

Turkish Airlines Takes Security to New Heights with Cisco AMP for Endpoints and Cisco Umbrella

Effective threat hunting and incident response capabilities to better protect customer and business data

Challenges:

- Lacked proactive threat hunting capabilities and needed to accelerate incident response and detection
- Needed to gain in-depth visibility into all devices, applications, and files operating in their network
- Required to more effectively secure critical business data against advanced attacks

Solution(s):

- Cisco Advanced Malware Protection (AMP) for Endpoints
- Cisco Umbrella

Results:

- Enhanced visibility with added threat hunting capabilities to prevent attacks from entering into their network
- Seamless interactions between solutions resulted in shorter time to detect and respond against advanced threats
- Implemented ransomware and fileless malware protection to strengthen defenses for customer and business data

The customer summary:

Customer name:

Turkish Airlines

Industry:

Airline and Operations

Number of employees:

31,500

Location:

Istanbul, Turkey

Website:

www.turkishairlines.com

Widen your world

Today, air travel has revolutionized how people explore the world. If you're feeling inspired to hike Mount Kilimanjaro or crave some downtime at a beach in Bali, you're simply a plane ticket away. Not only is the world easier to travel, but it is now more accessible. We can visit friends and family or do business across the world, all through a quick flight purchase online. With almost every step of the buyers' journey becoming digitized – from buying airfare on a website, flight check-ins on your mobile devices to scanning your ticket before boarding the aircraft – the idea of widening your world has become increasingly less complex. However, with these innovations come potential security risks for both Turkish Airlines and their customers.



Voted Europe's best airline: Turkish Airlines

It has been said that Turkey lies in the center of the world. As such, it is the perfect location to position one of the largest global carriers paired with the largest airport in the world, right at the geographical heart of our planet. With simple access to four prime regions – Asia, Europe, Africa and the Middle East – Turkish Airlines has earned the notable distinction of serving to over 302 destinations in 2017, the most of any major carrier.

Founded in 1933, Turkish Airlines has grown to be one of the world's largest airlines. As the national carrier of Turkey and a Star Alliance member since 2008, Turkish Airlines currently employs over 30,000 people and flies to over 120 different countries. The airline's Chief Information Officer, Ali Serdar Yakut, states that "by 2023, Turkish Airlines is looking to increase the number of aircrafts to 500" in hopes of better connecting the world.

Prioritizing customers means prioritizing security

In 2017, Turkish Airlines serviced approximately 80 million customers. With such a large amount of customer and business data to maintain, the need for exceptional security was crucial. Turkish Airlines' Vice President of Information Technology Governance, Kadir Yildiz, stated that "the primary goal is to ensure customer satisfaction at all cost."

Yildiz also mentioned that "in recent years, security has become more important than IT operation". It has simultaneously created more demand for automation due to the industry modernizing the customer's journey, but without the sacrifice of security. With confidential customer data potentially at risk, it was important for Turkish Airlines to upgrade their security posture to encompass more Endpoint Detection and Remediation (EDR) capabilities such as continuous monitoring to enable greater endpoint visibility. Yakut states "we need to be pioneering new technology to better understand our customers and also create efficiency in our operation". Because of the increase in customer demands as well as the frequency of cyberattacks, security became paramount for Turkish Airlines' business success.

With the escalation in sophisticated attacks, Turkish Airlines also needed to incorporate more effective threat hunting and incident detection and response capabilities. Their security team was previously spending countless hours, and even days, detecting and remediating threats. Turkish Airlines understood that it was necessary for them to decrease their time to respond to threats. Yakut stated: "having this operation without any disruptions and securing the data of these customers is really important for us."

“The flexibility and network visibility that is provided by Cisco AMP and Umbrella has made our operations more effective.”

Kadir Yildiz
VP of IT Governance



Let your customers focus on the experience

To more effectively secure customer and business data, Turkish Airlines deployed both Cisco AMP for Endpoints and Cisco Umbrella. With the ability to proactively hunt for advanced attacks, Turkish Airlines can now discover new threats before they can harm their business.

Most importantly, Turkish Airlines can now protect and remediate against attacks in a more efficient manner. Yildiz acknowledges “using Cisco AMP is like having another pair of hands, in a sense”. With Cisco AMP closely working with Cisco Umbrella, users gain the first layer of defense on the internet down to the very last layer on the endpoint. In addition, using Cisco Threat Response on top of these solutions will allow Turkish Airlines to gain the much-needed visibility and investigative analysis into their environment. Yildiz stated “We can monitor the whole system architecture through it.”

Turkish Airlines was most impressed with AMP’s retrospective security. Enabled by continuous monitoring of all applications and files that enter their network, Turkish Airlines is now able to leverage the rich application and file context to enhance their threat hunting capabilities. Yildiz emphasizes that “the flexibility and network visibility that is provided by Cisco AMP and Umbrella has made our operations more effective.” With Turkish Airlines focused on security, it will allow their customers to focus on the experience.

A simpler and safer tomorrow for Turkish Airlines

As a result, Turkish Airlines benefitted immensely from the new additions of Cisco AMP for Endpoints and Umbrella in their environment. What originally took them days to detect and remediate, now only takes them hours or mere minutes.

Turkish Airlines has, “started to provide uninterrupted services to end users at more than 400 locations”; Yildiz witnessed how investment in greater security is providing immediate and impactful returns for their business. With Turkish Airlines focused on strengthening their security postures, it provides them the freedom to deliver greater customer experience and service. With Cisco security, Yakut quotes “we are [securely] connecting the world.”

