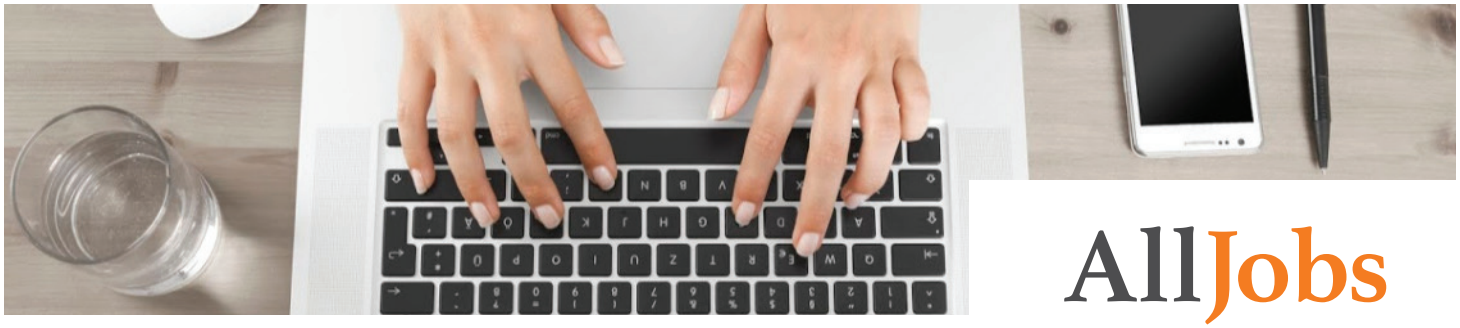
Reblaze

Web Application and API Security



AllJobs

High-Traffic Job Site Gets ‘Effortless’ Web Security

As the largest job board in Israel, AllJobs (www.AllJobs.co.il) faces similar challenges to other high-profile websites: frequent large-scale hacker attacks, constant attempts at data theft, and high requirements for data security.

Despite all this, AllJobs’ CTO Bonnie Grossman says, “I sleep well at night.”

It wasn’t always this way. As a prominent site with over one million unique visitors per month, AllJobs has long been a high-profile target for attackers and data thieves. AllJobs’ developers were constantly trying to update the site’s defenses against ever-evolving Internet threats.

Challenges with PCI DSS Compliance

Additional issues arose each quarter during AllJobs’ mandated PCI DSS scans. These scans ensure compliance with requirements set by the Payment Card Industry Security Standards Council.

As is typical for a high-profile site, AllJobs needed to commit substantial developer resources towards maintaining compliance.

Cyberattacks Get Worse

Then a large wave of attacks hit many Israeli websites, including AllJobs. This was the first occurrence of what is now known as “OpIsrael”: a periodic, internationally coordinated cyber-assault designed to “erase Israel from the Internet.”

The first OpIsrael attack drove Mr. Grossman to find an effective security solution. Although many products were available, most were unattractive: “With all those solutions I would need someone on my team to maintain them, make new security rules, check that the new rules aren’t doing any harm, and so on.”

After researching his options, he decided to try Reblaze.

(next page, please)

Industry

Employment and Recruiting

Challenges

- Defending against periodic large-scale attacks, while maintaining site availability to over one million users per month.
- Eliminating data theft & scraping.
- Implementing an effective security solution with minimal burden on IT staff resources.
- Maintaining PCI DSS compliance.

Solution

Reblaze was tested and then deployed as a comprehensive security solution.

Results

- Internet attacks (intruders, DDoS traffic, and scraping bots) are blocked automatically.
- Staff requirements are minimal: “Reblaze just works.”
- Security updates & upgrades are deployed across the network with no action required from IT staff.
- Full PCI DSS compliance is achieved and maintained automatically.

Reblaze is a next-generation platform that provides comprehensive, robust web security. It runs in the customer's cloud environment, protecting them from all forms of Internet attacks: system intrusion, data theft and scraping, DDoS (Distributed Denial of Service), and more.

Mr. Grossman found it especially appealing that he could test Reblaze with little effort and no risk. As he recalled, "There was nothing to lose, and everything to gain. The Reblaze team did all the work for me.

"And I liked that you can put the platform into a learning mode where it doesn't actually affect your traffic—it just watches and learns how your legitimate users behave. So I could test Reblaze with no risk at all."

After deployment, the AllJobs team used its learning mode to monitor their traffic. Mr. Grossman explained, "After one month of learning the rules and seeing how my visitors use the site, we saw all the rules we were going to activate. Then we went live."

Immediately Effective

Once Reblaze went into active mode, attacks against the AllJobs website ceased immediately. Even large-scale assaults are now filtered out automatically.

The AllJobs team was surprised at how effective it was. Mr. Grossman said, "I thought I would have to talk to the people at Reblaze, especially at first, asking them to change the rules because we're still getting attacked, or we're getting false alarms and my users can't surf my site, or some other problem. But there was nothing like that."

The platform also updates itself automatically as needed. Even as new Internet threats arise, the Reblaze team issues upgrades across the network to protect their clients. Again, no user action is required.

When Mr. Grossman was asked if Reblaze created any work for his IT staff, he replied that there was none. "If Reblaze took me more time than nothing, I'd turn it over to my senior developer and let him deal with it. But there's nothing to deal with. Reblaze just works."

"The implementation process went very quickly. And best of all, it required no work from me."

"Before Reblaze, maintaining compliance was challenging. Since we deployed Reblaze, every scan has been clear."

"The reason I chose Reblaze and still use it, is because I do no work at all. That's very important to me. It just works."

Bonnie Grossman, CTO, AllJobs

Reblaze: Web Application and API Protection (WAAP)

Core technologies include:	Added value services include:	Contact:
Next-Gen WAF/IPS, Multilayer DDoS Protection, Precise ACL, API Security, ATO Prevention, Scraping Prevention, Advanced Human Detection and Bot Management, Unified Management Console, and Real-Time Traffic Analysis.	Mobile/Native Client SDK, Layer 7 Load Balancing, Global Secured CDN, and a complete DNS solution.	contactus@reblaze.com Int'l: +972 (73) 200-5200 U.S./Canada office: (408) 907-7712 www.reblaze.com