

Manufacturing Better Visibility and Control with Palo Alto Networks

“The PA Series enables us to distinguish between business and non-business applications and decide which applications will run on our network, plus it simplifies our IT infrastructure and makes it easier to use.”

—Pat Wagner, IT Director for Curt G. Joa, Inc.

BACKGROUND

Since 1932, Curt G. Joa Inc. (JOA) has been one of the world’s leading engineering and specialty manufacturers of machinery for the production of disposable products such as baby diapers, sanitary napkins, incontinent pads and related single use items. The company employs an array of existing converting modules and builds, tests and verifies the process on its own test stands for producers in more than 55 countries worldwide. With this approach, JOA can provide shortened machine delivery schedules, validated process concepts and sample products for test markets for its customers.

RUNNING THROUGH VENDORS. RUNNING OUT OF PATIENCE

As a leading engineering and specialty manufacturer of machinery, JOA’s IT team oversees a global corporate network that monitors high volumes of incoming and outgoing email traffic and application usage. It is paramount for the company to protect its network from increasingly sophisticated network threats, and maintain control over access to Web 2.0 and other rich Internet applications. To achieve these objectives it must be able to identify applications, users and threats at a highly granular level to limit non-business traffic as necessary -- all without adversely affecting the firm’s critical business activities.

To date, JOA was somewhat disappointed in the network security solutions it had deployed, which included legacy firewalls and proxies. “Our existing firewalls and proxies weren’t giving us the control, visibility and reporting tools we needed,” explains Pat Wagner, IT Director for JOA. “Our proxy only let us do lookups and put out warning messages. I wasn’t real happy with the logs because they only produced IP addresses. With hundreds of users, it meant we were looking up addresses all the time.”

Despite these limitations and cumbersome reporting functionality, Wagner thought her IT infrastructure was doing a decent job of protecting the company from threats. That is, until she learned what Palo Alto Networks could do. Wagner was intrigued by the unparalleled level of visibility and granular control of applications the Palo Alto Networks PA Series next-generation firewall promised. Skeptical, she arranged a trial. “We ran the PA Series on a customer’s network and on our network head-to-head against our incumbent proxies to see what each picked up,” describes



ORGANIZATION:

Curt G. Joa, Inc.

INDUSTRY:

Manufacturing

CHALLENGE:

Lack of visibility and control of applications and websites; poor reporting and usability from existing network security technology.

SOLUTION:

Replace proxies and URL filtering with PA Series for an unparalleled level of visibility and granular control of applications by user.

RESULTS:

- Application visibility and control
- Enforce granular application usage policies
- Reduced risk from threats
- Upgrade and consolidate network infrastructure

"I don't get enthusiastic very often, but the PA Series thrills me. I can easily go in to see user activity, denied sources or anything. It's simple, intuitive and effective."

Pat Wagner,
IT Director,
Curt G. Joa, Inc.

Wagner. "We were shocked to discover that our proxy wasn't recording things it found onto the log report. It simply stopped logging at certain points and would lose everything it had previously recorded. We also thought it was blocking and picking up everything it should have, but it wasn't. We were extremely impressed by what the PA Series caught that our existing infrastructure didn't."

VISION AND INFORMATION = REDUCED THREATS

Based upon its impressive performance during the trial, JOA chose the PA Series to identify traditional and emerging applications – including those that are SSL encrypted – and to equip it to create and enforce appropriate use policies down to the individual user and application. Upon fully implementing the PA Series, JOA discovered more threats and prohibited applications that had been slipping past its old firewalls and proxies – such as Peer-to-Peer (P2P), Instant Messenger (IM) and spyware – which had clearly been impacting performance and productivity.

Wagner and her team now benefit from granular, readily understandable network reports on individual users' application usage, a capability not possible with its previous infrastructure. "I can't tell you how many times I wanted a report for the business and couldn't get it," states Wagner. "I need my security solution to give me the information I need when I need it, like the PA Series does. It is a great network visibility tool that makes it easy for me to go in and see who's doing what, where they're going and what the threats are."

Now JOA has enforceable security policies in place and has mitigated its exposure to threats -- all without sacrificing employee productivity. And, by upgrading its IT infrastructure to Palo Alto Networks, JOA has the ability to replace two appliances with just one - the PA Series. "There is no downside whatsoever to the PA Series," Wagner says. "It's a great, comprehensive solution."



Palo Alto Networks
232 E. Java Drive
Sunnyvale, CA. 94086
Sales 866.207.0077

www.paloaltonetworks.com