SOLUTION BRIEF

Remove the Risk to Sensitive Data Created by Mobile & IoT

ALTR protects sensitive enterprise data in a connected world

Previously unfathomable connectivity and mobility have shaped the past decade. Untethered workers were freed to tap into business data anytime and anywhere, while connected Internet of Things (IoT) devices ensured there was more than enough data to keep them busy.

Mobile and IoT are all about greater experiences, connection, and convenience. But at what cost?

Consumers jumped headfirst into the uncharted waters of mobile and IoT. Businesses (some reluctantly) were quick enough to follow, with many forced to adapt as the line between users' personal and business devices became blurred. New innovations and functionalities bring with them new vulnerabilities. Not only does IT now have to worry about the security of company assets, but also the myriad end-user devices with access to sensitive corporate data. The attack surface has expanded.

So, what's more important: getting new applications out the door and into your customers hands, or making sure your sensitive data is safe?

An expanded attack surface

More than 80 percent of Americans have a smartphone, and U.S. households have an average of 11 connected devices. As 5G coverage expands, the number of endpoints will only increase, for both consumers and businesses. IDC forecasts there will be 41.6 billion connected IoT devices by 2025.

With that kind of penetration, it's no surprise that mobile and connected devices present an alluring target for cybercriminals. It only takes one vulnerability to give easy access to a user's sensitive and private data. But the breach of a single device is just the beginning.

When cybercriminals get access to a device, they can also get access to corporate data that device's owner may be privy to through their employer. The business breached may be none the wiser that someone other than the end-user is accessing their data. Worse still, when they do determine something is amiss, it can take months to figure out what exactly was taken.

The risks of mobile and IoT

Apple and Google go to herculean efforts to keep devices secure, and those efforts result in security measures that are generally near impossible to best. It's why the FBI spent $900,000 to get access to an iPhone.

However, the latest patches and updates often fail to make their way to devices in a timely manner due to the complexity of the mobile ecosystem. A Federal Trade Commission report found devices are not effectively getting the security patches they need, expanding the attack surface and increasing the changes of a breach.

Most successful attacks are not through zero-day exploits, but rather known and not yet patched vulnerabilities. Even if we could ensure always-up-to-date, ironclad security on mobile and connected devices, humans remain the weak link in the security chain, potentially letting malicious software in through back door application installations or unintentionally letting bad actors in through the back door.

New networks of untrusted devices and millions of new data flows have had a multiplier effect on the risk to data, but connectivity and mobility are instrumental for innovation. So again, how can businesses realize these benefits without compromising on data security?

Connectivity without compromise

The current process of tacking on security solutions at the end of the development process is not only inefficient, but it adds unneeded costs and complexity. The bottom line is this approach is a nightmare for everyone. Development comes to a halt, while security is pouring time and money into tools that are clearly not full-proof and IT is bogged down ensuring these tools are properly installed and integrated into the application. This “aftermarket” approach to security isn’t working for anyone.

80% | of Americans have a smartphone

Fortunately for everyone involved in this process, there is a dramatically simpler, more effective data security model. ALTR’s DataSecurity as a Service allows for connectivity and mobility without compromising on data security.

Protection across untrusted devices

ALTR protects your data wherever it is, whether accessed from a mobile or connected device, a laptop, in the cloud, or on-prem —assuring security with real-time data access monitoring, governance, and at-rest protection of your sensitive data, all delivered easily as a service.

Dynamic masking allows you to easily decide who can see what data, ensuring users only have access to the minimum number of fields needed todo their job. To top it off, you can also set thresholds to block access once the limit has been reached. By controlling what and how much sensitive data users can access and logging all data requested and returned in an immutable audit log, ALTR mitigates the risk to data, wherever it is.

Protection across untrusted devices

Today’s anywhere, anytime users require anywhere, anytime protection that works -- security beyond patches and updates. With ALTR, you have the freedom and flexibility to innovate faster and deliver more features, functions and customer experience without sacrificing your security, privacy, compliance, or customers’ satisfaction. Plus, security and compliance teams are satisfied because they finally have the visibility, control and protection that they need.