

Customer Case Study: AppsFlyer

Hunters XDR helps AppsFlyer Connect the Dots across Attack Surfaces

BACKGROUND

AppsFlyer is a mobile attribution and marketing analytics company for marketers, ad agencies and app creators. Founded a decade ago, AppsFlyer today has over 12,000 customers worldwide, working with many of the leading brands around the world across all market segments. Born in the cloud, it uses infrastructure from AWS, and its security team primarily uses cloud-based apps and services. For security management they use a SIEM based on Elastic, and in terms of security products they primarily use EDR and monitoring tools. All of them are connected to Hunters XDR, which seamlessly ingests all of their data.

AppsFlyer's security team comprises four different groups: the GRC, security engineering, a dedicated team to develop internal security tools, and the security operations team which is in charge of all the monitoring and incident response.

AppsFlyer's main goal was to scale up their SOC: putting the security tools they already had in place for a better use, maximizing the capabilities of the team and switching from a reactive defense mode to a proactive security approach.

Even though the team had a strong set of security tools in place, they were poorly connected and generated many alerts that were missing context, making incident response and mitigation cumbersome and inefficient.

KEY CHALLENGES

- Inability to unify alerts and events generated by point security solutions
- Lack of context to alerts, requiring manual, lengthy investigations
- Reactive and alert-driven SOC management
- Lack of visibility over complex attacks where attackers' try to hide in plain sight
- Decreased productivity due to manual processes and inability to prioritize alerts



"The main value that Hunters XDR provides me as a CISO is that it connects the dots across solutions. My teams now have better visibility of the issues that we have in our environment, and we can connect alerts to a bigger story. My team can now handle issues in a more efficient and accurate way than before."

Guy Flechter, CISO at AppsFlyer



QUICK FACTS

AppsFlyer was founded over ten years ago with a mission to help marketers succeed. By empowering brands with a holistic view of every user journey across platforms, channels, and devices, AppsFlyer aims to be every marketer's best friend. Today, they are the global attribution leader.

Customers: Over 12,000

Partner integrations:
Ecosystem of over 6,000

Employees: 900

Global offices: 18

Funding: \$300M dollars

HOW HUNTERS HELPED

Hunters XDR seamlessly connected to AppsFlyer's data sources, and within minutes they could already enhance the visibility they had over the entire security environment. By connecting to all their existing security telemetry, and using context and threat intelligence to correlate sparse sources, alerts were now placed in context and connected to one another, leading to concrete Attack Stories that their SOC could act upon with high confidence. Alert handling and remediation of threats was more efficient, and they could devote more resources into proactive security activities.

KEY OUTCOMES AFTER DEPLOYING HUNTERS XDR

Faster Mitigation



Ability to mitigate incidents faster and more efficiently

Fast Time to Value



It took a matter of minutes to deploy and starting to see insights

Increased Business Agility



Increased business agility with faster and more effective detection of threats across existing systems

Actionable Insights



Connecting events and alerts from sparse sources into actionable Attack Stories

Extended IR Capabilities



Extending the incident response capabilities of their SOC with Hunters' expert services

Better Visibility



Achieving better visibility into the security environment, eliminating blind spots