

# Mykonos Software Secures Brown Printing Web Applications in Real-Time

Brown Printing Company, headquartered in Waseca, Minnesota, is the third largest magazine printer and the fifth largest catalog printer in the United States. The company has more than 2,200 employees and operates three state-of-the-art web off-set printing facilities that produce over 1,000 different magazines and catalogs.

## Business Security Problem

Brown Printing Company's security infrastructure relied on traditional network firewalling techniques and is comparable to others in similar industries. The IT Infrastructure team is effective at dealing with network level intrusions, but had limited visibility into malicious behavior taking place at the web application layer (Layer 7).

**10% of our traffic was in some way malicious.**

Business and technology changes require Brown Printing Company to increasingly rely on its Web applications to communicate

bi-directionally with its customers and client base. The company's goal was to ensure their Web application layer was as secure as possible. They wanted full visibility into what was happening with their Web applications and were seeking a solution that could protect their business from the disruption of malicious attacks. The company looked at traditional signature-based Web application firewalls (WAF's) but the budgetary concerns, along with the prospect of spending countless resource hours configuring and managing the WAF, made purchasing a WAF a difficult solution to justify.

## Why Mykonos Software Was Selected

Brown Printing Company had three requirements for meeting its Web application security goals:

- ▶ **Attack visibility** – A real-time detection security product that shows abusive and malicious behavior taking place on their Web application.
- ▶ **Prevention of attackers** – Real-time prevention was deemed vital. Unlike traditional security solutions that require IT Security teams to scour a log-file of malicious behavior that took place sometime in the past month. Brown Printing wanted a solution that prevented threats immediately.
- ▶ **Easy deployment and configuration** – Required an advanced technology with easy deployment and simple configuration and management without requiring countless hours of IT security resources.

Brown Printing's IT professionals chose the Mykonos Web Security because "the Mykonos technique is different from anything else in the market and detects real-life attackers in a very innovative way. Within 20 minutes, we had the Mykonos Web Security up and running and we were looking at the activity taking place on our web applications", said Keir Asher, Senior Technical Analyst, Information Technology.

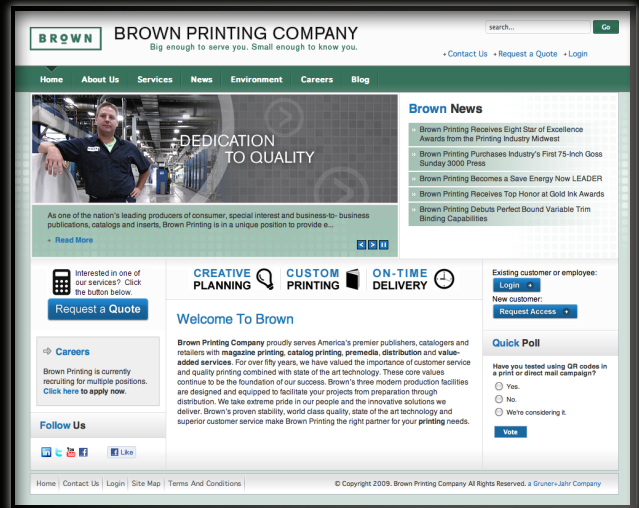
## About Mykonos Software

Mykonos is the smartest way to protect Websites and Web applications against hackers, fraud and theft. Using deception-based techniques, its Web intrusion prevention system detects, tracks, profiles and prevents attackers in real-time—with no false positives.

**Headquarters**  
370 Brannan Street  
San Francisco  
CA 94107  
USA

**Rochester, NY Office**  
4 Commercial Street  
Suite 101  
Rochester, NY 14614  
USA

**Website:** www.mykonossoftware.com  
**Phone:** 650.329.9000  
**Toll free:** 877.88WINGS  
**Email:** sales@mykonossoftware.com



## What the Mykonos Web Security Detected

During the first month of deployment there were 210 malicious incidents against Brown Printing's Website. This activity came from three sources—malicious spiders, malicious bots, and malicious users. Five real-time attackers were detected on the site. These attackers used hacking techniques associated with seeking sensitive information such as credit card or social security numbers but were unsuccessful at creating an attack.

*“We were surprised by how many incidents we detected on our site. 10% of our traffic was in some way malicious. Before installing the Mykonos Web Security we were unaware of how frequent the malicious attacks were occurring on our site.”*

**Keir Asher, Senior Technical Analyst, Information Technology**

