

DOTComm Eliminates False Positives and Hundreds of Hours Managing SSL Certificates with Akamai Web Application Protector



Keeping up with emerging threats, layer 7 rules, and SSL certificates is time-consuming. Web Application Protector is a cost-effective solution that alleviates us of those tasks so we can focus on delivering business value to our county.

– Jim Dolinski, Web Application Developer, DOTComm

Ensuring Secure, Reliable Access to Critical Resources

Established in 2003, Douglas Omaha Technology Commission (DOTComm) provides technical support and consulting to over 70 governmental entities in the Omaha and Douglas County area of Nebraska. More than 5,000 government workers spread across 120 locations rely on DOTComm services every day.

Jim Dolinski – who has worked for DOTComm for more than 20 years – is in charge of web application development and integrations for the organization. His team supports more than 100 sites and applications serving over 100 government departments. As part of delivering on its mission, this team needs to ensure the availability and security of these resources while working with limited resources and budget. To that end, they have been increasingly taking advantage of cloud-based solutions.

Struggling with Web Security Challenges

In 2016, rather than invest millions of dollars to replace its outdated legacy infrastructure, DOTComm began migrating its sites and applications to a large cloud services provider. The organization also used a cloud-based web application firewall (WAF) along with robust alerting tools that enabled it to monitor for outages.

Unfortunately, the WAF did not perform as expected. Over a two-year period, DOTComm experienced more than 10 outages, each of which brought down a subset of the organization’s websites and applications. These outages lasted



COMPANY

Douglas Omaha
Technology Commission
Omaha, Nebraska
www.dotcomm.org

INDUSTRY

Public Sector

SOLUTIONS

Web Application Protector

KEY IMPACTS

- Eliminated unplanned site outages
- Saved 100 hours annually managing SSL certificates
- Enabled legitimate site traffic more easily
- Freed the team to refocus on delivering business value
- Established strategic partnership with professional security experts

DOTComm Eliminates False Positives and Hundreds of Hours Managing SSL Certificates with Akamai Web Application Protector

anywhere from 15 minutes to several hours – an unacceptable amount of time when they impacted the availability of 24/7 mission-critical services related to public safety.

Even when the outages affected less mission-critical DOTComm sites and applications, the organization had to deal with complaints from county departments and citizens. Because the WAF vendor refused to take accountability for these outages, Dolinski was forced to pore over his log files to prove that the issue was the vendor's responsibility. Once engaged with the vendor for support, Dolinski was often frustrated by dealing with entry-level personnel who lacked deep knowledge of the WAF.

To make matters worse, the WAF vendor was supposed to manage DOTComm's SSL certificate renewals. However, lacking a graceful certificate renewal process, the vendor often failed to renew DOTComm's certificates before they expired. As a result, DOTComm sites would either go offline or throw SSL errors.

As soon as the contract with the WAF vendor expired, Dolinski began to evaluate other solutions.

Improving Its Security Approach with Web Application Protector

At first, Dolinski opted to take advantage of its cloud provider's WAF. "This is a good solution, providing basic rules, and it solved our certificate renewal issues. But we don't have the resources nor the time to keep up with emerging threats and write and maintain more sophisticated WAF rules," he explains.

Dolinski realized that by using the cloud provider's WAF, DOTComm wasn't catching and blocking as many threats as it should – in spite of running security at many layers of its infrastructure.

With a clear understanding of DOTComm's security needs and gaps, Dolinski looked for a solution with a managed rule set that monitored for active threats. He also wanted to work with a professional, responsive vendor that took ownership of its product. Akamai and its Web Application Protector solution fit the bill.

By leveraging Akamai's experienced professional services team, DOTComm avoided common WAF implementation stumbling blocks. "With the guidance and best practices of Akamai's experts, we quickly migrated our first four sites. They prepared us to set up our environment for the future, and within a week, we migrated another 60 sites on our own," explains Dolinski.



He wanted to work with a professional, responsive vendor that took ownership of its product."

DOTComm Eliminates False Positives and Hundreds of Hours Managing SSL Certificates with Akamai Web Application Protector

Refocusing on Delivering Business Value

Ultimately, DOTComm plans to onboard all its websites and applications to the Web Application Protector solution.

“We love the automatic rule updates because we don’t need to keep track of the latest security threats,” says Dolinski.



We love the automatic rule updates because we don’t need to keep track of the latest security threats.”

In addition to immediately seeing fewer denials of service, DOTComm has virtually eliminated false positives and unplanned outages. This means Dolinski and his team have saved hundreds of hours because they are no longer troubleshooting these types of incidents. Plus, county employees and constituents no longer complain about websites and applications being unavailable because of outages.

Dolinski appreciates the real-time visibility that Web Application Protector provides into detected attacks. “With our previous solution, it was difficult to drill down and figure out which rule was blocking traffic and why. The Akamai solution makes it easy to identify why traffic has been blocked,” he continues.

Whereas Dolinski’s teams spent about 100 hours annually addressing certificate renewal issues previously, it now spends no time. “Akamai Web Application Protector enables us to push web security to trusted experts, freeing us to refocus on delivering business value instead of writing security rules,” he concludes.



DOTComm provides technical support and consulting to over 70 governmental entities in the Omaha and Douglas County area. Over 5,000 dedicated government workers spread across 120 locations rely on our services every day. With a 24/7 service center and service offerings across all IT disciplines, we are a unique blend of talented individuals who are continually striving to better serve our clients through actively living our Mission, Vision and Values. For more information, visit <https://www.dotcomm.org>.



Akamai secures and delivers digital experiences for the world’s largest companies. Akamai’s intelligent edge platform surrounds everything, from the enterprise to the cloud, so customers and their businesses can be fast, smart, and secure. Top brands globally rely on Akamai to help them realize competitive advantage through agile solutions that extend the power of their multi-cloud architectures. Akamai keeps decisions, apps, and experiences closer to users than anyone – and attacks and threats far away. Akamai’s portfolio of edge security, web and mobile performance, enterprise access, and video delivery solutions is supported by unmatched customer service, analytics, and 24/7/365 monitoring. To learn why the world’s top brands trust Akamai, [visit www.akamai.com](http://www.akamai.com), blogs.akamai.com, or [@Akamai](https://twitter.com/Akamai) on Twitter. You can find our global contact information at www.akamai.com/locations.

Published 08/19.