

Our Mobile Addiction what could possibly go wrong?

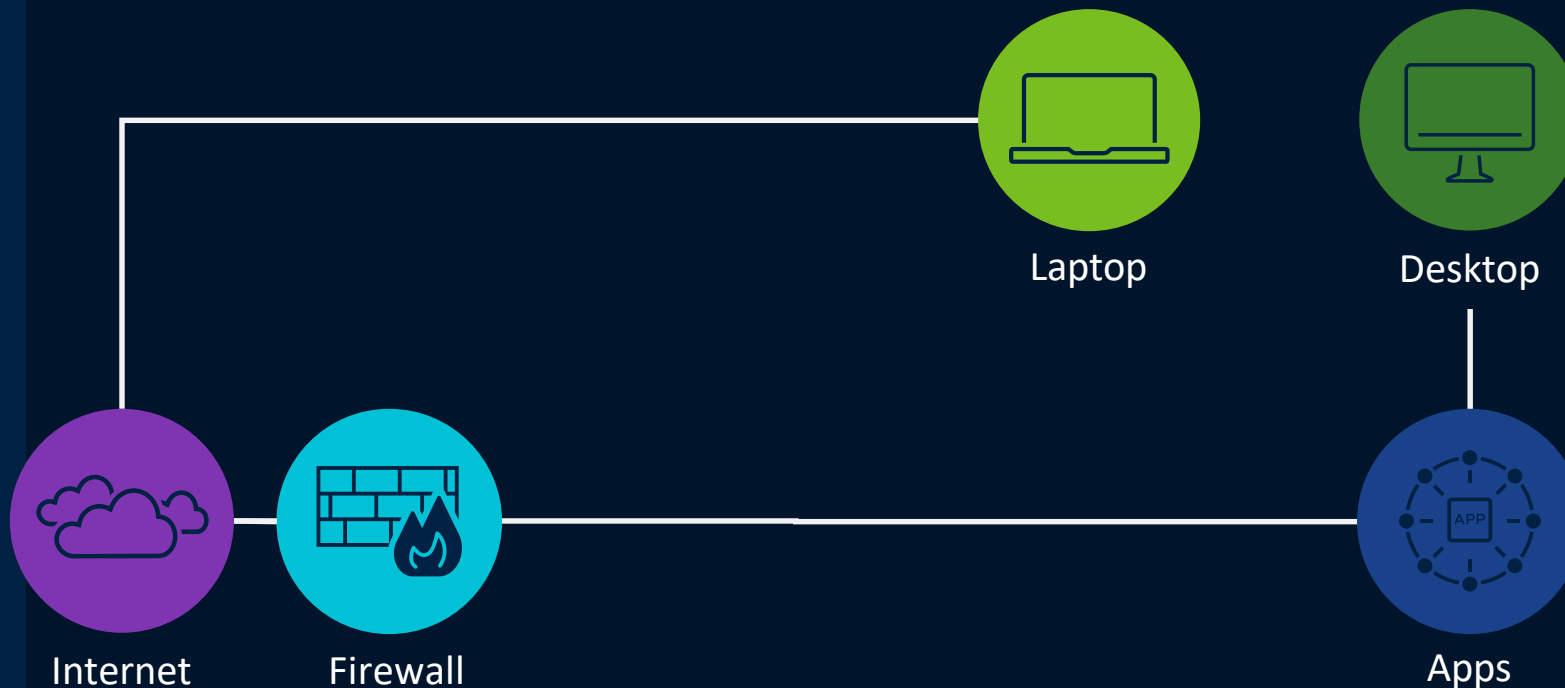
Jon Baker

Staff Solutions Engineer - VMware EUC

November 20, 2019

In the beginning

Trust wasn't really a thing



First, there were apps.

Then we added a desktop to access them from the office desk.

Then a laptop to work on them from home (offline)

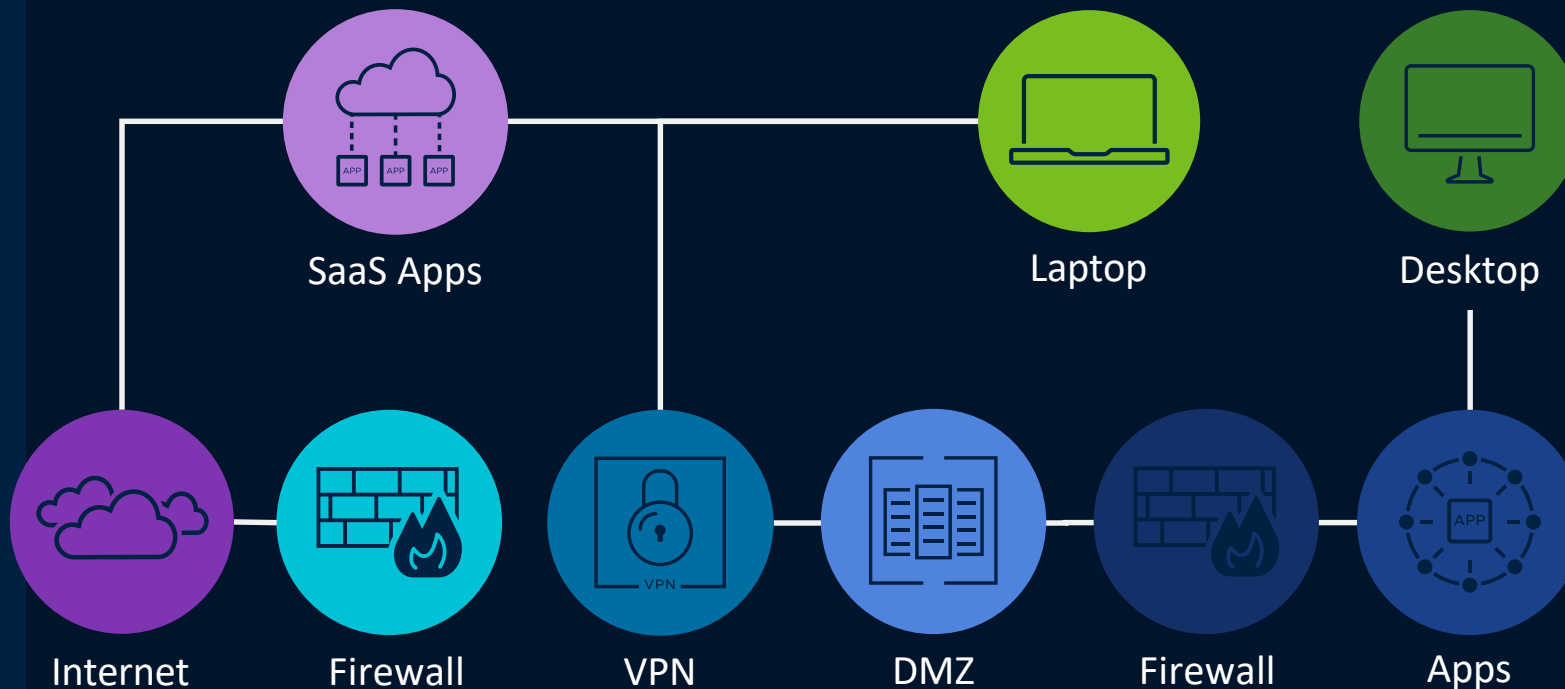
Enter the Internet, and we could connect to the office from anywhere.

But we needed to protect our apps, so we added a firewall.

Firewalls became the control point for access to all of our apps and networks.

Then things got complicated

The Internet created new challenges



But we still wanted to work from anywhere...

So we came up with VPNs, which stretched the office network to our laptops.

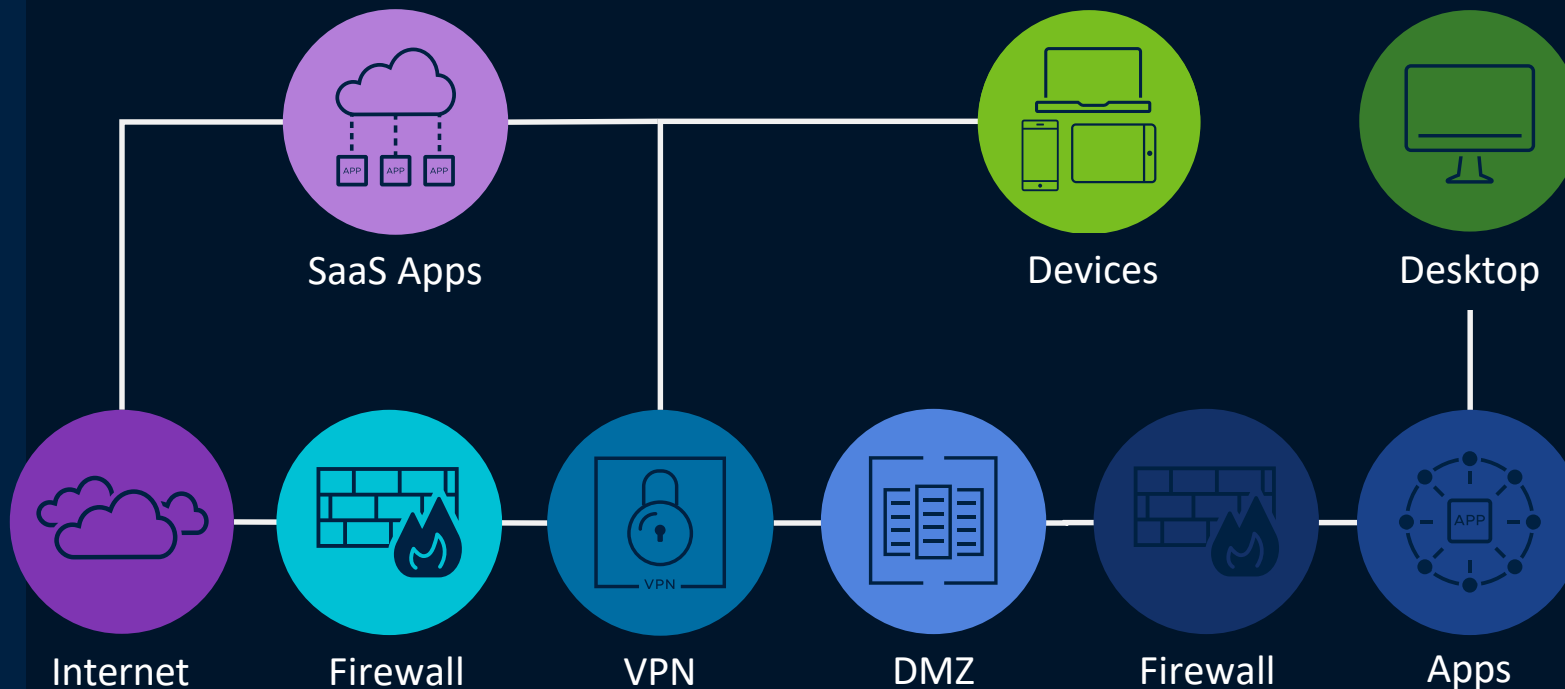
But that gave people too much access, so we added DMZs and more firewalls.

And this worked for a long time.

Until SaaS apps showed up. And they didn't run inside our network.

SaaS and mobile hit the scene

We had to track a lot more things in a lot more places



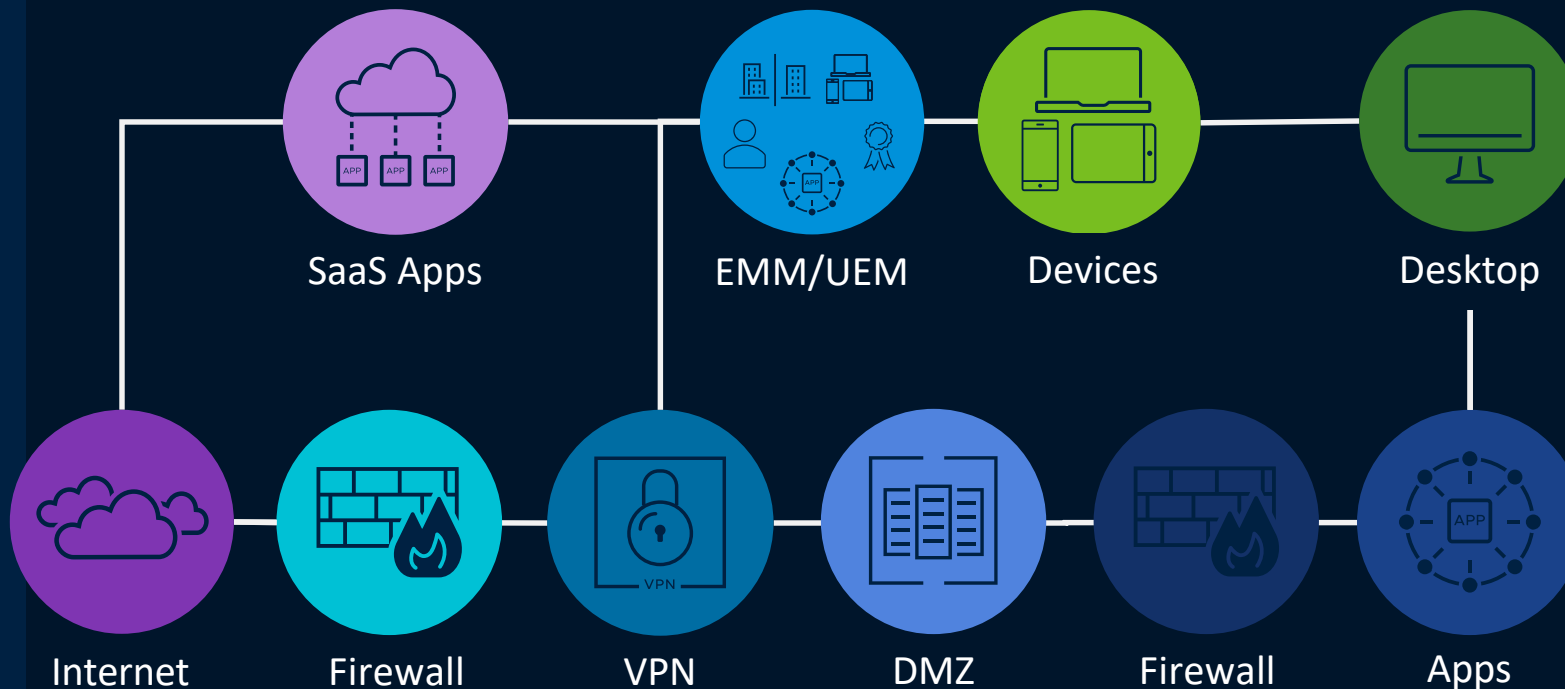
Now add smart phones and tablets and watches and...

Some of us tried to control SaaS access by making everything look like the office.

This let us keep our control point at the firewall, but it forced everyone to come through the office network first.

The perimeter went global

Different times call for different measures



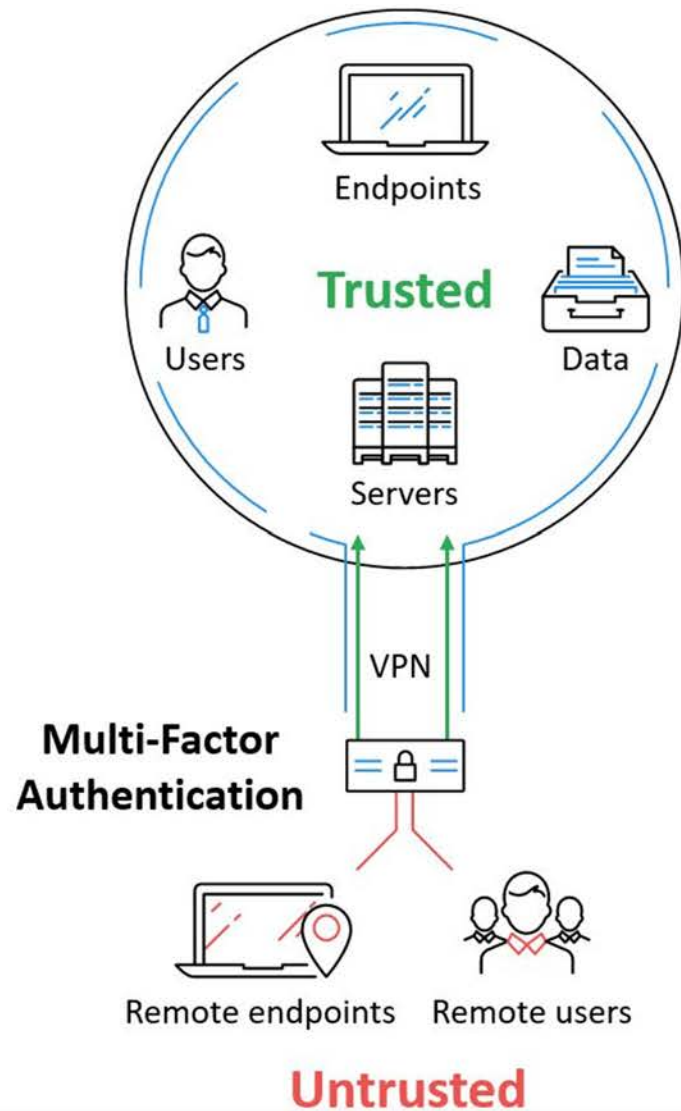
What if we could manage control from any device?

What if we could dissolve the perimeter firewall and treat external access the same way we treat internal access?

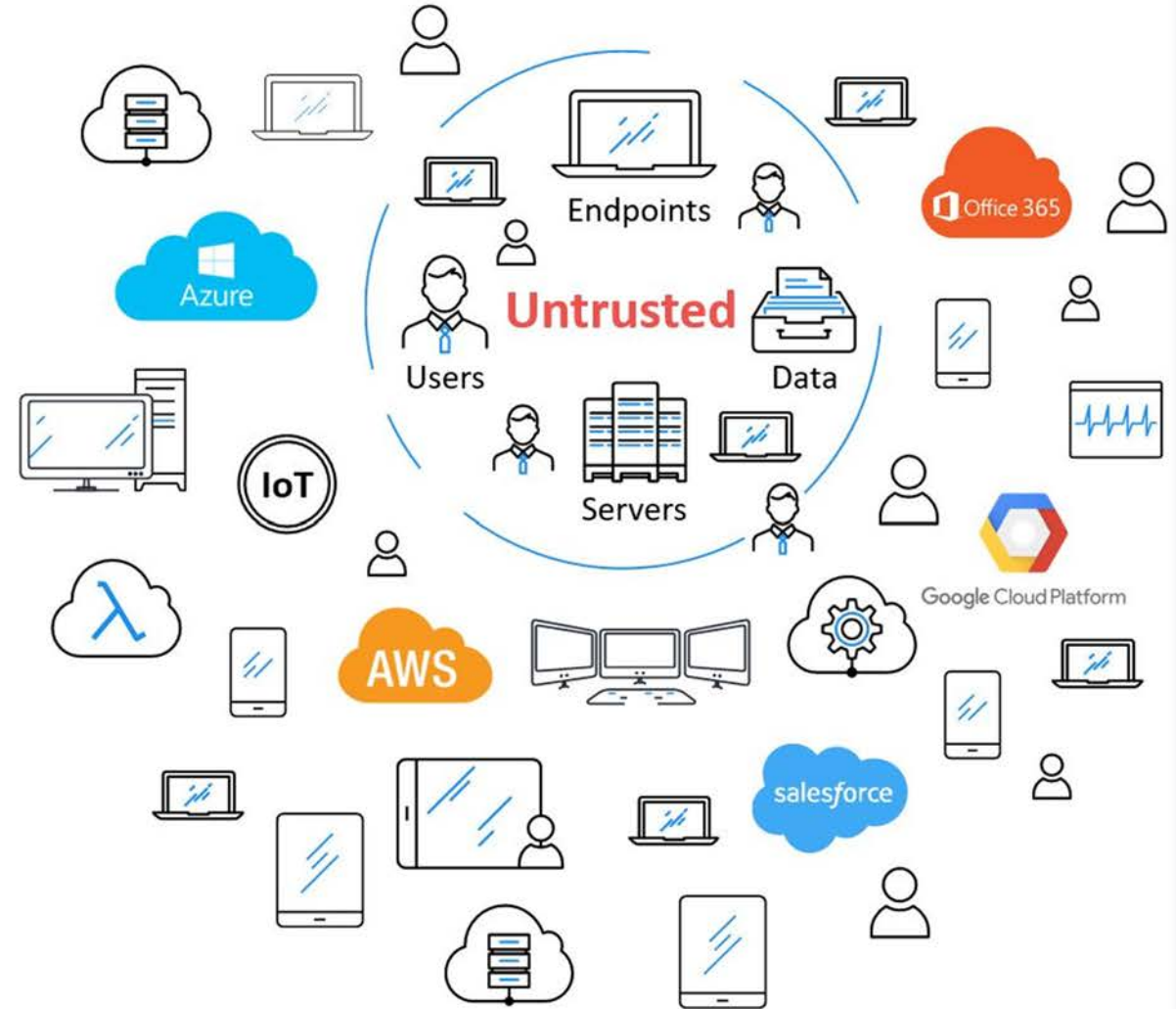
What if we could provide certificate-based authentication and single sign-on from mobile devices as well as your PC or Mac?

What we need is a new control point.

Legacy Networks

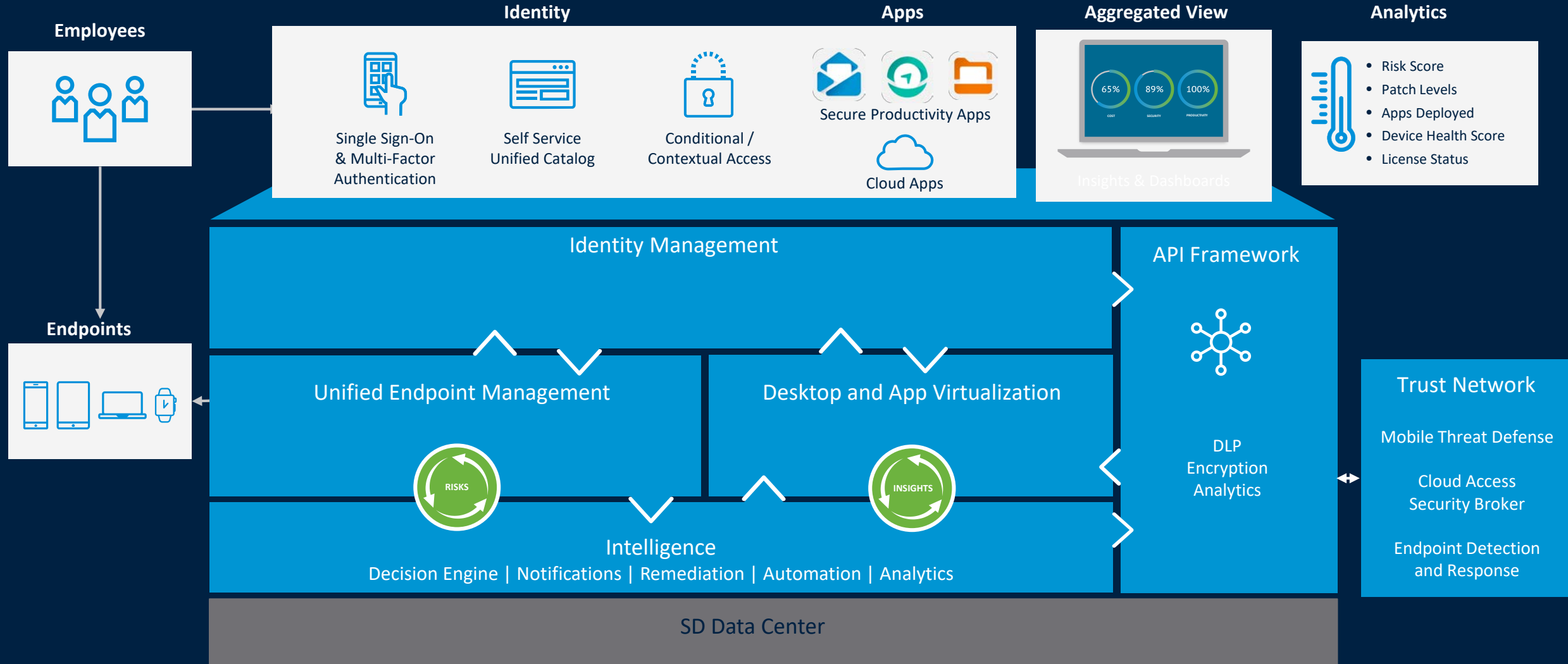


Today's Perimeter-less Networks



Digital Workspace Security

End-to-End Security



So how do we secure things today...





Ring-a-ding: IoT doorbell exposed customer Wi-Fi passwords to eavesdroppers

-Arstechnica

Google enlists outside help to clean up Android's malware mess

-Wired

“Attackers can use that access to trick vulnerable phones into giving up their unique identifiers, such as their IMEI and IMSI numbers, downgrade a target's connection in order to intercept phone calls, forward calls to another phone or block all phone calls and internet access altogether.”

-Techcruch

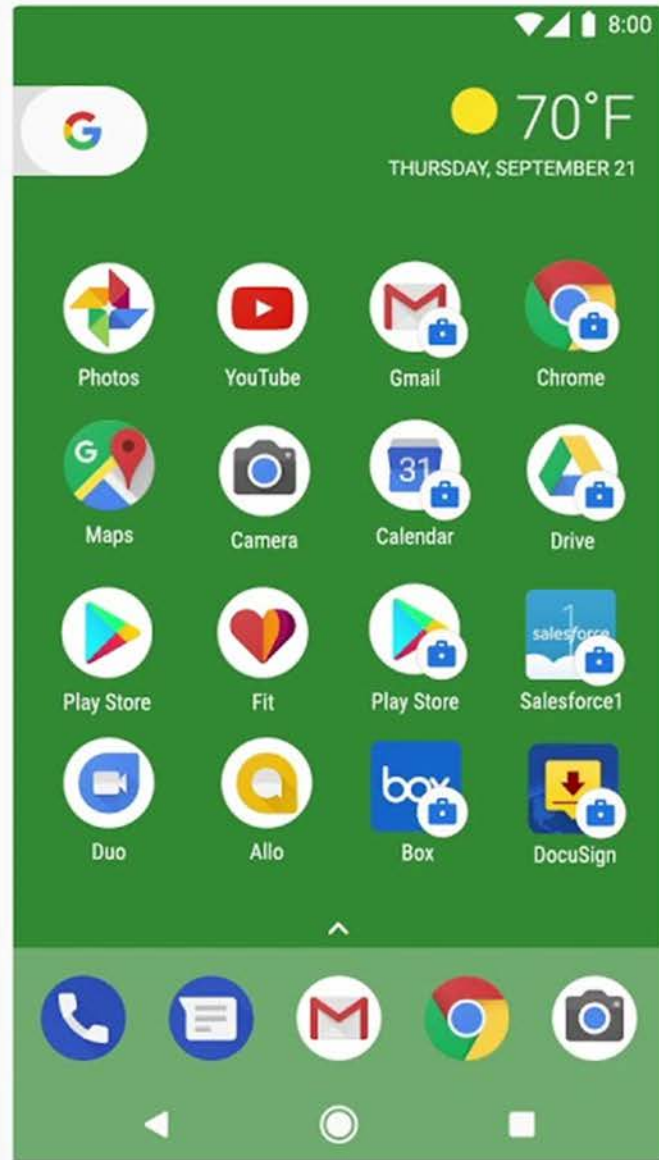


Facebook App Using iPhone Camera Without User's Knowledge

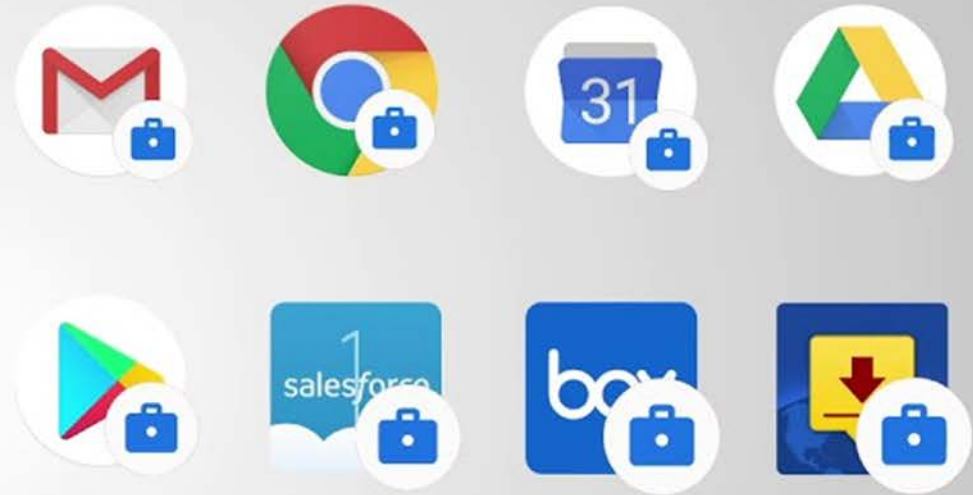
-mactrast




iOS & iPadOS 13 for
Enterprise



Androidenterprise




 Sign in with Google


 Sign in with Facebook

 Sign in with Twitter

 Sign in with Microsoft

 Sign in with GitHub


 Sign in with Foursquare

 Sign in with LinkedIn

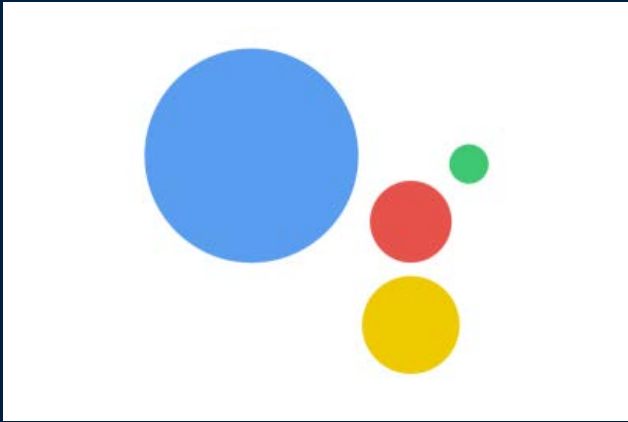
 Sign in with Instagram

 Sign in with Evernote

 Sign in with Dropbox

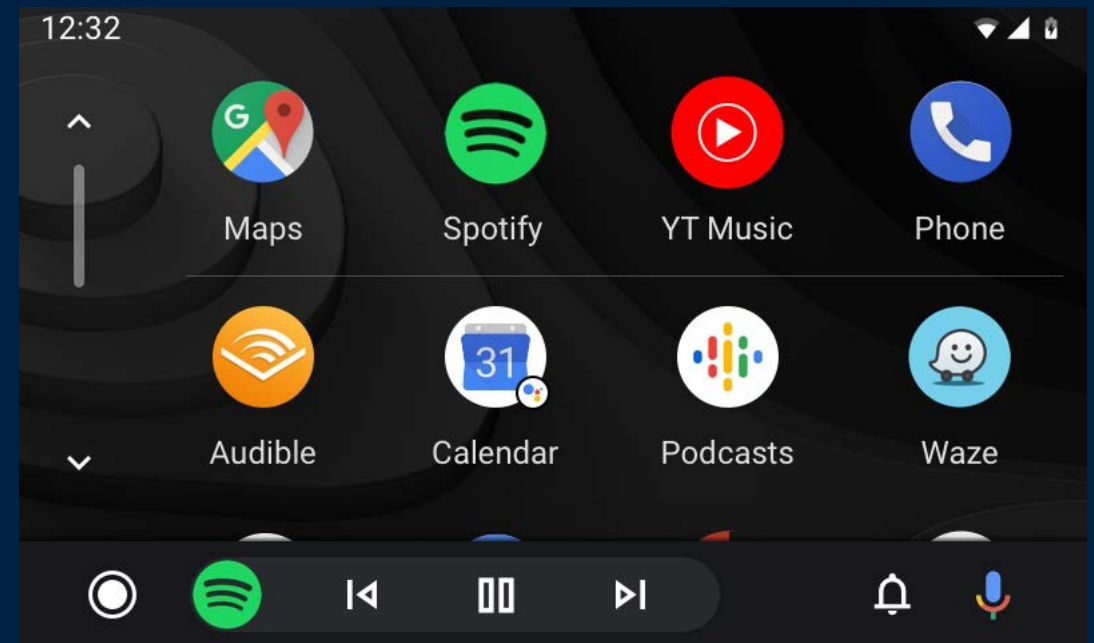
 Sign in with Apple



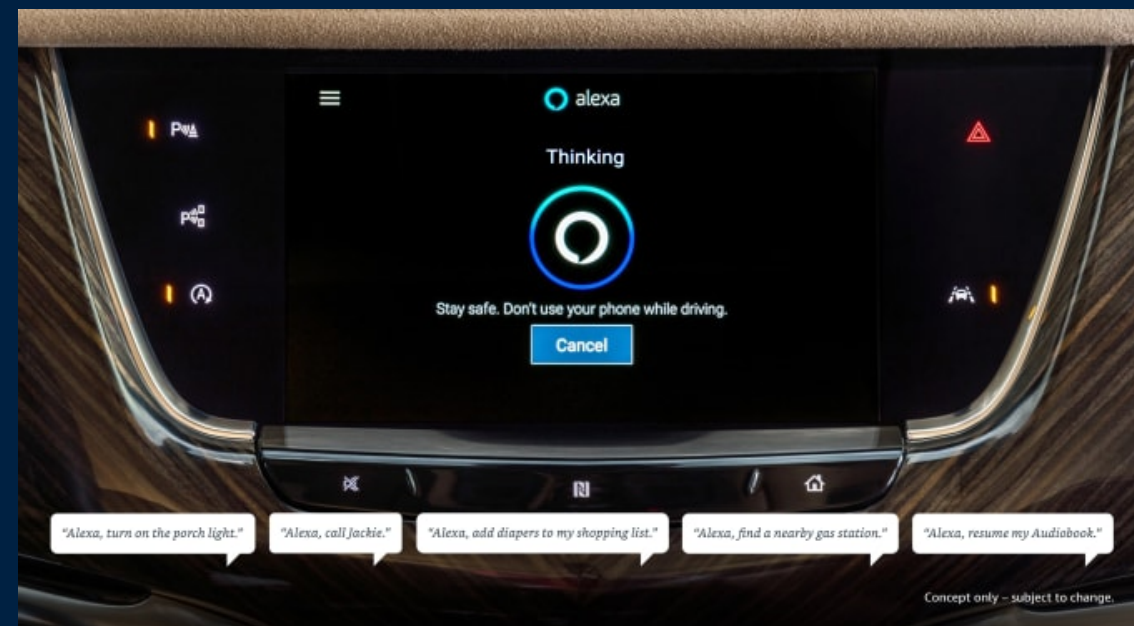
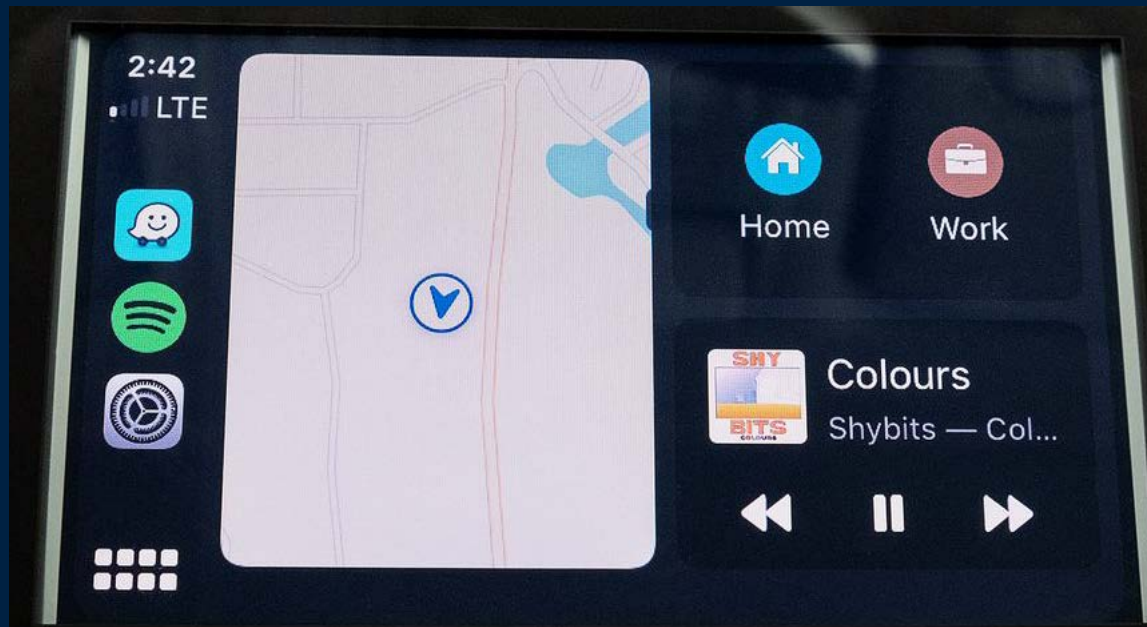


Who's Listening...





Anyone Distracted Yet?





Questions