CISO GLOBAL

A **CISO GLOBAL** CASE STUDY

TRONICS AMERICA

Cloud Architecture: A Showcase of Speed, Security, and Efficacy

SECURED MANAGED SERVICES

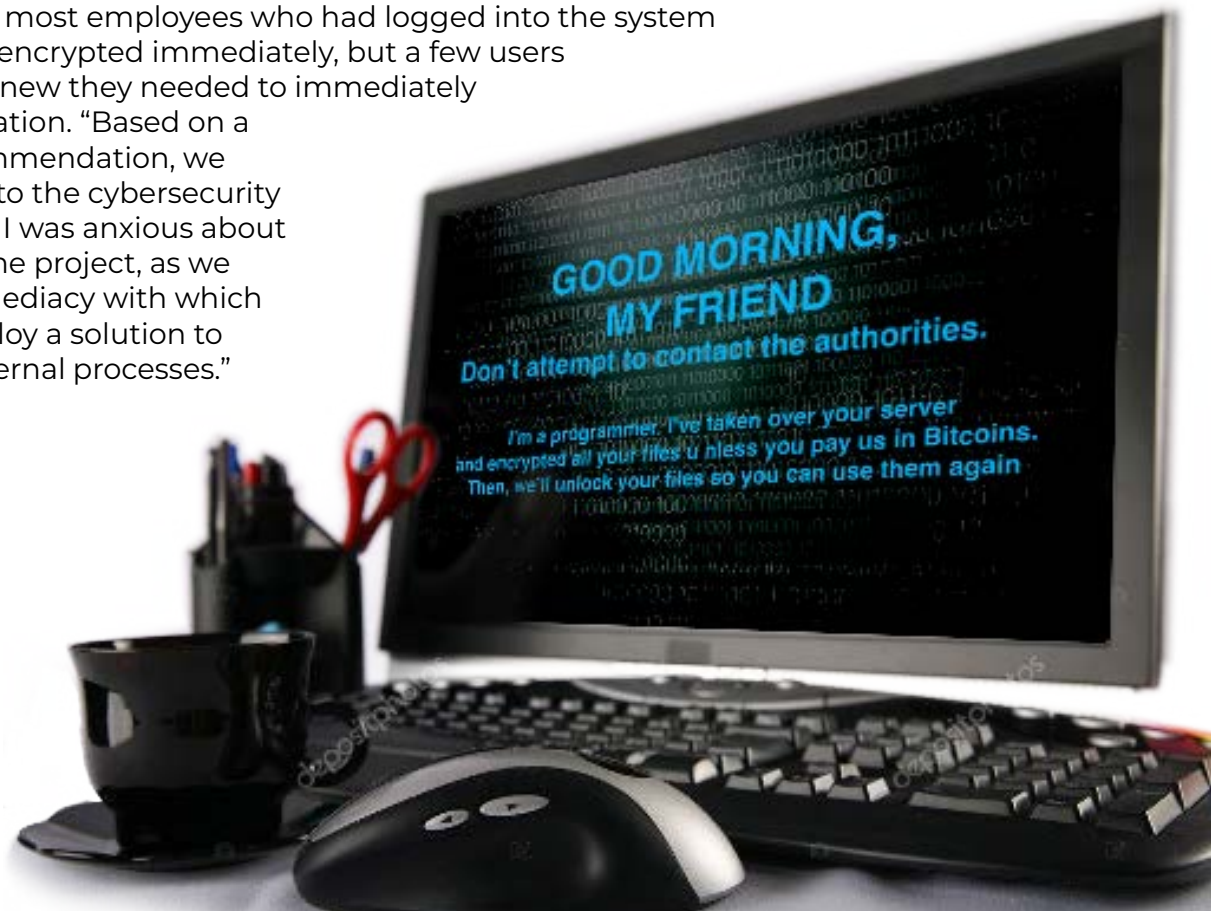
Tronics America Labeling Systems, a division of Aldus, was founded in 1985 and manufactures, installs, and services its line of turnkey pressure-sensitive labeling machines and labeling equipment. Based in Indiana, Tronics customers include companies, from start ups to Fortune 50 businesses, that span the primary packaging industry across North America, with successful labeling machine installations worldwide.

"Good morning, my friend. I've taken over your server!"

In business for almost 3 decades, Tronics had always seen itself as a cyber secure organization. Its environment was Microsoft Windows-based, and the company had just upgraded to new servers, though a few older workstations were still connected to their network. Company leadership knew they needed to made replacements and upgrades but didn't see this as a priority—or a vulnerability. This all changed, however, when Tronics fell victim to a ransomware attack. General Manager Richard Dew recalled:

> *I came in one morning to find a "Good morning, my friend" blue message on our main server and "Don't attempt to contact the authorities. I'm a programmer. I've taken over your server and encrypted all your files unless you pay us in Bitcoins. Then, we'll unlock your files so you can use them again." It is not the kind of message you want to see first thing in the morning!*

Unfortunately, most employees who had logged into the system had their files encrypted immediately, but a few users did not. Dew knew they needed to immediately triage the situation. "Based on a glowing recommendation, we made the call to the cybersecurity gurus at CISO. I was anxious about the speed of the project, as we knew the immediacy with which we had to deploy a solution to restore our internal processes."



Enter CISO Global

Tronics depended on a farm of terminal servers connected to directory, application, and file servers, all of which were irrevocably compromised—right down to the employees' desktops, denying them the ability to operate. Tronics' situation required CISO to perform a formal incident breach response (IR) investigation. CISO's IR breach team isolated the environment and identified the root cause. In the face of such an extensive loss, their prognosis determined that Tronics would need to rebuild its IT infrastructure. Combined with the type and extent of the attack, CISO's experts recommended that Tronics move to the Cloud with AWS.

Dew and his team understood the scale and scope of the attack and what it meant to their operations; they realized that this remediation effort was an opportunity for Tronics to implement a lasting and positive paradigm shift. To this end, they worked with CISO toward implementing a new Cloud-based solution.

Criteria for a New Solution

Tronics had three key requirements for any public cloud platform provider:

1. Tronics had a highly developed, customized, and integrated workflow around IP creation and document sharing that was key to its success delivering services to its Fortune 50 clients as well as other customers. This needed to be replicated, or ideally, improved.
2. Tronics wanted a persistent, mature security model for the platform, the underlying instances, and the end user interaction with those systems.
3. Tronics needed all of this in about a week.

Only one public cloud platform could reliably meet all three objectives: Amazon Web Services.

Assessing AWS

CISO's team of AWS Solution Architects immediately began the process of understanding all the workflows and business processes that made Tronics successful. The team devised a Proof of Concept (POC), and it was architected and implemented to validate assumptions and confirm the efficacy of the solution stack. The team also performed a total cost of ownership assessment to ensure the recurring costs were within acceptable tolerances; they identified several AWS services, including FSx and WorkSpace cloud-based virtual desktops, that would retain

Tronic's workflows, demonstrably improve security and recovery capabilities, and reduce its overall cost burden.

The Tronics AWS Environment – Key Elements

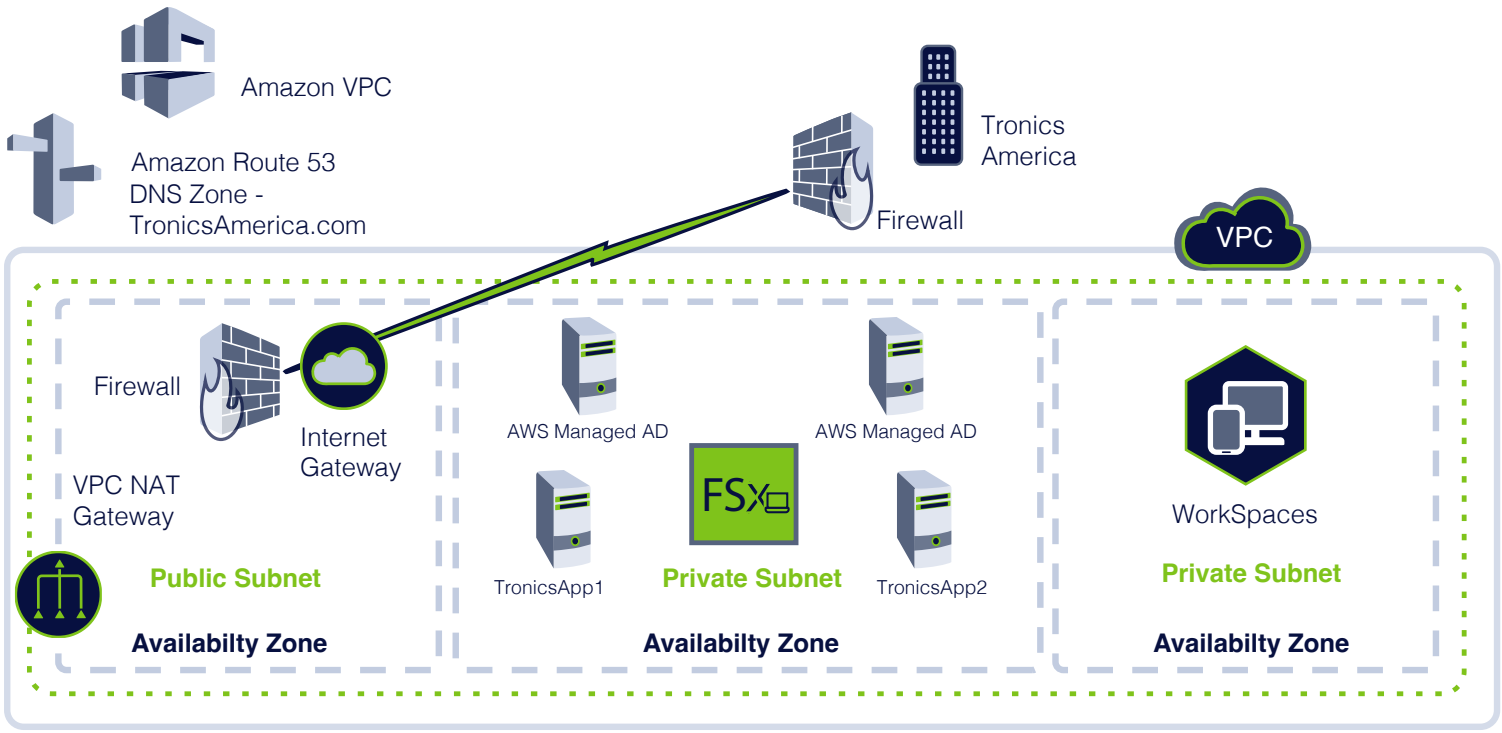
The CISO Cloud Team and Tronics were now on the same page with AWS; Tronics understood the POC, AWS's features and services, and costs involved. But most important, Tronic's goals were assessed as achievable.

Amazon FSx, a fully managed Windows-based file system, allowed Tronics to add encryption protocols for data at rest and data in motion to its workflows, ensuring that its IP and sensitive data remained encrypted. CISO deployed a fleet of AWS WorkSpaces for all employees, ensuring encryption of data on each unit, as well as AWS GuardDuty to monitor abnormal activities on the platform and traffic coming or going from instances. Because the CISO team had determined Tronics' security gaps, they were able to properly deploy least privilege access for each employee. Implementing FSx and WorkSpaces also allowed the team to deploy an end-to-end encryption approach to make sure that all sensitive data was locked down. Backup and recovery capabilities were significantly improved, with Recovery Point Objectives and Recovery Time Objectives measured in minutes. Tronics' environment was hardened without being burdensome, was not overly complex, could be recovered quickly, and could be easily scaled to meet the company's future needs.

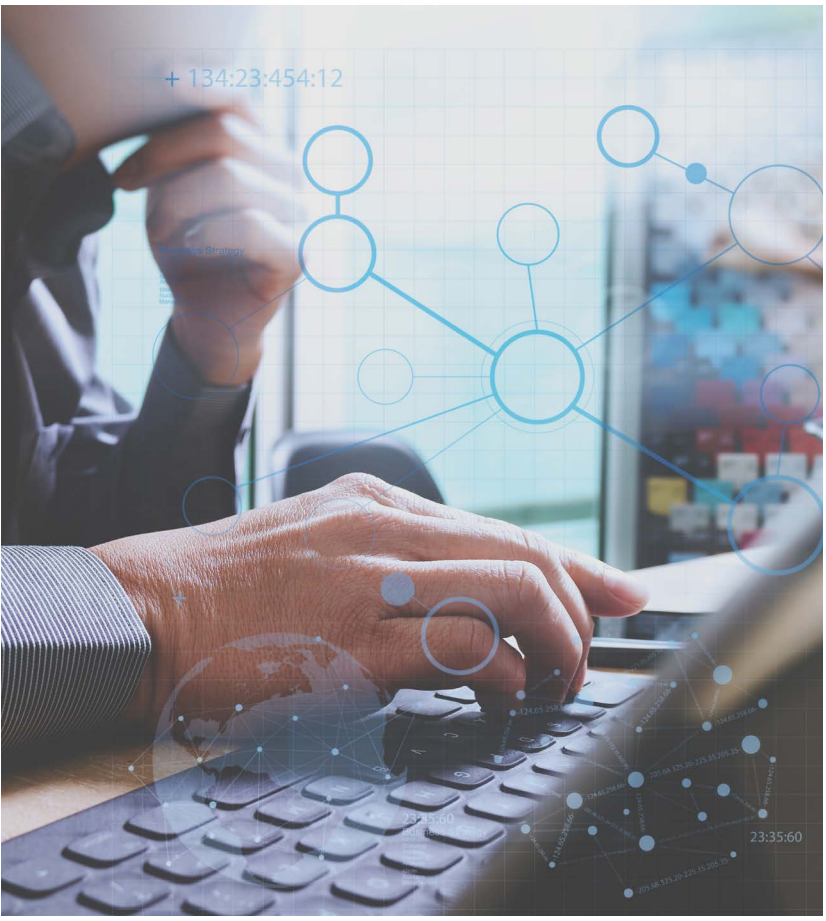
CISO recommends AWS to clients because it simplifies the task of securing an environment through multiple options in preconfigured and premanaged solutions. It offers security, disaster recovery, and other continuity-minded components, so a solution can be customized and tailored to an individual organization's use case. CISO clients using AWS are able to work with holistic IT security experts who can help them leverage and configure these options in a way that is unique to their business needs and gives the assurance that their systems and the data they store are reliably accessible, secure, and scalable. The options are straightforward and easy to understand, so CISO finds clients understand how everything fits together.

Lessons Learned

As part of CISO's emphasis on cybersecurity as a culture, the IR and AWS Solution Architects teams took the opportunity to help educate Tronics on its security posture. This included lessons learned regarding implementing company-wide employee security awareness training about phishing attacks and the



danger of ransomware—what emails are okay to click and what emails need to be flagged and deleted, and the importance of alerting Tronics' security team about suspicious or questionable emails so they can determine if they are safe.



Current State

The Tronics AWS environment is now engineered to be a secure solution—security by design—and Tronics leverages the powerful AWS security and access control options following the shared responsibility model. This is the CISO AWS Solution Architects team's principle: to build controls into the architecture from day one. Tronics has taken a step forward as an industry leader willing to demonstrate for other organizations how to approach their security more holistically, including network architecture, security controls, configurations, information storage and sharing, and the people who interact with all those systems.

The Future With AWS

Tronics was lucky. Though its systems were irrevocably compromised and could no longer operate, the company was able to save a vast majority of its sensitive data. By switching to an AWS toolset, Tronics has leveraged redundancies, disaster recovery and backup strategies, and business continuity plans to handle whatever comes its way. Tronics is protected and poised to scale securely, continuing to serve its valuable client base with the reliability and dependability the company has always delivered.

ABOUT CISO GLOBAL

About Us

A leader in cybersecurity and compliance services, CISO Global brings together expert practitioners and thought leaders to provide tailored solutions that drive cyber resilience. The company's top-tier talent spans geographies, specialties, industries, regulatory frameworks, and focus areas and includes auditors, compliance specialists, certified forensics experts, ethical hackers, security engineers, and around-the-clock analysts.

To learn more, visit www.ciso.inc.

AICPA SOC
aicpa.org/soc4so
SOC for Service Organizations · Service Organizations ™

SOC 2® Type II Audited

CISO GLOBAL

480-389-3444 | www.ciso.inc