Lookout®

WHITEPAPER

Putting the trust in Zero Trust

Mobile security for a new age of work

There are three key statements enterprises must consider in order to move forward in protecting corporate resources from leakage and attack:

1. The perimeter has disappeared.
2. Legacy security technologies do not apply.
3. Devices cannot be trusted.

As employees continue to use a mix of managed and unmanaged devices, it sets up the need for a new security architecture: Zero Trust for mobile.

The problem

Your perimeter has disappeared

Work has fundamentally changed. Critical data has moved to the cloud and employees are able to access it from any network, on any device, wherever they are in the world. For example, employees don't often have to connect to a VPN in order to check their work email or view/download sensitive documents on the go.

Enabling mobility and the ability to access data seamlessly is a great advancement for enterprise productivity, but it causes a serious challenge to security teams who rely on perimeter provisions such as firewalls and secure web gateways.

The reality is, enterprise data simply does not live there anymore. It's fluid, moving, and accessible. Data in the cloud is accessed by mobile devices, so corporate data usage remains outside the reach of most security tools. With this ecosystem shift, two new security necessities emerge:

1. **Move key security functions to the mobile endpoint**
   As mobile devices don't operate within traditional perimeters, security must move to those endpoints. It doesn't make sense to put guards in front of your castle when the castle walls don't exist anymore. Security needs to be everywhere the data is accessed by employees.
2. **Establish a Zero Trust access model for mobile**
   Even with security residing on the endpoint, the enterprise should never assume the device is innocent until proven guilty. This new world demands that all device health must be continuously checked in order to allow access to corporate data.

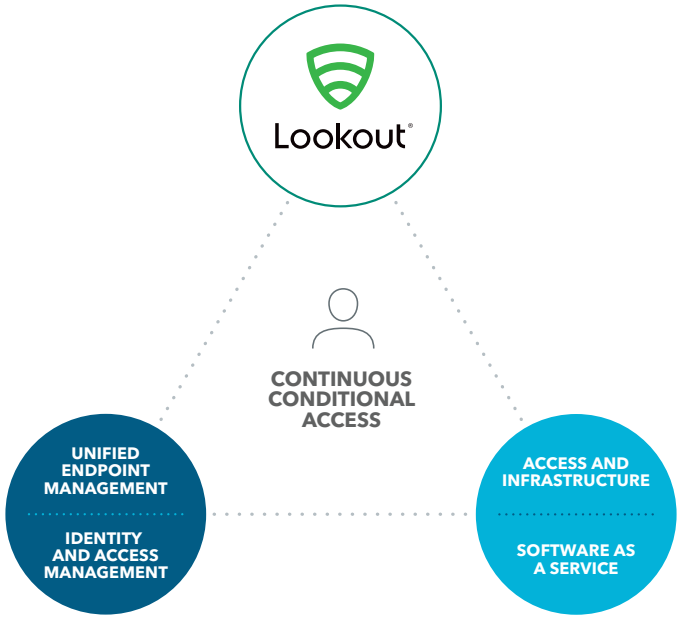
Zero trust: The origins of this term are from a 2013 research paper by Forrester for NIST titled, *Developing a Framework to Improve Critical Infrastructure Cybersecurity*. That research was itself based on earlier work into de-perimeterization done by the Jerricho Forum beginning in 2004.

A new security architecture

Continious Conditional Access

In practice, Zero Trust necessitates a new security strategy that enables dynamic monitoring of mobile endpoints as they connect to corporate data - continuous conditional access. At its core, continuous conditional access is made up of three distinct, but connected puzzle pieces:

- Endpoint protection
- Access to cloud
- Identity



Assessing device risk using an endpoint protection solution is a crucial aspect of a Zero Trust architecture. This approach requires continuous visibility into any threats or risks on the device. Only with this continuous visibility can an organization decide whether or not an employee device is healthy enough to authenticate and access corporate resources. Through this protection, policies can be enforced, in real time, based on an enterprise's specific risk tolerance. **Any endpoint security model must include mobile endpoints** – otherwise an organization has a massive blindspot. **While organizations will spend over $7B on endpoint protection in 2020, only $300M of that will focus on mobile. (Gartner Information Security Forecast Q2 2019)**

The rise of cloud productivity services like Microsoft Office 365 and Google G Suite, is driving a rapid increase in mobile users working with corporate data beyond email. Access to these cloud services must be monitored on a continuous basis.

Protecting access to the corporate cloud without relying on perimeter defense is another crucial aspect of this architecture. To make this possible, critical security protecting cloud access must move to the endpoint. Most corporate data accessed by laptops is now available on mobile devices. Put another way - every cloud service has a mobile app. Office 365, Google G Suite, Salesforce, Workday, ADP, and so on.

Integration of continuous endpoint monitoring with an identity solution, such as a Single Sign-on (SSO) provider, can allow an employee to authenticate and access corporate resources. At the same time a user can be dynamically denied the ability to authenticate when their device is deemed insecure. As the endpoint risk is continuously assessed, with access revoked any time a new risk is detected. One example of this is a user connecting to a malicious network. While they are connected to that network, access to corporate email and other enterprise apps will be blocked.

Continuous Conditional Access

We refer to the continuous assessment of risk and using that assessment to control access to resources as "Continuous Conditional Access." This means that together, the three pillars of Zero Trust security are always watching to ensure that your enterprise risk levels are not crossed. Mobile risks come from devices running an out of date OS, rooted or jailbroken devices, or users that have installed applications posing a risk to enterprise data. When these risks are present, access is denied, thereby protecting your corporate resources.

Solution

How Lookout allows you to embrace Zero Trust security

Lookout has specifically designed our platform to give enterprises a tangible way to bring Zero Trust security to their organization. Lookout Continuous Conditional Access protects corporate data accessed by any mobile device in the enterprise.

Only Lookout delivers dynamic monitoring of device health that leverages security telemetry from nearly 200 million devices worldwide and over 100 million analyzed apps. This gives us advanced visibility into mobile threats, regardless if it resides in an application, device, or on the network. Because of this, we are able to provide enterprises with immediate visibility into potentially harmful scenarios happening on employee devices, at any given point in time.

Through mobile endpoint security

Using Lookout Mobile Endpoint Security, enterprises can enable Continuous Conditional Access to their corporate data, from any device. This ensures that two things happen: policies are enforced at all times and device health is validated, both before authentication, and continuously during, access to corporate resources.

Enterprises have the opportunity to select, based on their risk tolerance, policies that help ensure devices stay compliant with internal and external mandates. If a device exceeds the acceptable level of risk, as defined by the enterprise, Lookout will send a remediation message to the employee, flag the issue to the admin in the Lookout Mobile Endpoint Security console, and log the employee out of any corporate cloud resources.

Results

The new world is secure, whether managed or unmanaged

The way people work has changed. According to IDC, "Intense demand for mobile and remote worker business solutions will follow in the wake of COVID-19's disruption, as governments, businesses, and individuals rely on mobile devices more than ever to help alleviate the impact that mandated social distancing will have on regular business operations worldwide." (IDC Worldwide Business Use Smartphone Forecast, 2020–2024).

The way data is stored, the way employees move around, the myriad of devices connecting to corporate resources all contribute to a rapidly changing digital transformation that enterprises must embrace to get ahead. Mobile users are now first class citizens in the enterprise, and organizations that want to protect cloud data must implement Zero Trust on mobile to be secure.

Your perimeter has disappeared. Legacy security technologies just don't work anymore. The devices your employees use cannot be trusted, but there is a way to secure corporate resources despite this new fluidity. Lookout Continuous Conditional Access delivers Zero Trust in a mobile and cloud world.

About Lookout

Lookout is the leader in mobile security, protecting the device at the intersection of the personal you and the professional you. Our mission is to secure and empower our digital future in a privacy-focused world where mobile devices are essential to all we do for work and play.

The broad adoption of smartphones and tablets have created new and endless ways for cybercriminals to convince you to willingly use your mobile device for their unlawful gain. The most common start of a cyberattack is a phishing link and mobile devices have enabled new ways to send them to you. Phishing risks no longer simply hide in email, but in messaging, social media, and even dating apps. Because we use these devices for both, protecting against phishing is critical for our personal and professional lives.

Lookout enables consumers and employees to protect their data, and to securely stay connected without violating their privacy and trust. Our platform uses artificial intelligence to analyze data from nearly 200 million devices and over 100 million apps to protect you from the full spectrum of mobile risk. As a result, Lookout delivers modern endpoint security with the most comprehensive protection from device, network, app and phishing threats without prying into your data.

To learn more, visit lookout.com.