![Caesars Entertainment logo]

CASE STUDY

Caesars Entertainment Onboards Data Swiftly and Securely for M&As

Palo Alto Networks partners with Caesars Entertainment, the world's leading gaming and hospitality company, to protect their growing operations with Prisma Access.

![Palo Alto Networks logo]

Customer

Caesars Entertainment

Industry

Gaming and hospitality

Country

United States of America

Challenge

Caesars Entertainment, rapidly growing through mergers and acquisitions, needed to protect operations from unknown security risks in acquired entities.

Requirements

Must enable fast, secure onboarding of data from M&A properties

Solution

Prisma® Access cloud-delivered network security provides comprehensive, scalable protection with a consistent work-from-anywhere user experience.

Securing a Growing Entertainment Empire—Even Amid COVID-19

With a tiny bingo parlor in Reno, Nevada, what would eventually be called Caesars Entertainment put down roots in 1937. From their earliest days and through the decades, all four of the company's founders were known for bringing major innovations to the casino industry, and for defining what great looks like in gaming and entertainment. This included building Caesars into a world-renowned brand.

Fast-forward to July 2020, when Caesars Entertainment was acquired by Eldorado Resorts. The two legendary brands merged under the name Caesars Entertainment—becoming the largest gaming organization in the world, with 55 properties spread around the globe.

The fact that the Eldorado–Caesars merger happened in the midst of the COVID-19 pandemic should have made things more difficult for Bobby Wilkins, vice president of cybersecurity at Caesars Entertainment, but Wilkins wasn't flustered. He simultaneously moved tens of thousands of employees to home offices with secure remote connections to Caesars' network while designing and preparing to securely integrate terabytes of enterprise data at the merger go-live, and maintained management of those users since, including the critical merger dates.

Wilkins ran a tight security ship, maintaining a relatively small staff when compared to their major competitors. When the merger happened, putting the right people in the right places at the right time took some finessing. Having the right tools was crucial to help him and his team stay where they needed to be—ahead of attacks and able to scale to meet new demand.

Caesars Entertainment is the largest gaming organization in the world, with 55 properties spread around the globe

Challenge

FAST AND FREQUENT ACQUISITIONS CALL FOR A SECURE DATA ONBOARDING PROCESS

Having been involved in perhaps 20 acquisitions in his 29 years at Caesars, Wilkins says the biggest security risk when merging with a new organization is simply that so much is unknown. "You don't know how they've protected their network. You don't know what vulnerabilities you might inherit. You don't know what might be hiding there," he explains. "You need to protect yourself before you open yourself up."

The second-most urgent challenge is to understand the needs of the new entity's users, and provide the access they require—just enough, and no more—to the enterprise network and various systems and data so they can do their work once the merger is complete.

That can be difficult, according to Wilkins. Many business users simply don't know what data they need—and from what systems—to get their jobs done.

"You always end up with surprises during onboarding," says Wilkins. "On go-live days everyone wants everything to work, right away. But there's always something that's not perfect." Because of this, Wilkins always forms a rapid response SWAT team for go-live days to be on call to patch any missing connections as soon as they are identified.

To add to the pressures of a timely integration, all of this was taking place during the pandemic. "Making sure, in the era of COVID-19, with all the shutdowns and remote working, that we had the resources available to both operate what was already running and also send crews to ensure that merger connections were going smoothly—that was [another] major challenge," says Wilkins.

Requirements

A SCALABLE, SIMPLE WORK-FROM-ANYWHERE SOLUTION

Knowing they would continue to grow made platform-style simplicity paramount to Caesars' security strategy, and for protecting their M&A investments. Workers needed to be protected everywhere as their ranks grew.

Platform approach to security: This was Wilkins's top priority. Prior to moving to their current Palo Alto Networks security implementation, Caesars had 17 different cybersecurity systems installed. Simply learning each of these ate up valuable employee time. Wilkins said he "did the math" and found that if he sent each person in the department to one class per year in each of those 17 products, he would lose approximately 40 percent of employee productivity for the year. Wilkins was therefore determined to find a security platform with a consistent user interface across all components.

Secure and consistent user experience for remote workers: There was also the issue of employees being sent to work from home due to COVID-19, many of them connecting to the network from remote geographies. The extended network had to be protected without interfering with productivity. Wilkins wanted employees to have the same experience as if they were connected directly to the network at a company location, no matter where they were working.

Scalable protection: Because some mergers can be quite large—the acquisition by Eldorado is a case in point—Caesars needed a security solution that could scale as necessary to meet the traffic demands of each subsequent M&A onboarding exercise.

> **"** You always end up with surprises during acquisitions. On go-live days everyone wants everything to work perfectly, right away. But there's always something that's not perfect.

— Bobby Wilkins, *Vice President of Cybersecurity, Caesars Entertainment*

Solution

PRISMA ACCESS DELIVERS PROVEN SOLUTION FOR CAESARS

Because of the potential risks, Caesars has put tremendous effort into their M&A security vetting process. "We make sure not to compromise ourselves by being overly eager to connect," says Wilkins.

The due diligence Caesars performs during an acquisition or merger is multidimensional. First and foremost, Caesars never fully opens their network to a new company. Instead, it deploys Prisma Access, a cloud-delivered security platform that is part of the Palo Alto Networks SASE solution. Prisma Access allows Caesars to put up a shield between the organizations, ensuring security policies reflect exactly which systems and data the merging entity's users need to access. Prisma Access consolidates multiple products, including Firewall as a Service (FWaaS), Cloud Secure Web Gateway (SWG), Zero Trust Network Access (ZTNA) and Cloud Access Security Broker (CASB) capabilities, all in a single platform. "It delivers what we need," says Wilkins.
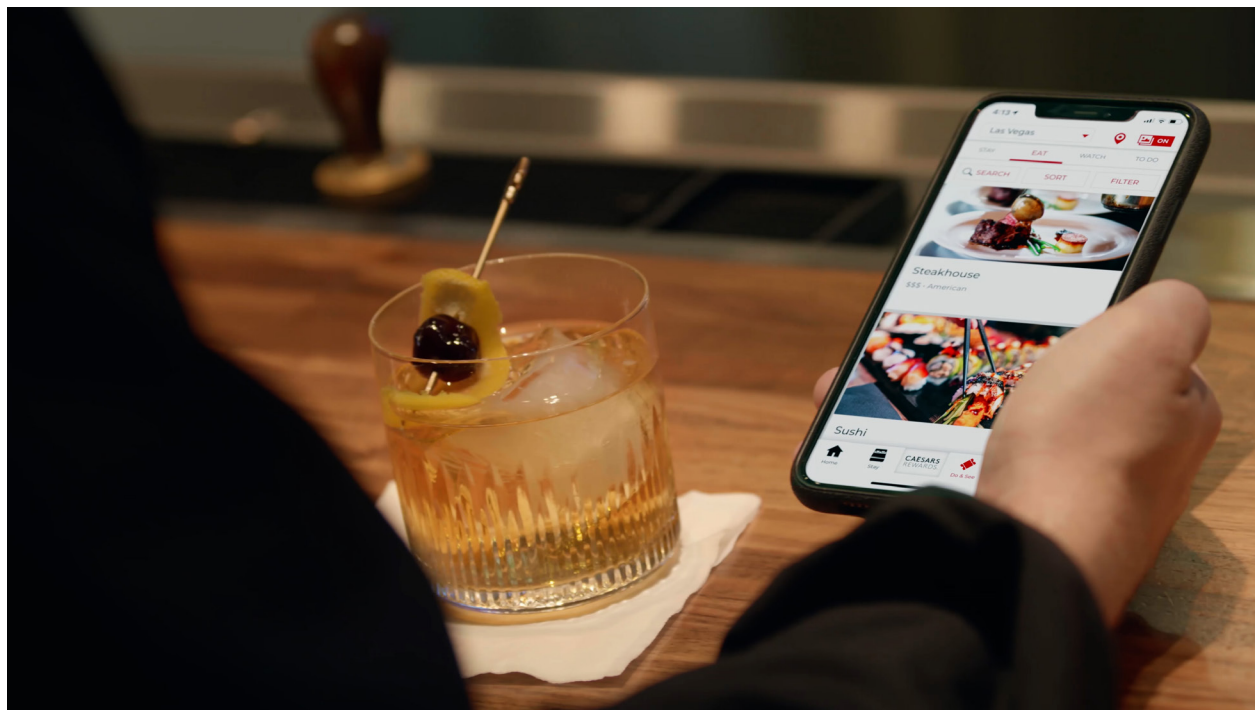
Securing personalized mobile applications is paramount for Caesars' customer experiences across their properties

Caesars' cybersecurity team recently made a decision to transition to a Zero Trust network. As a result, Caesars has updated their cybersecurity reference architecture to reflect the move to Zero Trust and is moving to implement an always-on firewall-based approach as part of this process.

"In pre-zero-trust days, we would have reached the point where we thought we'd done enough, and would put the new firm on the network," says Wilkins. "But in today's zero-trust world, we'll keep that firewall segmentation intact, because there's really no reason that Property A should ever talk directly to Property B." When users of Property B need to access Property A corporate assets, Prisma Access allows Caesars to codify the right policies to ensure that they get what they need.

After establishing appropriate security and access policies with Prisma Access, Caesars then performs what it calls a "dual risk assessment." It engages an external third-party cybersecurity firm to check out both organizations— Caesars and the new company—in a full vulnerability and risk assessment. "This way, both sides feel sufficiently comfortable to connect their networks," Wilkins says.

> "
> This allows us to deliver better applications to our customers.…
> We're a more competitive company as a result."
>
> — **Bobby Wilkins, Vice President of Cybersecurity, Caesars Entertainment**

Benefits

FASTER ONBOARDING OF M&A PROPERTIES

Caesars has been doing mergers for a long time. As such, it has homegrown systems in place to establish rapid connectivity when onboarding an acquired (or in Eldorado's case, a merged) entity. These systems are designed to be secure. Prisma Access takes that security to a new level, however, at speeds previously unmatched. In the past, it took as long as 90 days for Caesars to securely integrate the network of an acquired company. Now, with Prisma Access, it takes one to three days maximum.

Before deploying Prisma Access, Caesars used traditional site-to-site virtual private networks (VPNs), which required them to create tunnels between their different entities. "Whereas with the Prisma Access site, we've got our endpoint defined at our data center, and all we have to do is add the new partner site to that," says Wilkins. "Since we're already connected to the cloud, it couldn't be easier."

SAFE AND FAMILIAR REMOTE USER EXPERIENCE

Prisma Access enables Caesars to assign the same internet outbound policies to their users, whether they're on or off the corporate network. They get the same experience, no matter which company asset they access. "And if they have a problem, it doesn't matter where they are, we can work through it," says Wilkins. Prisma Access also stops them from accidentally going to dangerous sites, "whereas a traditional VPN wouldn't provide that protection," he says.

Traditional thinking was that the only way to protect an extended enterprise network was to bring the traffic to the perimeter firewall. The cloud-based delivery model of Prisma Access brings the service to where it is needed: the edge. This allows cybersecurity teams to seamlessly extend a consistent security architecture to every corner of their network, preventing both known and unknown threats.

INCREASED AWARENESS OF THE NETWORK ENVIRONMENT

Wilkins says Prisma Access allows Caesars greater visibility into the network and its traffic without having to hire additional cybersecurity professionals. "For us, that's key," he adds, "because we're not going to get more people, so we need to better leverage the ones we have." With the enhanced visibility Prisma Access provides, his team can exact increased control, and share appropriate systems and data much more easily.

ABILITY TO STANDARDIZE PROCESSES

The Palo Alto Networks portfolio has enabled Caesars to standardize security onboarding tools with a common user interface. "This makes our processes more simple, consistent, and less prone to errors," says Wilkins. Previously, each acquisition or merger required taking a unique approach to adequately secure networks and systems during onboarding. Today, with Palo Alto Networks, the process is more standardized and easier to repeat, dramatically expediting Caesars' ability to integrate networks and systems flawlessly.

A COMPETITIVE ADVANTAGE FROM A SECURE NETWORK

With Prisma Access, Caesars has been able to standardize security operations, allowing the software to tackle "routine" security issues. Those routine issues add up to 90 percent of all required onboarding tasks.

This gives Wilkins's staff the luxury of spending their time on the 10 percent of cybersecurity issues that need special attention, such as re-architecting a merged company's security posture or processes.

The net result? "This allows us to deliver better applications to our customers—applications that can both interoperate and be securely innovated whenever required without creating a lot of friction," says Wilkins. "We're a more competitive company as a result."

For more information, visit the Palo Alto Networks Prisma Access webpage.