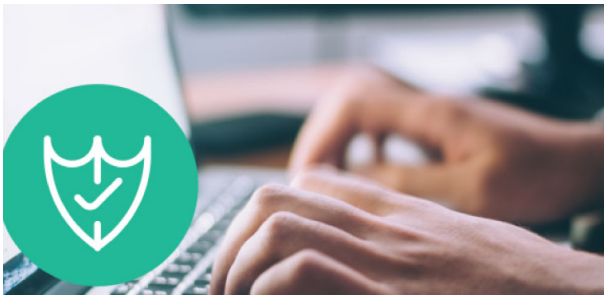
AudienceView's Cybersecurity: Preventing & Protecting Against Breaches

5 MIN READ



Enhanced Security Measures. Steps Taken to Safeguard AudienceView's Campus, Professional, and Unlimited Products.

Companies across the board have been affected by cybersecurity breaches, compromising sensitive data and exposing the vulnerabilities of their systems. From companies like Yahoo, Marriott, Target, Capital One, and Sony Pictures to your ticketing provider, robust cybersecurity measures are crucial to safeguard sensitive information and mitigate the potential risks associated with cyber threats.

As cyber threats become increasingly sophisticated, organizations must remain vigilant in their efforts to safeguard sensitive data. At AudienceView, we prioritize cybersecurity as a fundamental aspect of our operations. In this article, we will shed light on the comprehensive security measures implemented by AudienceView across their suite of products, demonstrating their commitment to breach prevention, protection, and advanced security tools.

Enhanced Infrastructure and Advanced Security Tools for AudienceView Products

At AudienceView, we prioritize cybersecurity as a fundamental aspect of our operations. We continually invest in enhancing our infrastructure to establish a strong and secure architecture specifically tailored for AudienceView products. By optimizing our footprint, we achieve improved efficiency without compromising on security. Additionally, we integrate advanced security tools that proactively scan for potential threats and monitor any abnormal activities, ensuring the utmost protection for AudienceView products. These advanced security tools enable us to stay one step ahead of cyber attackers, providing a robust and resilient security infrastructure for our valued clients.

By collaborating with Mandiant, a renowned cybersecurity company, we further enhance our ability to safeguard client data and combat potential threats. This collaboration allows us to leverage Mandiant's expertise, advanced technologies, and proactive monitoring capabilities, reinforcing our commitment to maintaining the highest standards of cybersecurity. Through this partnership, we strive to provide our clients with a robust and resilient security infrastructure, offering them peace of mind in an increasingly complex digital landscape.

Web Application Firewalls

Web application firewalls (WAFs) act as intelligent gatekeepers across our products, reinforcing our defensive capabilities and scrutinizing incoming and outgoing data packets for any signs of malicious intent. By swiftly blocking harmful content, we create a robust barrier against cyber threats, ensuring the integrity of your data. Our web firewalls align with industry best practices, further enhancing our security measures for AudienceView products.

Security-First Development Practices

At AudienceView, our development practices revolve around a security-first approach. We have instilled a culture that places paramount importance on security throughout the development lifecycle. Regular code scanning and automated server patching allow us to proactively identify and address vulnerabilities. Furthermore, secure coding practices protect sensitive information from potential exploitation. By ingraining security into every stage of our development process, we mitigate risks and enhance the overall protection of your data.

Additionally, we have taken significant steps to enhance internal protocols and promote a security-focused culture within AudienceView. Our comprehensive anti-phishing training programs raise awareness about phishing attacks and empower our team to identify and respond to potential threats effectively. We enforce elevated password requirements, implement robust access controls, and authentication protocols to ensure stricter measures around document and application accessibility. These measures collectively bolster our internal defenses and reinforce our commitment to protecting sensitive information from unauthorized access or misuse.

Data Validation and Filtering

To safeguard our clients’ data, we have implemented stringent data validation and filtering mechanisms. Our systems are designed to thoroughly validate all input fields, rejecting any content that may pose a security risk. For instance, we actively scan and filter out freeform fields containing credit card numbers or primary account numbers (PAN). This extra layer of protection ensures that your valuable data remains secure within our systems.

Continual Investment and Adaptation

We recognize that cybersecurity is an ongoing battle, with threats constantly evolving. To maintain the highest level of protection, we are committed to continual investment in cutting-edge technologies and practices. Our dedicated security teams remain vigilant in monitoring emerging threats and swiftly implementing necessary countermeasures. By staying ahead of the curve, we ensure that your data is shielded from potential security breaches in the ever-changing cyber landscape.