SUCCESS STORY

Japanese gaming giant launches revolutionary online game where Elastic protects collectible digital artwork and NFTs

Japanese gaming giant launches a new online game and deploys Elastic to protect collectible digital artwork, NFTs, and players against theft, forgeries, and other illegal activities.

Region
Japan

Industry
Media & Entertainment

Solution
Elastic Observability

Reduces instances of NFT fraud

With Elastic, this Japanese gaming giant can closely monitor NFT trading and protect the business and its users from fraud and other illegal activities.

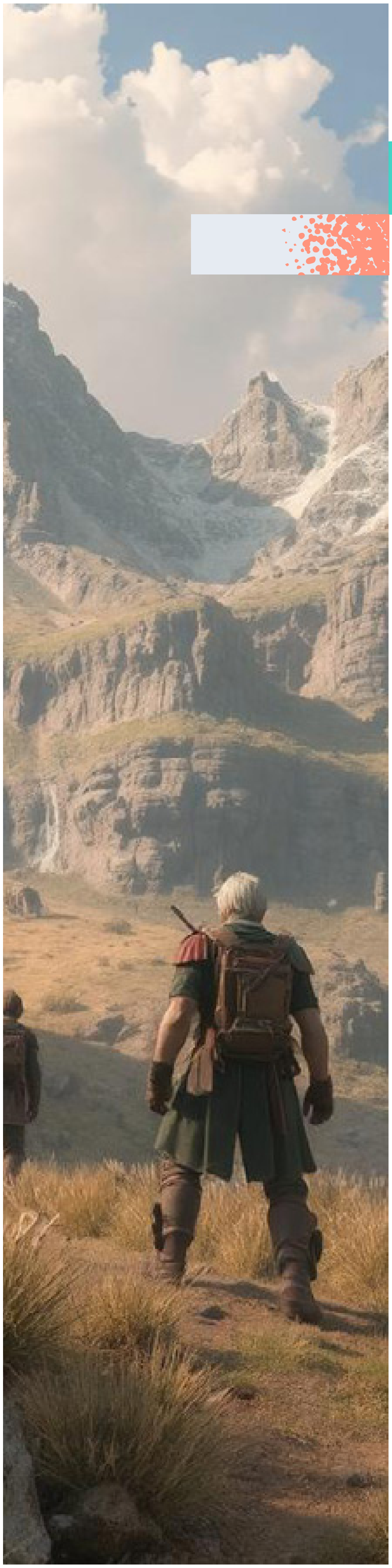
Opens the door to new Web 3.0 opportunities

With Elastic now deployed to protect the online gaming environment, this Japanese world leader in electronic gaming can expand its Web 3.0 business.

Future-proofs the business against emerging threats

This Japanese gaming giant can harness the fast-evolving capabilities of Elastic, including generative AI features that streamline security workflows.

World-leading Japanese gaming giant launches revolutionary online game with collectible digital artwork and NFTs protected by Elastic running on Google Cloud



This highly respected Japanese gaming giant has been at the forefront of digital gaming for over 30 years through its legendary role-playing games, and partnerships with other leading gaming publishers, selling millions of copies of their games worldwide.

In keeping with its innovative reputation, the company recently announced a new online game that uses Web 3.0 technologies including crypto-currency wallets, non-fungible tokens (NFTs), and blockchain technology to create a unique player experience.

Their latest game is a completely new form of NFT-based entertainment, where 10,000 collectible artworks meet real game utility. Each NFT is a character with its own unique design, background, and role within the story. To piece together the mysteries of the world, users compete to find the items hidden throughout the gaming world, using secret information held by each character. The game's genre can be defined as narrative-unlocked NFT entertainment.

The company's new game is experimental, exploring new approaches to social games and community building with blockchain gaming features while putting in place the infrastructure necessary for a secure gaming environment.

This presents a new set of challenges for the company's Security Operation Center. "The business is constantly pushing the boundaries of game design. Our job is to be just as innovative when protecting the business and its customers" says the SOC manager, at this gaming company.

In the case of this new game, protecting player NFTs is a primary concern.

So-called ‘rogue NFT’ counterfeits of legitimate NFTs pose a threat to the integrity of the gaming environment by infringing on the copyright of the original creator and attempting to mislead buyers into thinking they are buying a legitimate NFT. Above all they pose a reputational threat that could undermine trust between the game publisher and players worldwide.

The SOC manager also wanted to monitor legitimate tokens across their entire lifecycle, from the moment they are minted to when they change hands on an NFT marketplace. “What might start as a legitimate purchase might end up being used for illegal purposes including fraud, money laundering, and tax evasion,” he says. To support a ‘know-your-transaction’ process, the company set out to detect suspicious transactions in real-time.

Building a new line of defense for Web 3.0 gaming

This Japanese gaming company has used Elastic for several years to protect its business from many threats, including video-game pirates and hackers seeking illegal access to pre-release game code. The software runs on virtual machines in its Google Cloud environment and ingests more than 10,000 events per second.

Many members of the security team have worked with Elastic in previous roles. They include the Senior Security Engineer who configured the deployment. “NFTs present a new set of challenges, but we’ve already put in place a new line of defense against many of the threats in this space,” he says.

The Senior Security Engineer and his team recently integrated data from OpenSea, the world's largest NFT marketplace where buyers and sellers interact every day across blockchains including Ethereum, Polygon, and Arbitrum.

With OpenSea data in Elastic, the company can monitor and detect unauthorized activities including the presence of rogue NFTs. "Elastic enables us to identify actors who are abusing our trademarks," says the SOC Manager. "We can write detection rules to filter the data and trigger defensive actions."

Elastic also enables the security team to analyze NFT buyer and seller activity. With Elastic's powerful Graph function, it can explore complex data relationships and use the Kibana Graph user interface to visualize insights that would be otherwise difficult to detect.

The company also uses Elastic to protect sellers from being scammed. The security team enriches data with threat intelligence from blockchain risk-scoring tools to spot problematic trades. For example, if an unusually large number of items are being sold on a particular exchange, the company can more easily assess whether the activity is suspicious or not.

> Elastic gives us the openness and flexibility to ingest events from new sources, set alerts for suspicious activity, and visualize the threat with Kibana dashboards.
>
> Senior Security Engineer, Leading Japanese Gaming Company

Growing the NFT business

The company will shortly release a set of collectible action figures with NFTs for proof of ownership and authenticity. It is also partnering with other leading players in the Web 3.0 space to widen the availability of next-generation games that don't require expensive gaming consoles. "Elastic opens the door to enabling a range of business opportunities in a more secure manner by protecting NFTs and the wider Web 3.0 environment," says the SOC Manager.

The security team already uses Elastic's machine learning to identify anomalies and threats, and they can see its potential to provide additional layers of defense to the gaming environment. The business also plans to increase its use of Elastic machine learning and artificial intelligence features.

He is also keeping a close eye on the latest generative AI features in Elastic, including the Elasticsearch Relevance Engine (ESRE) and the Elastic AI Assistant. Use cases include automatically generating a recommended course of action when an alert is triggered, reducing the time spent by security engineers searching document databases. "We are very interested in these features and how they can be applied to gaming security," concludes the SOC manager.

> As well as protecting the business, data gathered in Elastic enables us to understand wider trends. We can use this information to uncover additional business benefits and drive further growth in the gaming industry.

Senior Security Engineer, Leading Japanese Gaming Company