Securing Smart Cities

EM3LABS
+33 751 355 857
solutions@em3labs.eu
www.em3labs.eu

The City of Las Vegas is comprised of more than 20 different departments and provides services to Las Vegas, Nevada's population of more than half a million people. In late 2018, the city's chief innovation officer decided to add another layer of cybersecurity to the city's email, storage, and communication assets. The city selected BitDam ATP because of its high cyberattack detection rates, low false-positive levels, and ability to cover the Microsoft collaboration platforms used by the city: Outlook, OneDrive, and Teams. Since then, BitDam ATP, hosted on Microsoft Azure, has blocked dozens of instances of ransomware, phishing, and more, preventing attacks from penetrating the city's network and saving the city millions of dollars in cyberattack remediation.

A city's need for secure collaboration

Over the past few years, the City of Las Vegas has relied on Office 365, using its cloud-based email service, OneDrive, and Teams to enhance productivity and support collaboration between employees as well as external communications with citizens, vendors, and partners.

While these communication channels are essential, they pose a cybersecurity challenge, as they are potential attack vectors for bad actors aiming to penetrate the city's network. The city's employees communicate with a wide variety of businesses and individuals, with many of them being one-time contacts. This makes them more vulnerable to attacks, as they do not know most of the contacts with whom they communicate in person.

The City of Las Vegas is comprised of more than 20 different departments, using various technological platforms, policies, and processes. The IT security team serves all departments, protecting all users and endpoints.

Michael Lee Sherwood, Chief Innovation Officer, City of Las Vegas, is constantly looking for additional ways to protect the city. *"In cybersecurity, nothing's ever enough. There's always more you can do," he said.*

Security is all about layers

While the City of Las Vegas already had a secure email gateway in place, Sherwood and his team were looking for advanced threat protection (ATP) as an additional layer on top of the city's cybersecurity solutions. They wanted to make enterprise collaboration secure and ensure that end users – the city's thousands of employees – would be safe to click any file or link that appeared in their Office 365 inboxes, OneDrive accounts, or Teams channels. They wanted a cloud-native security solution that would work in harmony with Office 365 and that would be easy to deploy without affecting users' productivity or the way in which they collaborate. “We look at taking a layered approach, and a layered approach is using multiple products – not just one,” Sherwood said.

Protecting all collaboration channels

The City of Las Vegas chose BitDam ATP because of its top detection rates with low false-positive levels and started by deploying BitDam ATP for email. BitDam scans emails pre-delivery to eliminate threats like ransomware, known and unknown malware, phishing, and zero-day attacks before they enter the network. “Deploying BitDam ATP was a five-minute task and the impact was immediate,” Sherwood said. “Once set up, users experience almost zero latency between the time of entry to email delivery, so it was truly seamless.”

BitDam helps organizations around the world secure their enterprise collaboration platforms. Using BitDam ATP for Office 365 email, OneDrive, and Teams protects organizations against advanced content-borne threats hidden in files and links, regardless of their type and delivery method.

Detecting attacks pre-delivery across various collaboration platforms, BitDam’s attack-agnostic cloud-based solution empowers organizations to collaborate safely. BitDam uses Microsoft Azure Platform as a Service (PaaS) resources – including Azure Kubernetes Service and Azure Cache for high performance and increased scalability – to protect organizations of all sizes from ransomware, phishing, and other threats that other security solutions fail to uncover.

Preventing losses of millions

The city soon expanded into protecting its OneDrive and Teams assets with BitDam ATP. “Hosted in Azure, BitDam ATP offers high scalability and agility, making the integration with Microsoft’s collaboration platforms an extremely easy task and literally a two-click assignment,” said Liron Barak, CEO and Co-founder, BitDam.

Protecting OneDrive, BitDam ATP scans all content before it is accessible to end users, and it quarantines malicious files so users cannot be lured to click them. BitDam ATP for Teams scans both files and links shared via Microsoft Teams' Teams, Channels, and Chats (private and public) and quarantines malicious content.

According to Sherwood, “It has made a difference and has identified incidents other products in the city’s environment failed to detect.” Within a few weeks, BitDam ATP detected:

- 26 attacks that bypassed the city’s secure email gateway
- 6 unique attacks
- 2 Emotet trojans

At that time, the savings were already estimated at more than $2 million. According to US-CERT, the United States Computer Emergency Readiness Team, the typical remediation cost of each Emotet infection is up to $1 million for local governments.

“BitDam has been our go-to security tool for all of our Office 365 offerings, and we saw some good results with it,” Sherwood said. “The BitDam system evolves and changes with our organization and interweaves with the technology solutions we are going with.”