NOT JUST A GAME

Colin Fernandes *reveals the importance of protecting sensitive data and what gaming companies can do to play their part*

When you mention the words, "data security," what mental picture do you get? Most people think about media representations of hackers in black hoodies, surrounded by Matrix-style green numbers. Others immediately think of banks or other financial services institutions that one would assume need the most protection. Whichever group you fall into, it's likely you didn't immediately jump to gaming.

And yet, security for gaming companies is just as important – if not more so – than financial institutions. The global games market was valued at $137.9 billion in 2018 by research firm Newzoo, and there is an estimated customer base of between 2.2 and 2.6 billion people worldwide that are gamers. From the casual gamer who plays a bit of Candy Crush Saga on their smartphone to pass the time through to the enthusiast waiting for the midnight launch of the latest AAA game like *Call Of Duty* or *FIFA*, each of these players will generate huge volumes of data.

This customer data includes payment information and a variety of personal information depending on the circumstance. For games where players may be children, the situation is even more serious. When it comes to regulations around protecting data the most recent piece of legislation was, of course, GDPR – the EU's General Data Protection Regulation. Under GDPR, the expansive definition of "personal data" includes everything from names and email addresses to biometrics and IP addresses.

> IT TEAMS HAVE TO BE AT THE CUTTING EDGE DEPLOYING APPS AND SERVICES TO CUSTOMERS

Gaming companies gather a massive data lake of personally identifiable information (PII) and sensitive children's data, including dates of birth, email addresses and data from smartphones using gaming apps with location services. The scope of information that's collected and the fact that much of it belongs to children and young adults makes this data particularly sensitive.

Games like the Pokémon Company's *Pokémon Go* serve hundreds of millions of users within its multi-tenant Amazon Web Services (AWS) environment. The majority of these players will be children and young adults, so this is a good example of how gaming companies have to ensure that their security deployments live up to the restrictions and requirements mandated by GDPR.

SENSE OF RESPONSIBILITY

John Visneski, director of information security and data protection officer at The Pokémon Company International explained it as follows: "We have additional responsibilities around sensitive data under GDPR, so we have to regularly maintain the necessary compliance standards. Our approach to security is that this has to be a business enabler and our main goal is to provide a safe place for our customers to enjoy our brand. When a parent goes to buy or download a Pokémon product, they can sleep well knowing their child's data is protected. Our approach to user privacy and data security is therefore an essential part of our overall brand."

Gaming companies face the same challenges as every other business or organisation around keeping their IT networks and data secure. Consumers want confirmation that their data is safe without it hampering a seamless experience, and herein lies the challenge – how can gaming companies maintain data privacy without disrupting operations?

They have to keep this security in place without affecting the customer experience and they have to achieve this with small IT teams. Cloud services like AWS are often used to provide the back-end infrastructure to cope with scalability, but this does not provide all the necessary insight.

For companies involved in gaming, a hit game can mean huge additional customer numbers and scaling up quickly. However, achieving scale and visibility at the same time is a bigger challenge. Teams need to get ahead of this growth and take measures to log and track access of all data flowing across their environments in one place.

IT security across all businesses involves looking at a range of technologies, from network security and firewalls, through to data protection and vulnerability management. For gaming companies that provide apps or run websites, the web application security side is also important to consider.

Effective network security involves protecting the integrity and usability of your network and the data running on it. Combining layers of defences at the edge and in the network, policies and controls are implemented across each layer, ensuring that authorised users can gain access to network resources, but prevents malicious actors from carrying out threats. Network security is a more involved area today as many companies now run a mix of internal on-premise IT infrastructure alongside modern applications hosted in the cloud.

The global games market is valued at $137.9 billion with between 2.2 and 2.6 billion gamers worldwide

PROTECTIVE BARRIERS

Firewalls are key in any network security strategy. They act as a barrier between your trusted internal network and untrusted outside networks. They monitor incoming and outgoing network traffic and can decide whether to allow or block this traffic based on a defined set of security rules. At the same time, firewalls can provide logs of activity for further correlation and analysis.

Application security involves looking at the elements that make up each application and how they behave over time. By looking at data created by each application element over time, you can see normal behaviour and spot outlying activity that should be investigated. Alongside this, application security involves looking for errors in logic and processing that can lead to wrong data being created, additional privileges being granted or code being run when it should not be.

Each of these areas of security creates data for analysis, and good performance relies on good data in turn. By looking at logs and metrics across all of your IT, you should be able to analyse your IT systems for bad behaviour and stop those bad actors before they have an impact.

As well as these more traditional aspects of cyber security, there are also challenges specific to the gaming industry to bear in mind. These involve threats to the service that gaming companies provide, and can vary from irritations that break games for other players through to more serious attacks that can lead to theft of accounts or financial details.

For Visneski at The Pokémon Company, threats can range from the niggly and ridiculous through to dangerous threats: “We also face more specific issues as a gaming company. These range from irritations like cheating within the game to more negative actions like creating false accounts, trying to level up *Pokémon Go* accounts to sell them, as well as the use of bots that can automate common gameplay steps to create an unfair advantage. We have to treat these as security risks as well, and both identify and remediate this malicious activity before it affects other customers.”

Each of these issues – from minor problems through to game-breaking security flaws – has to be analysed and treated in order to prevent them from affecting the customer experience. To ensure effective handling of these security issues, gaming companies need to conduct real-time data analysis and interrogate multiple data streams.

A HIT GAME CAN MEAN HUGE ADDITIONAL CUSTOMER NUMBERS AND SCALING UP QUICKLY

The solution to what could seem like quite a vast problem is machine data analytics. Machine data analytics involves collating and analysing information from multiple data sources, including metrics and log data from multiple applications. By bringing this data together into one place, you can get a better picture of how applications are performing as well as the potential security risks.

This can be especially useful for companies that have smaller IT teams and that are more data-driven in their businesses. Generally speaking, gaming companies tend to fall into this category, as they have both fewer internal staff and have to look at their monetisation strategies carefully, given the costs of developing and running their IT infrastructure over time. Getting better data on security and operations can help answer questions on how customers are responding over time as well as security.

VITAL INSIGHTS

Similarly, the majority of businesses are finding it more and more difficult to hire and retain staff with security skills. When you can’t just keep hiring more people to deal with issues, there is certainly a role for automation and analytics. By making it easier to automate security analysis and machine data analytics together, gaming IT teams can get more insight into what is really taking place.

Of course, machine data analytics can be of use to far more than security teams. The same data can also provide insight to other teams including finance and operations and even marketing. By looking at data on application performance and customer experience responses, gaming companies can work out how to improve experiences across the board. This not only helps maintain security; it provides a direct link between security analysis and opportunities for return on investment.

For many business leaders and IT teams, gaming is seen a niche that is not relevant to their markets. However, gaming IT teams have to be at the cutting edge when it comes to deploying applications and services to their customers. They have to deal with huge variations in customer activity over time. They need insight into specific customer activities just as much as the overall network and cloud performance side. Most importantly, they have customers that fall into the category of requiring more careful handling around their data.

Games platforms like *Pokémon Go* have to handle huge amounts of data – across application instances, cloud platforms, networks and customer behaviour data – and link these all together for analysis. The process must be seamless and it must provide insight. For their customers, security is not a game. Why would you take a different approach? ●

Colin Fernandes is director of product marketing EMEA at Sumo Logic. He leads the company’s education and marketing campaigns in Europe, helping companies understand the challenges and opportunities around modern application design and implementation at scale. Prior to Sumo Logic, he worked at VMware where he was responsible for the company’s operations around the telecoms and cloud management sectors.

It’s the responsibility of the developers of games like *Pokémon Go* to ensure that data gathered about the player is not abused

Picture credit: The Pokémon Company