

# Airport Security Model for IT




**1 Cisco AnyConnect**

Like your driver's license, you have to show your proof of who you are to get into an airport, and AnyConnect works like this to secure endpoint access and ensure they are "compliant" to be on the network.




**2 Cisco Umbrella (OpenDNS)**

This is a No-fly List check — it blocks malware, botnets and phishing, preventing them from getting on the network (or on the plane) by automating threat protection to detect attacks before they are launched.




**3 Cisco Identity Services Engine (ISE)**

Cisco ISE verifies who/what/when/where, just as your airline ticket would document and authenticate the device connecting to the network. If it's deemed unqualified to enter, it can even contain a suspicious device for remediation.



**4 Cisco ASA w/ FirePOWER Threat Defense**

This is a single platform next-generation firewall (NGFW) that offers multilayer protection. Like a TSA agent standing guard and looking for potential issues, it determines if you're allowed to proceed to the gate. It combines the proven security capabilities of the Cisco ASA Firewall with industry-leading Sourcefire® threat and advanced malware protection features in a single device.




**5 Cisco Cloud Web Security, Cisco Web Security Appliance (WSA) and Cisco Email Security Appliance (ESA)**

Like the extra security an x-ray machine provides, these applications correlate files and block suspicious attachments with global threat intelligence, advanced sandboxing and real-time malware blocking for web and email security. They continuously analyze file activity across your extended network, so you can quickly detect, contain and remove advanced malware.




**6 Cisco CloudLock**

CloudLock acts as a cloud access security broker (CASB) and provides visibility and analytics around user behavior and sensitive data in cloud services, including SaaS, IaaS and PaaS. We can compare it to the passport, with country-specific protections.




**7 Cisco AMP and Cognitive Threat Analytics**

Just to be thorough, sometimes we need to check your hands for suspicious residue. In this case, AMP Threat Grid analyzes suspicious behavior in your network against more than 450 behavioral indicators and a malware knowledge base sourced from around the world. As a result, AMP Threat Grid provides more accurate, context-rich analytics into malware than ever before.




**8 Cisco Stealthwatch**

With Stealthwatch, you see everything happening across your network and data center. You can uncover attacks that bypass the perimeter and infiltrate your internal environment, just as a camera security system would be used to prevent potential issues.



**9 Cisco TrustSec**

Now it's time to present your boarding pass, the final check before getting on the plane. TrustSec is scalable and agile segmentation technology that is embedded in more than 40 switches, routers, wireless devices and other Cisco products. Control access to critical enterprise resources by business role, device type and location, so policy changes can be made without redesigning the network.



**Cisco's network security strategy — a pervasive and layered approach**

Cisco network security is achieved in layers, and it has to be pervasive throughout, not just in one location on the network. Spend your time flying high with Cisco.



Find out more about Cisco at [OneNeck.com](http://OneNeck.com)