# CYBERSECURITY Q&A: WHAT YOU NEED TO KNOW

» The online gaming and betting sector is on a roll. Across Europe, online gambling revenue was expected to exceed €36 billion (£30bn) last year, a year-on-year increase of 19%. In the UK, online is the largest sector, recording gross gambling yield (GGY) of £4 billion in the period April 2020 to March 2021. Meanwhile, the UK's digital gaming market is set to record revenues in excess of $6 billion (£4.6bn) in 2022, driven by mobile. That will cement the country position as the sixth largest gaming market worldwide and Europe's biggest.

Yet as more resources are spent on cloud and digital investments to expand this footprint, companies in the sector also open them up to new cyber risks. Where there is money and users, financially motivated cyber-criminals are usually not far behind.

Here are answers to some of the most pressing questions gaming and betting firms are asking right now:

## What are the main cyber-threats to my business?

Whether they're targeting user data, aiming to disrupt services or hold companies to ransom, cyber-attackers have a wide variety of tools and techniques at the disposal. Some of the main threats include:

**Distributed Denial of Service (DDoS) attacks** used to overwhelm sites with traffic. They can be used either to force users to competitor sites, or to extort money from the victim organisation. One vendor claimed 77% of global DDoS attacks in Q3 2020 were aimed at the online gaming sector.

**Ransomware** is another critical threat to gaming and betting companies. It can result in theft of sensitive data and major service outages.


**Account takeovers:** These are typically focused on hijacking user accounts to steal sensitive information and/or drain them of funds.

**Bot-based attacks:** Automated bots are increasingly used in a variety of ways, such as "scraping" corporate and user data, and "expediting" attacks which give threat actors an unfair advantage in gaming or betting.


**Vulnerability exploitation:** This is used as an initial access vector in some ransomware attacks, as well as campaigns designed solely to steal sensitive IP and user information. Endpoints (eg, servers and desktops/laptops) running unpatched and vulnerable applications are typically targeted. The Trend Micro™ Zero Day Initiative™ (ZDI) released advisories on 1,604 vulnerabilities in 2021, 10% higher than during the previous year.

## How do I go about vulnerability management?

More CVEs were published in 2021 than any year previously, making patching a major headache for many organisations, especially as they roll out new cloud systems. Organisations need a risk-based patching programme which assesses the likelihood of particular vulnerabilities being exploited in their organisation. And then automated systems to apply vendor patches. Virtual patching is a useful complementary technique which will protect all vulnerable systems from known and unknown threats until official patches can be applied.

## Should my security programme prioritise prevention?

Preventing threats—via good cyber-hygiene like prompt patching, multi-factor authentication and encryption—is certainly important. But no organisation can be 100% breach-proof. That's why you also need effective threat detection and response capabilities. Extended detection and response (XDR) that works across email, server, cloud, network and endpoint layers offers the ability to act rapidly to contain breaches. It's especially critical if your business is targeted by an APT group, such as the DRBControl espionage campaign of 2019. These actors go to tremendous lengths to stay hidden, using publicly available and custom tools to breach networks, elevate privileges, perform lateral movement and exfiltrate data.

## Should I be concerned about my remote workers?

Yes. The new era of hybrid working means many employees will continue to work from home post-pandemic, potentially on unsecured laptops. Trend Micro research shows they may also be more willing to take risks than their office-bound colleagues. Any security policy must be updated accordingly, to include regular security awareness training sessions, limit risky behaviour and ensure endpoints are patched and secured. Offer employees work devices if possible, tighten access controls and consider remote device management software.

## Is best-of-breed security the preferred security model?

While it has its attractions, too often best-of-breed can lead to multiple point products—which means more security overheads for your IT team, and more coverage gaps for threat actors to hide in. A platform approach from a reputable vendor can deliver more comprehensive protection, while reducing management overheads and combining prevention with detection and response. This will allow you to apply the right security at the right time to mitigate risk.