

A person wearing a yellow hoodie and large headphones is sitting at a desk, playing a game on a large monitor. The monitor displays a first-person shooter game with a large explosion on the left side. The person is smiling and looking at the screen. The desk has a keyboard and a blue can. In the background, another person is visible working at a desk.

zensar

**We play the game,
so you can win.**

Delivering digital
security superpowers
for gaming platforms.

An  **RPG** Company

The gaming space has grown exponentially in recent years—and so have the accompanying threats. With millions of gamers worldwide hooked on a wide range of interactive experiences, the gaming industry has been gaining immense popularity. This has made it a prime target for cybercriminals, seeking to exploit its vulnerabilities. What is especially worrying is the common target group of kids, aged between 3 and 16.

Just between July 2022 and 2023, over four million cyberattacks targeted the global gaming community. Amongst these, 30,684 were found to be unique files masked as popular games, mods, cheats, and other game-related software; they affected 192,456 users worldwide.



Four Reasons Attackers Target the Gaming Industry

The gaming industry is an attractive target for cybercriminals for four key reasons:



Financial Gain:

The huge revenues generated by the gaming industry attracts the attention of cybercriminals, especially those seeking to

- steal credit card information
- sell virtual goods and currencies on the black market, or
- use ransomware attacks to demand payment for restoring access to games or gaming networks.



Large User Base:

Popular gaming platforms, which typically have millions of users, provide attackers with a large pool of potential victims. The more users a platform has, the greater the potential impact of a successful attack.



Valuable Virtual Assets:

Many games feature virtual assets such as rare items, in-game currencies, or high levels of progression. These assets can be lucrative targets for theft and resale in underground markets.



Hacktivism:

Some attacks on the gaming industry may be ideologically or politically motivated. Hacktivist groups often target gaming companies to protest against their policies or simply to make a statement.

Common Security Challenges of Online Gaming Platforms

The first step toward defending your gaming platform is to understand the different avatars that the threats come in. These are some of the common challenges you're likely to face:

Account Hijacking: Attackers may hijack user accounts via phishing, malware, or credential stuffing—enabling them to steal virtual assets, disrupt gameplay, or engage in fraud.

Cheating and Exploits: Hackers are known to use cheats, like aim bots or wall hacks, which cause frustration for players. Such methods of exploiting game vulnerabilities could undermine the integrity of online gaming.

Distributed Denial of Service (DDoS) Attacks: DDoS attacks overwhelm gaming servers, causing downtime, latency, and degraded performance. These disruptions are either caused by attackers for extortion or by rivals to gain a competitive advantage.

Data Breaches: The user data collected by online gaming platforms makes the platforms vulnerable to data breaches. This can lead to identity theft, fraud, and reputational damage.

Phishing and Social Engineering: Attackers often impersonate game developers or support representatives to trick gamers into revealing their credentials or installing malware.

Insecure APIs and Integrations: Integrating with third-party services may pose security risks. Vulnerabilities in the integration can be exploited for unauthorized access or data breaches.

Fraudulent Transactions: Fraudsters may use stolen payment information to target gaming platforms. This necessitates robust fraud-prevention measures.

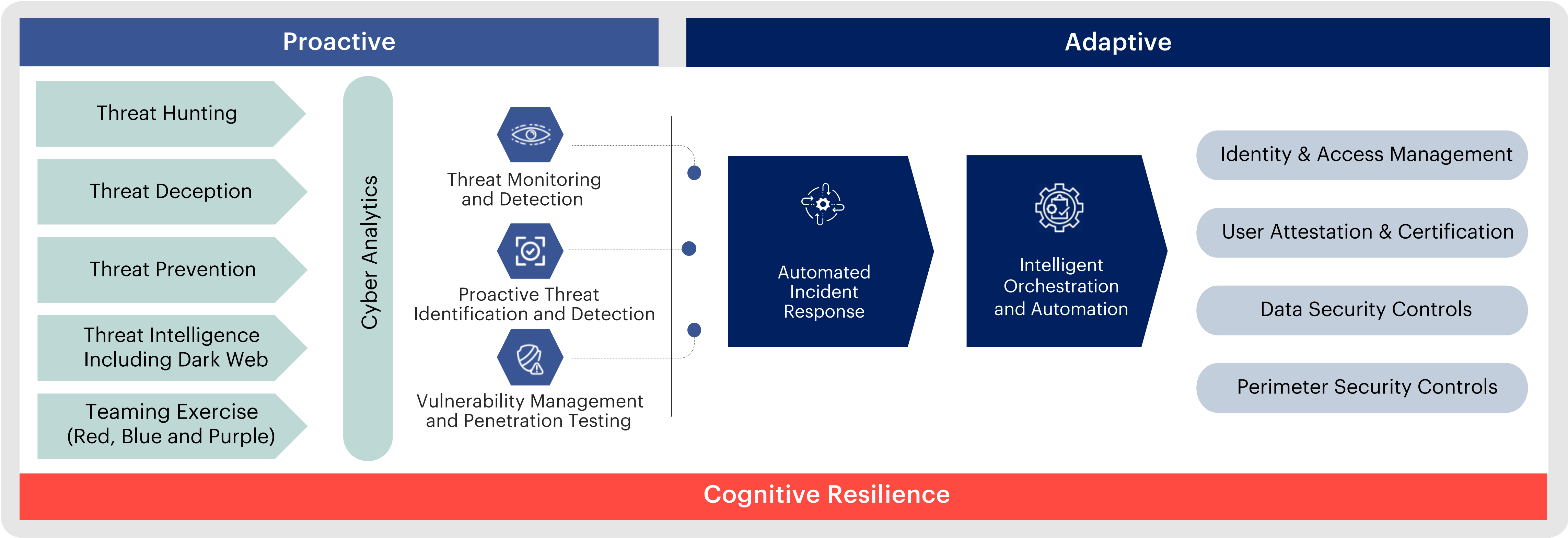
Privacy Concerns: As users tend to worry about personal data security, compliance with regulations and transparent privacy policies are critical to build trust and mitigate risks.



Zensar Can Help You Level Up Your Digital Security Resiliency

As the threat landscape is constantly changing, the gaming industry’s priorities and practices must evolve to keep up. The situation requires you to invest in robust cybersecurity solutions and perform regular vulnerability assessments of applications to fix bugs.






You can count on Zensar to help you stay a step ahead of malicious actors. We can deliver the whole package—infrastructure, applications, and data security best practices—vital for running your business with immunity against cyberattacks.



We Are The Synergy Between Technology and Expertise

At Zensar, we understand what it takes to secure your gaming platform. Combining future-ready technology with proven expertise, our curated web application security solution employs a multi-layer approach to identify and neutralize the various vulnerabilities and threats in your environment.

Technology alone is not enough to combat cyber threats. At Zensar, we use a unique innovation cycle that combines technology with expertise to continuously improve solutions at a speed and sophistication unmatched in the industry

 ZenSOC's	 Innovation	 Partners	 Accelerators & Frameworks	 Skills
Prescriptive MDR aka SOC to provide the Detection, Hunting and respond to incidents by providing round the clock services	Innovation hub consisting of ZenLab collaboration with various team. Blue Teaming, Red Teaming and Purple Teaming	360 degree partnership with leading players to detect and respond attacks	Modular and scalable platforms to meet your cybersecurity objectives	Collaboration with local University and Zensar's Centre of Excellence to provide intensive cybersecurity training to upskill and reskill
<ul style="list-style-type: none">• 6 ZenSOCs - U.S U.K India• Dashboard• 430 Use Cases• Follow the Sun• Threat Hunting & vertical specific Use Cases	<ul style="list-style-type: none">• R&D Labs• ZenLab• Threat Intelligence Platform• Weekly Cyber Security Advisory	<ul style="list-style-type: none">• Data Security• Threat Protection• Threat Detection & Hunting• Cloud & Infra Security• Identity & Access Management	<ul style="list-style-type: none">• ZenSOC• CloudSecure• CertSecure• ZenVAPT• KeyCert• ZenTrust IAM• Data Discovery• DLPGovernance	<ul style="list-style-type: none">• 650+ certified security resources• Zensar Cyber Center of Excellence• Zensar Security Architecture & Engineering

Here's an outline of our approach:

Risk Assessment: We start with a thorough risk assessment to

- identify potential vulnerabilities and threats, specific to your gaming platform
- evaluate the security posture of third-party integrations and APIs, used within your gaming platform, to factor in the security risks, and
- ensure compliance with relevant security standards and regulatory requirements, such as GDPR and PCI DSS.

Application Security: Our developers

- follow secure coding practices to minimize vulnerabilities, such as SQL injection and cross-site scripting, into our web applications
- configure security headers and the Content Security Policy (CSP) to mitigate various types of attacks, such as XSS and clickjacking
- conduct regular security testing, including penetration testing and vulnerability assessments, to identify and remediate security weaknesses, and
- ensure that the required security controls are implemented for the SaaS-based applications in use.

Identity and Access Management: With the goal of preventing unauthorized access to user accounts, we implement strong authentication mechanisms, including

- Multi-Factor Authentication (MFA)
- Role-Based Access Controls
- Single Sign On (SSO), and
- Privilege Identity Management (PIM).

Data Encryption: We protect sensitive data, both in transit and at rest, using

- strong encryption algorithms, and
- key management practices.

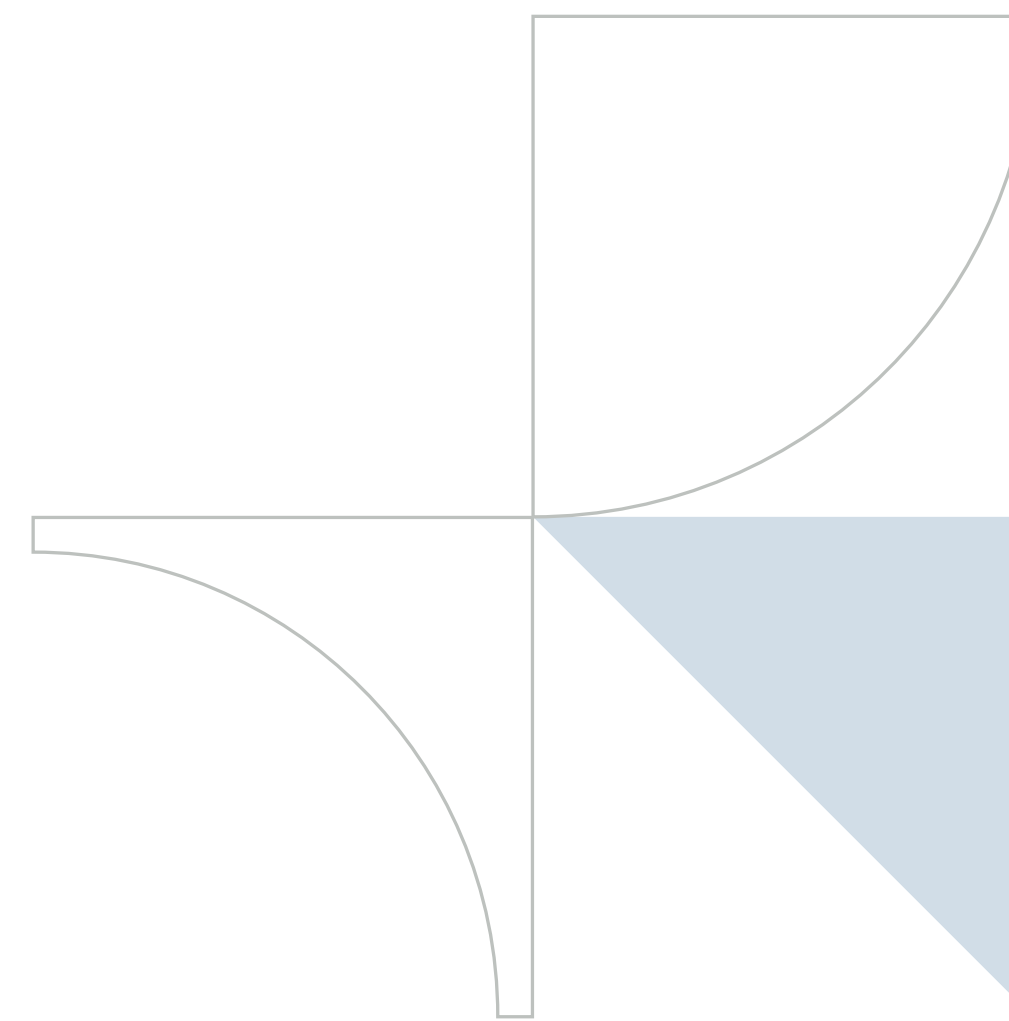
Security Incident and Event Management (SOC Operations):

Our team of experts can help you

- respond effectively to security incidents and breaches with an incident response plan, and
- leverage pre-defined use cases to implement automation, using the SOAR platform.

User Education and Awareness: Finally, we provide guidance on

- educating users about security best practices, and
- reporting security incidents or suspicious activities.



Complete Portfolio of Digital Security Solutions

As data protection is a critical component in any compliance, the cybersecurity of any infrastructure that stores user information must be a priority. Poor authorization controls and security protections could result in severe penalties. And to complicate matters, the Privacy Act states that organizations must implement “reasonable security” measures - which leaves security compliance open to interpretation.

Having successfully implemented data security solutions for organizations across the globe, we can help implement reasonable security measures to

- protect the data privacy rights of your users
- meet requirements related to regulatory compliance and local regulations
- put in place best practices for data collection and usage, and
- respond to consumer requests regarding their data with transparency.



20+

Service Offerings



650+

Security SME



45+

MSS Customers



600+

Cyber Security Certifications



70+

Partners Onboarded

Secured Sensitive Data

An end-to-end data Protection through matured frameworks

- Data Security

 - Data Discovery, Classification & Governance
 - Encryption, Tokenization & Masking
 - Key and Certificate Life Cycle Mgmt.
 - CASB & Data Leak Prevention

Managed Security Threats

Through next-gen attack prevention & breach simulation

- Threat Protection

 - Application Security – SAST, DAST, IAST & SCA
 - Low/No Code, DevSecOps, API Security
 - Vuln Assessment & Penetration Testing – On-Prem & Cloud
 - Mobile Security (Apps & Platform)
 - Red, Blue & Purple Teaming

Improved Security Posture

Through defense-in-depth approach

- Threat Prevention

 - Perimeter-less Network Security
 - Omni-channel Endpoint Security
 - Cloud Security Assessment & Compliance
 - Cloud Workload Security
 - SASE based security controls

360° Security Monitoring

End to end threat visibility to reduce mean time to remediate

Threat Detection & Hunting

- Advanced Security Analytics (AI & ML)
- Proactive Threat Hunting
- Unified Security Automation, and Response (SOAR)
- Incident Response
- Threat Intelligence
- Threat Deception
- Prescriptive SOC

Zero Trust Security

“Don’t Trust – Always Validate” at the core for secure & automated IAM

Identity & Access Management

- Identity Governance & Administration
- Identity Lifecycle management
- SSO, MFA, Password less security
- Customer Identity Access Management
- Privileged Access Mgmt.

Services:

Advisory & Consulting | Implementation & Engineering | Managed Security Operations



CHALLENGER

Product Challenger for
Strategic Security Services



CONTENDER

Major Contender IT
Managed Security Services



CONTENDER

Major Contender Managed
Detection and Response
(MDR) Services



CHALLENGER

Security Challenger
In RadarView



MAJOR PLAYER

Cognitive IT Infrastructure
Management

An Ecosystem of Thriving Partnerships

At Zensar, we build comprehensive solutions, enabled by symbiotic partnerships that deliver more than the sum of our individual capabilities.

Data Security Classification, DLP, Encryption, CASB	THALES	Microsoft Azure	netskope	zscaler CATO NETWORKS	FORCEPOINT	MICRO FOCUS
Threat Protection Vulnerability Assessment, Pen Test, Red/ Blue Teaming	QUALYS	Nessus vulnerability scanner	NOZOMI NETWORKS	sonarqube HCL AppScan	KALI LINUX	TruOps Cyber Risk Management
Threat Detection & Hunting MDR, SIEM, Threat Hunting, Deception, TI feeds, Brand protection	Microsoft Sentinel	cisco splunk>	Radar	SMOKESCREEN	FireEye	DARKTRACE
Threat Prevention Cloud & Infra Level Security	Microsoft Azure aws	FORTINET paloalto NETWORKS	Carbon Black. CROWDSTRIKE	resilient an IBM Company	radware	IMPERVA
Identity & Access Management IAM, IGA, PIM, PAM, Zero Trust	SAVIYNT okta	Microsoft Entra ID	SailPoint The core of identity Security	BeyondTrust	CYBERARK	MICRO FOCUS

*Note: The list is not comprehensive

Diverse. Vendor Agnostic.
Vendor Centric.



Secure the gaming experiences that you deliver, with Zensar Technologies. We'd love to chat with you about how we can help fortify your online gaming platform with our web application security services.

Get in touch with us today.

zensar

An  **RPG** Company

We conceptualize, build, and manage digital products through experience design, data engineering, and advanced analytics for over 145 leading companies. Our solutions leverage industry-leading platforms to help our clients be competitive, agile, and disruptive while moving with velocity through change and opportunity.

With headquarters in Pune, India, our 10,500+ associates work across 30+ locations, including Milpitas, Seattle, Princeton, Cape Town, London, Singapore, and Mexico City.

For more information please contact: velocity@zensar.com | www.zensar.com

