PIASC Selects **Acronis** Detection and Response to Secure Critical Data and Systems

Threat-agnostic approach neutralizes ransomware and zero day threats while improving boot times and system performance

BACKGROUND

Printing Industries Association, Inc. of Southern California (PIASC), the trade association or the commercial printing and graphic arts community in Southern California and Clark County, Nevada, has implemented Acronis Detection and Response software. The solution, using OS-Centric Positive Security, was selected to provide a proactive last line of defense to secure critical data and systems.

PIASC administers the Printing Industries Benefit Trust, which provides competitive employee benefits to over 1,000 member companies and their 21,000 employees and dependents. That means it must comply with HIPAA requirements governing the security of the protected health information (PHI).

INCREASING RISKS AND COSTS

Even in the wake of significant data breaches that continue to make news headlines worldwide, organizations across all industries continue to struggle to mitigate the damage a breach can cause. IBM Security's 2018 Cost of a Data Breach Study found that the average cost of a data breach globally is $3.86 million, a 6.4 percent increase from its 2017 report. In the U.S., the news is even worse with the average total cost equaling $7.91 million.

For roughly the past 25 years, the security industry has been focused on preventing hackers from passing the gates. This perpetual cat and mouse game cannot be won. Today, organizations and individuals feel under siege and less secure than ever.

After learning that several member companies had experienced costly breaches, PIASC realized it was time for a new approach.

KEY CHALLENGES

- Guard against cyberthreats
- Managing multiple endpoint security solutions
- Performance degradations

KEY REQUIREMENTS

- Ability to consolidate security solutions
- Improve performance
- Leverage a managed service model to reduce burden on internal IT staff

KEY BENEFITS

- Consolidated from 5 solutions down to 2
- Improved boot times and system performance on devices
- Fully managed service handles all upgrades, maintenance and security issues

PIASC BEFORE ACRONIS

Prior to implementing Acronis Detection and Response, PIASC was concerned about its exposure to ransomware and malware attacks. It was managing as many as five disparate endpoint security solutions, most with overlapping functionality, in a clear case of "the more, the better" that did not address the exposure but frustrated users with performance lags and boot times of up to eight minutes.

To solve these issues, PIASC started evaluating how to:

- Implement industry-leading protection for endpoint devices and servers
- Improve desktop/laptop performance and employee productivity
- Eliminate on-premises infrastructure that the organization would have to maintain
- Achieve hands-off management via a vendor-provided service, alleviating the strain on the IT staff

> "When I came onboard I had an opportunity to rebuild our infrastructure from a clean slate. We believe that the best way to minimize risk is to complement reactive defenses (antivirus) with advanced proactive defenses (Acronis Detection and Response), thereby implementing a complete approach. Anything less creates unwanted exposure."
>
> **Lou Caron,**
> **President and CEO of PIASC**

THE SOLUTION: ACRONIS DETECTION AND RESPONSE

Acronis Detection and Response addresses the biggest cybersecurity challenge in today's digital era: effectively dealing with both current and emerging threats, thus ending the futile cat and mouse game. This unique threat-agnostic approach has proven to successfully neutralize ransomware, evasive malware and zero-day threats. Acronis Detection and Response complements all existing endpoint protection tools, creating true defense in depth security.

PIASC selected Acronis Detection and Response and deployed it within days, reducing the endpoint security footprint to just Acronis and an antivirus solution. Boot times and system performance have significantly improved. To alleviate the responsibilities of the internal IT staff, PIASC chose to leverage the Managed Detection and Response services so Acronis' cybersecurity experts handle all upgrades, maintenance and security issues.

According to Lou Caron, President and CEO of PIASC, "When I came onboard I had an opportunity to rebuild our infrastructure from a clean slate. We believe that the best way to minimize risk is to complement reactive defenses (antivirus) with advanced proactive defenses (Acronis Detection and Response), thereby implementing a complete approach. Anything less creates unwanted exposure." He continues, "Any organization handling PHI and PII should consider the last line of defense approach of Acronis Detection and Response to avoid data breaches and business interruption caused by ransomware and evasive malware."

ABOUT ACRONIS

Acronis unifies data protection and cybersecurity to deliver integrated, automated cyber protection that solves the safety, accessibility, privacy, authenticity, and security (SAPAS) challenges of the modern digital world. With flexible deployment models that fit the demands of service providers and IT professionals, Acronis provides superior cyber protection for data, applications, and systems with innovative next-generation antivirus, backup, disaster recovery, and endpoint protection management solutions.

Founded in 2003 and with dual headquarters in Switzerland and Singapore, Acronis is a global organization that is trusted by 100% of Fortune 1000 companies. Learn more at acronis.com.

Acronis

Learn more at
www.acronis.com