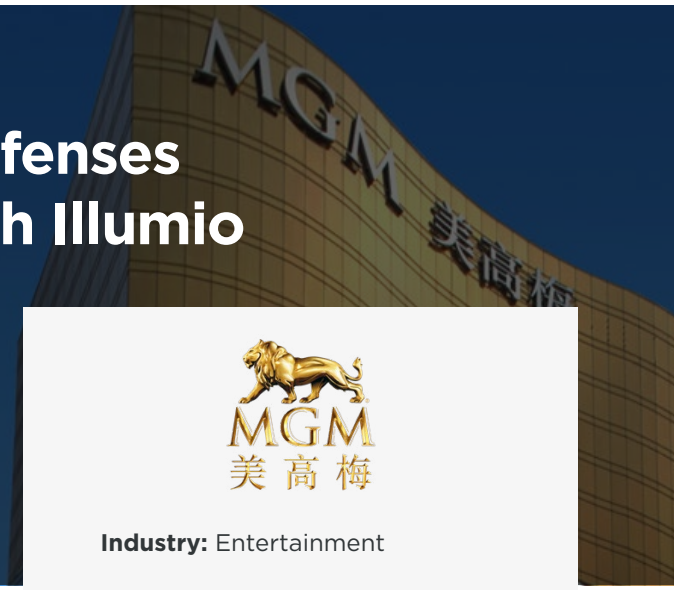
illumio

CASE STUDY



MGM China Strengthens Its Defenses Against Lateral Movement With Illumio

World famous integrated resort operator gains unprecedented visibility into application traffic and workload-level segmentation control without heavy agents or network upgrades

MGM 美高梅

Industry: Entertainment

Location: Macau, China

Environment: On-premises data center "server farm"

Challenge: Improve security against cyberattacks by deploying micro-segmentation to isolate and protect key digital resources

Solution: Illumio Core

Benefits: Prevention of lateral movement; full visibility into application traffic flows

Business Goals

MGM China is an integrated resort operator with casinos that are meccas for gamblers from around the world hoping to strike it rich. Such prominence also makes MGM China a high-profile target for hackers looking to hit the jackpot.

Like most any organization these days, MGM China needs to continually improve its defenses against ransomware and other cyberattacks.

With this in mind, digital security is paramount for MGM China. In particular, the company must protect its gaming applications and other systems that run in its on-premises data center.

Critically, the MGM China security team always needs to be one step ahead of rapidly evolving security threats. As part of this effort, MGM China wanted to limit lateral movement within its environment and enhance its protection against unknown threats.

Technology Challenges

To ensure hackers can't move freely in its data center to access valuable digital resources, MGM China focused on segmenting the traffic flows on its network down to the workload level, explains Edwin Leong, a data security architect with MGM China.

The digital security team of MGM China had been using logical and physical methods for segmentation with broad virtual zones and individual hardware firewalls, but that was proving increasingly problematic. It made managing policy and monitoring traffic unsustainable as more and more services came online.

"The traditional approaches to segmentation just were not scalable," Leong says.

"With Illumio, it all starts with its real-time map that gives us complete visibility into any application environment. It doesn't matter how complex it is, Illumio's map brings to light what's communicating with what and clearly shows which communications shouldn't be happening."

Edwin Leong,
Data Security Architect,
MGM China

MGM China was looking for an approach that didn't use inline and "heavy" agents that taxed server operating systems. His team was also seeking a simple architecture that didn't require changes to existing infrastructure, such as upgrading hypervisors.

How Illumio Helped

Leong learned about Illumio from a report by leading research company Gartner.

The team evaluated several vendors from the report and found Illumio provided superior visibility and a much simpler architecture that makes micro-segmentation exceptionally easier than other approaches, as well as lightweight agents that don't tax server computing power and hurt application performance.

Once the security team deployed Illumio Core, they were able to use Illumio's application dependency map to gain a full, detailed view of traffic flows across all systems in the data center to understand key security risks.

"The Illumio Policy Compute Engine also made enforcement simple and scalable by automatically generating the appropriate rules for each workload, even as new workloads are added or removed," Leong says.

Results & Benefits

Leong says Illumio has greatly reduced the time and effort his team spends on segmentation efforts, making it easy for them to quickly test and deploy enforcement policies.

"Illumio gives us much needed confidence that enforcement will not break our applications," he says.

Leong adds that this capability — along with the visibility provided by Illumio — has also been welcomed by the IT operations team, which can easily see the status of application communications across the data center.

With Illumio, MGM China was able to reach its goal of building stronger protection against lateral movement to keep cybercriminals from traveling freely through its data center and network.

"Illumio made it remarkably easy for us to design, build and operationalize a Zero Trust architecture with massive scale," Leong says.

> "Illumio Core solved our challenges of managing fine-grained segmentation policies at scale. We now have the proper protections in place to stop lateral movement and keep hackers from accessing our critical applications and data."
>
> **Edwin Leong,**
> **Data Security Architect,**
> **MGM China**

About Illumio

Illumio, the pioneer and market leader of Zero Trust segmentation, prevents breaches from becoming cyber disasters. Illumio protects critical applications and valuable digital assets with proven segmentation technology purpose-built for the Zero Trust security model. Illumio ransomware mitigation and segmentation solutions see risk, isolate attacks, and secure data across cloud-native apps, hybrid and multi-clouds, data centers, and endpoints, enabling the world's leading organizations to strengthen their cyber resiliency and reduce risk.