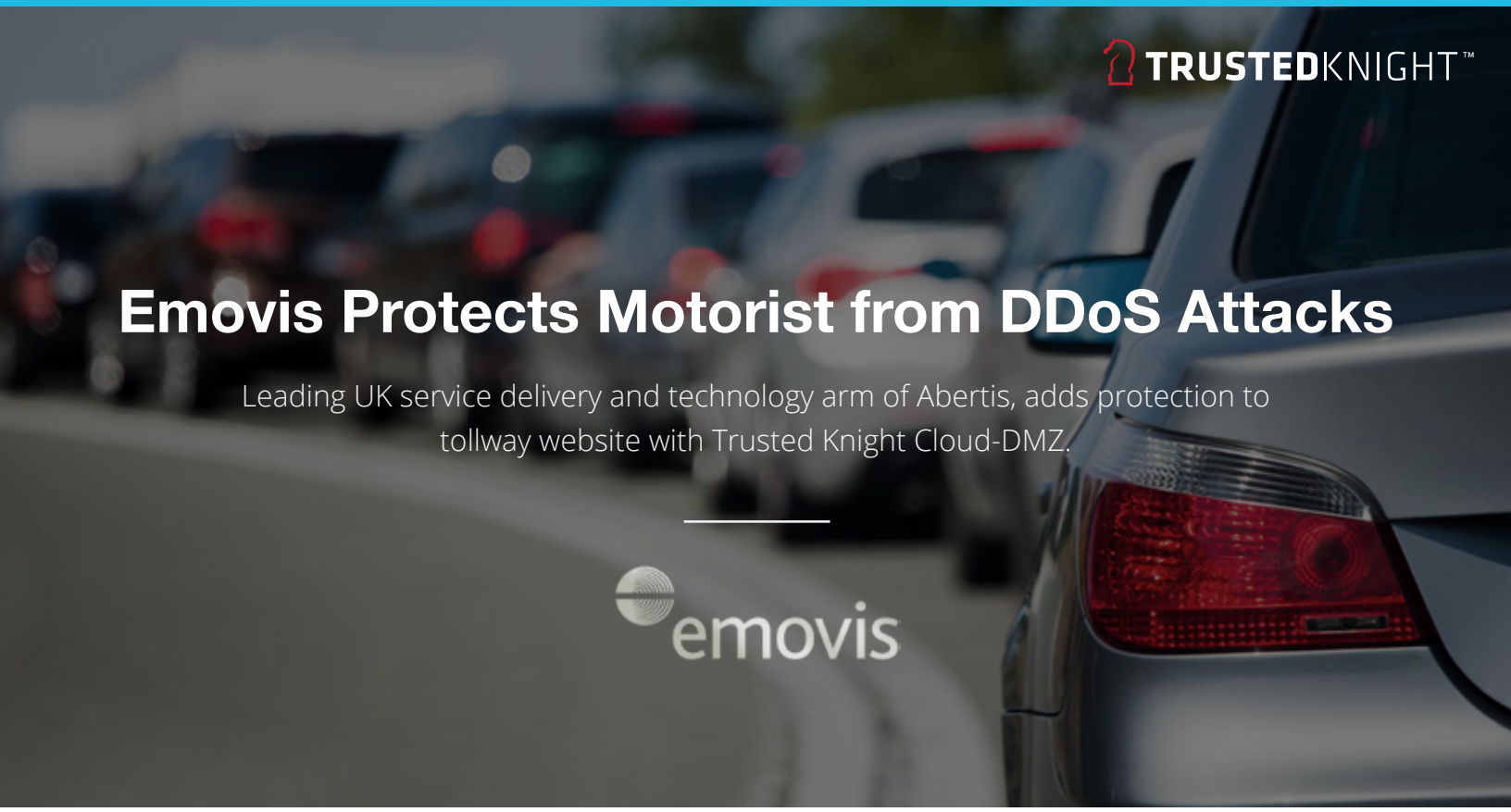

Emovis Protects Motorist from DDoS Attacks

Leading UK service delivery and technology arm of Abertis, adds protection to tollway website with Trusted Knight Cloud-DMZ.

Emovis is the leading service and delivery arm of Abertis in the global market for management of electronic tolling and smart mobility solutions. With their focus on keeping roads moving through electronic tolling around the globe, they are also a clear target for web-based attacks on their ecommerce applications.

When Emovis was chosen by the UK government for a seven-year contract to operate the Dartford Crossing, where more than 160,000 vehicles pass daily, it came with rigorous digital standards required for all government agencies and service providers. Emovis was up for the challenge of finding the right solution to a variety of requirements.

Key Requrements:

The Digital Service Standard is a set of 18 criteria to help the UK government create and run user-friendly digital services. All public facing transactional services must meet the standard.

Included in these standards are requirements to ensure a consistent user experience with other government services, that the site be built with agility in mind for easy updating and that user information is kept secure while transacting. In particular, the government is concerned about the potential for Distributed Denial of Service (DDoS) attacks.

With the significant e-commerce component of the Emovis tolling website, they were considered a high-risk target for DDoS attacks. As such, the government required Emovis to find an agile solution to keep user data safe from DDoS attacks, man-in-the-browser attacks and other web-born vulnerabilities.

Solution:

Emovis selected Trusted Knight's Cloud-DMZ as the best preventative solution in combating DDoS attacks and other web-born vulnerabilities. Cloud-DMZ is a true cloud-based web application firewall (WAF) and an alternative to a conventional DDoS mitigation solution.

The Cloud-DMZ approach processes web systems to understand the application and how users access information, and then creates an agile replica of the original website to respond instantly to requests, reducing the need for back-end processing.

The secure replica website is deployed in the cloud and can easily scale when a volumetric attack grows. As a result, Cloud-DMZ contains any level of DDoS attack without impacting user experience and with virtually no attention from internal IT or security teams.

Detecting and mitigating DDoS Traffic

Emovis wanted to do more than just block suspicious traffic that may produce false positives and keep legitimate users from accessing their ecommerce application.

Emovis found Cloud-DMZ was the most technically secure solution available. With Cloud-DMZ, malicious traffic is selectively blocked avoiding impact on customer experience. This is accomplished by using highly granular, contextual data and attack surface reduction and intelligent throttling of traffic to ensure legitimate requests are never blocked.

Instant and Agile Protection

Emovis needed to ensure that with frequent user experience updates their application releases wouldn't be held up by complex, hard to manage security products like traditional web application firewalls (WAF).

Cloud-DMZ deployment is automated and fast, which means web applications are instantly protected against DDoS on public facing areas as well as the frequently targeted post-login areas. Because 99% of the attack surface is removed via the secure replica, and traffic reaching the backend systems is highly monitored by security policies, reducing the responsibility of the security team's focus to a fraction of the original scope.

RESULTS

Emovis saw immediate protection against DDoS attacks and web-based vulnerabilities. The Cloud-DMZ infrastructure has eliminated the threat of stolen user data and allowed the Emovis team to focus on user experience because their teams are not overwhelmed with security alerts or maintenance requirements.