crownpeak

Advanced Cybersecurity and Edge Protection

Front-line cybersecurity protection for your entire web presence

Despite spending millions to establish secure networks, organizations of all sizes continue to face cybersecurity threats. As a result, hackers gain access to protected data, financial information, and intellectual property. To make matters worse, security operations centers (SOCs) may be so overwhelmed with alerts that they miss critical attacks - or detect them after vital data has been compromised.

Advanced Cybersecurity and Edge Protection from Crownpeak is a fully-managed service capable of defending against the most common and damaging cybersecurity threats. From sophisticated, multi-layer DDoS attacks, to vulnerability exploitation attempts and intelligence gathering, our Advanced Cybersecurity and Edge Protection is an unobtrusive defensive perimeter that can be rapidly deployed to any site or application without negative impact on visitor engagement or visitor experience.

Advanced Cybersecurity and Edge Protection features multilayered defensive capabilities that extend right out to the visitor's browser, helping ensure the security and availability of your sites and applications, as well as protecting your customer's data and ultimately, confidence in your brand. The service's innovative combination of real-time traffic inspection, defensive capabilities and continuously updated threat intelligence all work together to ensure your organization's security posture is ready to face a constantly evolving online threat landscape.

Crownpeak provides:

Application Performance Monitoring (APM): Application Performance Monitoring empowers developers and operational teams with detailed insight and analytics of the applications they run on Crownpeak. Our Advanced Performance Monitoring Software analytics help ensure easier diagnosis of application errors and discovery of opportunities to improve performance and visitor experience.

DDoS Protection: DDoS is an attempt to exhaust the resources available to a site or application in order to impair its ability to service legitimate traffic. Crownpeak Advanced Cybersecurity and Edge Protection automatically blocks the sources of both application layer and network layer attacks helping ensure your sites and applications remain open for business.

Vulnerability Exploitation: Web-application vulnerabilities can be exploited to gain access to systems and exfiltrate personal data. Crownpeak's Advanced Cybersecurity and Edge Protection combines real-time HTTP/S traffic inspection, threat intelligence, and stealth measures to detect vulnerability exploitation attempts, block traffic from common sources of criminal activity, and reduce exploitable information exposed by sites and applications. Using the service as part of an application security program enables customers to protect their digital experiences from common vulnerabilities including the OWASP Top 10.

Spam Protection: Spam continues to be a burden to marketing and operations teams. From junk form submissions to the poisoning of analytics and the subsequent impact on business decision-making, Crownpeak's Advanced Cybersecurity and Edge Protection reduces exposure to spam using a combination of bot detection with threat intelligence to block traffic from a range of recognized sources of cyber-crime and automated spam.

Threat Intelligence: Through professionally-sourced lists combined with our own regularly updated index of known threats, Crownpeak's Threat Intelligence prevents access to your sites and applications from recognized sources of malicious activity.

Why Choose Crownpeak's Advanced Cybersecurity and Edge Protection

Benefits include:

- Cybersecurity domain expertise - Crownpeak handles all strategy, configuration, and implementation giving customers the level of protection needed to filter out malicious traffic, while ensuring legitimate traffic gets access.
- Constant evolution - As new threats in the marketplace emerge, Crownpeak stays ahead of them, making and releasing adjustments as needed, often in real-time.
- Quick and seamless integration - Can be implemented and configured with minimal service interruption.
- Collective intelligence - Threat intelligence is pooled so a defense is continuously evolving. By observing an attack against one customer, Crownpeak will assess the applicability of the defense to the broader base and make it immediately available for all customers.

