Ziff Davis Information & Data Security Practices

Ziff Davis has a mature security program designed to provide high-quality services for our customers and to protect customer and company data and information assets. Ziff Davis' information security program ensures the confidentiality, integrity, and availability of our client and customer data through effective security management practices and controls. The objective of this document is to address questions that prospective and existing customers may have regarding our security program.

Ziff Davis has a comprehensive and holistic approach to risk management which encapsulates measures generally understood to be best practices with regard to cybersecurity, assiduous regard for data protection and the stewardship of the privacy of our users and employees, an aggressive strategy towards simplification of technology infrastructure, and a rigorous process of continuous evaluation and systems audit - executed by internal resources and independent third parties.

CyberSecurity

Ziff Davis' Information Security department, under the guidance of our CISO, has instituted enterprise-wide standardization of the key pillars of cybersecurity: "Table Stakes" security, next-generation endpoint protection, threat stream monitoring, vulnerability scanning, employee awareness, and employee onboard/offboard automation.

Table Stakes

Ziff Davis' Corporate Security Policy details the security requirements that allow our company to provide high-level and secure service to our customers. There are company-wide standards for password composition, rotation, management, and storage. Workspace and database encryption(all databases must be encrypted at rest and all data encrypted in transit)is required, along with multi-factor authentication for all systems that support it. Access control to Ziff Davis systems is closely vetted and reviewed as well. Ziff Davis systems must be properly hardened and vetted before connecting to our network to ensure the protection and privacy of data

Next-gen Endpoint Protection

All workstations and all product environments (Dev, QA, staging, production) must be outfitted with endpoint protection agents that scan not only for known malware, but also constantly monitor for system activity that falls within the scope of what is considered questionable. The software we employ is configured to instantly kill processes that it identifies as anomalous and operating beyond what's expected of ordinary system activity (as determined by baseline analysis on a BU-by-BU basis). The software is employed across the entire enterprise to ensure complete security coverage of all of Ziff Davis' brands. All Business Units must make use of the specific solution we've selected, and all data generated by the software is channeled to a central security data repository for analysis and presentation to the executive tier in the form of security dashboards.

Threat Monitoring

All systems throughout Ziff Davis are also required to support and host agents which bundle activity logs and send them to a central command center provided by our threat stream analysis vendor. We have vendor-managed services for 24/7 SOC analysis with dedicated resources responsible for sifting through possible security events, false positives, and surfacing only those events we have characterized as of interest to our in-house team of InfoSec analysts. Our team then responds to, escalates the alerts, and, as necessary, issues directives to the technical staff of the Business Unit in question with recommendations for both the process and timeline of remediation. Just as with the data from endpoint protection, all of the threat stream data is poured into a central security intelligence repository for analysis and executive consumption.

Vulnerability Management

Across the enterprise, Ziff Davis has a three-pronged approach toward vulnerability management: We employ a third-party service to perform internal scanning of our production and corporate networks, surfacing any potential frailty associated with end-of-life software, exposed ports, associated platform and software weaknesses, etc. In addition, on a rotating basis, we subject each Business Unit to external penetration testing executed by an independent third party. For both of the preceding, we report any discovered weaknesses to the relevant BU with recommendations for method and timeline for remediation. Finally, our Application Security team engages in regular "White Hat" ethical hacking exercises, the results of which are similarly shared with the BU. Recommendations are communicated with the BU to implement rapid remediation of any identified issues. As with all of the preceding, metrics data resulting from these efforts are automatically funneled to our central security intelligence platform.

Employee Awareness

Ziff Davis uses third-party providers of educational material to institute a regular cadence of mandatory employee training sessions for all employees designed to educate them on sound Information Security and Data Protection practices and alert our employees to the many warning signs of potentially malicious activity by bad actors intent on phishing, spear-phishing, deploying ransomware, etc. Employees are also educated on relevant security and privacy regulations, such as GDPR, CCPA, and PCI. Targeted training is given to certain departments or brands to fulfill our compliance obligations. Additionally, we randomly subject individual business units - and the company at large - to unannounced simulated phishing attacks, designed to test the ability of our workforce to use the training they've received to properly react to potential threats.

Employee Onboard / Offboard Automation

All global enterprise platforms are integrated with the principal source of truth of employee status. We have built a dynamic environment of end-user software and APIs that empower the Business Units to procedurally determine current employee status with the ease of an HTTP request. In addition, we are rolling out a single-sign-on solution that channels all system access for all employees into a single point of control. At present, our systems are directly informing regional IT and technology managers, who grant and revoke access on the basis of this automated data stream. At completion, the majority of that type of activity will be automated, and all of it predicated on the status of the employee as explicitly indicated by HR.

Data Protection and Privacy

Long before the advent of the institution of GDPR, Ziff Davis engaged in a comprehensive series of Privacy Impact Analyses across all business units, assisted and guided by an independent third party. Subsequent to the execution of the PIAs, we appointed a Data Privacy Officer and set about the process of creating a procedural approach to handling Data Subject Access Requests. The end state of those efforts is a fully automated process of protecting the rights of our employees and our users across all business units. A central platform for dispatching the requests was created, with a corresponding API tier that allowed each business unit to programmatically respond to the requests. We have adopted the most constrained interpretation of both CCPA and GDPR across the enterprise and respond to each request according to that standard.

Information Security Incident Response

Ziff Davis has a management team and process for information security incidents as set forth in its detailed Information Security Incident Response Plan. This plan details roles & responsibilities, procedural steps, and general incident response best-practices. Other crises are handled by the legal, internal audit, technology, security, HR, and C-level executive groups as appropriate, following a well-defined blueprint for response and escalation. If the materiality of a given crisis warrants further escalation, there is further recourse to the Board of Directors.

Simplification of Technology Infrastructure

The technological strategy of Ziff Davis is to focus the majority of our development efforts on processes that create synergies and improve our products. As a result, the management of technology infrastructure, financial software, CRM software, HR platforms, and platforms for internal and external communication (as well as a host of other platforms powering business processes) is increasingly transitioned to third-party "Software-as-a-Service" (SaaS) providers. Our Legal and InfoSec teams perform rigorous analysis of every potential vendor. Included in that analysis is an examination of the representations of the vendor of their level of compliance with frameworks of control essential to our business (SOX, PCI, etc). Risks that are identified are logged and communicated with both the business unit and vendor, which provides greater visibility into the organization's risk profile. With each major software-fueled business process we offload to a SaaS provider, the complexity of the universe for internal IT and Legal is reduced, eliminating a substantial area of risk.