employee base and created a global organization.

During this time, the COVID-19 pandemic forced the company to pivot to support a fully remote workforce in seven countries across four continents. These two seismic shifts made it apparent that the company needed to modernize its information security infrastructure and posture.

### Solution

First, TCC completed a NIST (National Institute of Standards and Technology) assessment to evaluate its existing security posture, identify the most critical cybersecurity gaps and assess new regional regulatory requirements facing the business.

The Channel Company enlisted Blue Mantis to develop a Zero Trust Architecture based on the Cybersecurity and Infrastructure Security Agency's (CISA) 2.0 model. This critical step included a thorough examination using the NIST Cybersecurity Framework (NIST CSF), which revealed cybersecurity gaps and priorities and provided a strong foundation for TCC's Zero Trust Architecture. CISA describes Zero Trust as a security framework that assumes that all network traffic is untrusted until proven otherwise. TCC's objective was to holistically address identified gaps in its cybersecurity strategy and this exercise with Blue Mantis helped accomplish this mission.

### Business Outcomes

- **Completely Overhauled Security Posture** – Through this comprehensive risk analysis, the Channel Company's management team gained a clearer understanding of its information security gaps and took immediate action to begin remediating these issues. Blue Mantis has guided TCC on its Zero Trust journey, and this requires a continuous improvement plan to keep up with the rapidly shifting threat landscape.
- **Aligned Diverse Security Programs** – Prior to engaging with Blue Mantis, TCC replaced its antiquated hardware and applications designed for a much smaller, single-location company with on-site employees with a cloud-first environment designed to support a fully remote workforce. This eliminated its physical data center, resulting in reduced IT management and improved security. Blue Mantis aligned the Zero Trust program with TCC's cloud-only strategy helping integrate TCC's newly acquired and diverse organizations into a cohesive cybersecurity strategy and framework.
- **Enhanced and Expanded Regulatory Compliance** – Improved auditing visibility and speed of compliance with geographic- and industry-specific legal and regulatory standards for data security, including ISO 27001, GDPR, CCPA, and new SEC reporting requirements.

### Benefits

- Dramatically improved cyber hygiene across a growing base of end users globally.
- Greater productivity, flexibility, mobility, and cost savings delivered through a newly implemented BYOD (Bring Your Own Device) policy.
- Increased level of trust and communication between TCC's executive team and IT especially as it applies to organizational risk management and the effort required to further TCC's information security modernization initiative.