Securing the World's Largest Airport with Cisco Advanced Malware Protection (AMP)

Scalable, integrated architecture that can decrease workload, time, and resources

Data is everywhere

When you think of security within an airport, what's the first thing that comes to mind? It is most likely security check points. These security measures are absolutely crucial when it comes to the safety of all customers and workers within the airport. However, these security standards are only protection against physical threats. What about cyberthreats? With advancements in technology, threats have evolved beyond physicality. Cyberthreats at an airport are particularly detrimental. Think about it: airports are goldmines for hackers. Not only do they store airline data from major carriers such as Turkish Airlines, United, or Lufthansa, the airport network also contains business data from restaurants and shops. More importantly, it carries millions of customers' data. Whether passengers are purchasing an item at a store, going through airport security, or connecting to the free airport Wi-Fi; data is essentially everywhere. Therefore, securing beyond physical threats at an airport is extremely critical.

Customer summary

Customer name:
Istanbul Grand Airport (IGA)

Industry:
Transportation

Number of employees:
1 million+ (once completed)

Location:
Istanbul, Turkey

Website:
www.igairport.com

Customer objectives

- Building an airport that includes a fully integrated security solution
- Implementing a flexible solution that can easily scale throughout the three construction phases of the airport
- Need in-depth visibility into all parts of the airport's infrastructure
- Need effective threat hunting and investigation capabilities

Solutions

- Cisco AMP for Endpoints
- Cisco AMP for Email
- Cisco AMP for Networks
- Cisco AMP for Web
- Cisco Threat Grid
- Cisco Stealthwatch
- Cisco Identity Services Engine

Results

- Effective security throughout the airport's IT infrastructure—from network, web, email, to endpoint
- Enhanced visibility and threat hunting capabilities to prevent attacks from entering the airport's network
- Integrated architecture allows IGA to see a threat once and block it everywhere in the environment, thus decreasing admin workload and time for remediation
- Scalability in management with flexible APIs

Constructing the largest airport in the world

Istanbul Grand Airport (IGA) was founded in 2013 and is on a mission to construct the largest airport in the world. IGA recently completed and launched the first phase of the airport, which encompasses two runways and can accommodate 90 million passengers. Once fully complete, IGA intends to hire approximately 1.5 million employees and will have the ability to connect up to 200 million passengers in over 300 destinations, annually.

The airport is currently being constructed in an area of 76.5 million square meters, north of Istanbul, which is Turkey's largest city and Europe's fourth most populated city; currently with 15 million residents and 7 million foreign visitors a year. Because Turkey sits geographically at the center of four critical regions—Asia, Africa, the Middle East, and Europe—this airport will be considered a central hub for the world.

“We’ve built Istanbul’s airport as the world’s largest airport and with security as a foundation. And we are happy to partner with Cisco to secure this airport.”

Ersin Inankul
Chief Information Officer,
Istanbul Grand Airport

Built with security as a foundation

IGA is constructing the Istanbul Airport from the ground up. But before even beginning construction, security was always a priority in the airport leadership’s blueprints. IGA acknowledged the importance of encompassing a strong security infrastructure and had plans to build the world’s largest airport with security as a core foundation. Emrah Bayarcelik, the head of security at IGA, states, “At IGA, our business objective is to provide smooth operations for our passengers, starting from the check-in point to takeoff.” In order to ensure the most effective security solution for this airport, IGA engaged with Destel, a Managed Detection and Response (MDR) partner, to fully understand the best options for the airport.

IGA’s Chief Information Officer Ersin Inankul explains, “One of the biggest challenges of this airport is integration.” Hence, a security solution that is integrated was one of the most important requirements for IGA. The leadership wanted the airport’s entire infrastructure to be fully aligned, from the network all the way down to the endpoints. “We were looking at the integration, visibility, and implementation features of the products,” says Bayarcelik.

“Out-of-the-box integration is really important to us. The implementation process is not easy in the SOC operations. But we saw that Cisco AMP Everywhere has very easy deployment features and usability features.”

Emrah Bayarcelik
Head of Security,
Istanbul Grand Airport

In addition, because the airport is building this structure in multiple phases, it required a solution that has the ability to easily scale. The projection is that IGA will expand from serving 90 million customers in phase one to 200 million customers in phase three. To scale at that extreme level, IGA understood that on top of incorporating an integrated security architecture, they also needed to ensure ease of use for their employees.

Lastly, Inankul stated that, “Endpoint is absolutely critical for me.” IGA and Destel, its MDR provider, understood the importance of securing the endpoints using solutions that provide both Endpoint Detection and Remediation (EDR) capabilities as well as Endpoint Protection Platform (EPP) features. Destel will manage IGA’s IT infrastructure for the next three years and requested an endpoint solution that has in-depth visibility and advanced threat hunting and investigative capabilities.

An airport that scales needs a security solution that scales

To fully secure the world’s upcoming largest airport, IGA and Destel deployed the Cisco® AMP Everywhere solution, which encompasses Cisco AMP for Endpoints, AMP for Networks, AMP for Email, AMP for Web, and Threat Grid. With a full Cisco Security integrated architecture, IGA feels confident that customer and business data will be protected and secured. Destel SOC Manager Suat Celikok says, “Using AMP Everywhere, we gain visibility, unified information sharing, and a faster time to detect and respond to threats.”

Additionally, Cisco AMP Everywhere is easy to deploy. Its flexibility will allow IGA to simply scale its IT infrastructure as the airport and IT team expands throughout their construction phases. Through the integrated architecture, IGA is fully protected—from network, to email, to web, all the way to endpoints. One of IGA’s SOC analysts, Anil Kus, explains, “We are using Cisco AMP Everywhere because it gives us file reputation, file analysis on our endpoint platform, web platform, network platform, and email platform.” Using AMP Everywhere, IGA will be able to see a threat once and block it everywhere else in their environment, thus decreasing the security administrations workload and time to detect and remediate against threats. “Without integration, my team will be focusing on false alerts and will be spending more time on different consoles”, says Celikok.

On top of everything, Cisco AMP for Endpoints gives IGA visibility into all devices, files, and applications that enter into the airport’s network. Through AMP’s retrospective security, IGA will be able to see the entire history of a particular file or device, leading to more effective threat hunting and investigative capabilities.

“When we started using Cisco AMP for Endpoints, we noticed greater visibility, more effective threat hunting and investigation, and faster detection and response.”

Suat Celikok
Security Operations Center Manager, Destel/Istanbul Grand Airport

Securing the central hub in our world

With the full Cisco AMP Everywhere architecture fully deployed in the airport’s infrastructure, IGA is able to protect both the airport’s business and customer data. Since deploying, they already witnessed greater threat hunting and investigative analysis and in-depth visibility in their network and endpoints.

With the next phase of the airport construction underway, IGA’s leadership is confident that they can easily scale this solution to their business goals. Inankul concludes “We have built Istanbul’s airport as the world’s largest airport and with security as a foundation. And we are happy to partner with Cisco to secure this airport.”

C36-741738-00 01/19