Lookout®

WHITEPAPER

# Putting the **trust** in zero trust: Post-perimeter 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: **Post-perimeter security.**

## 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, 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.

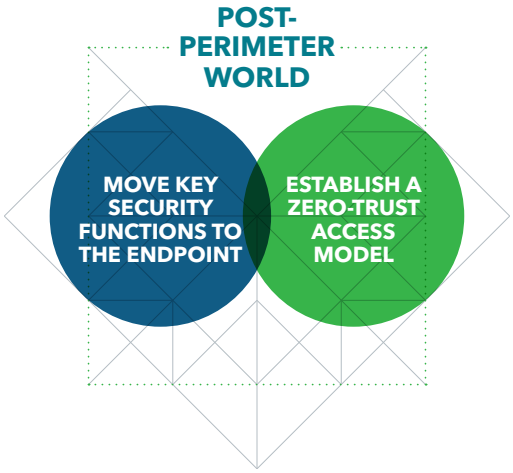
> **"Gartner predicts that 80% of worker tasks will take place on a mobile device by 2020."**
>
> – Gartner, "Prepare for Unified Endpoint Management to Displace MDM and CMT" June 2018

Attacks like phishing have also evolved to take advantage of the fact that perimeter security no longer applies. Corporate devices are personal now, as well. Social media apps, messaging apps, and others create an environment where employees can be phished and corporate credentials stolen through personal activities. Year-to-date in 2018, 50.8% of Lookout users with Safe Browsing turned on encountered a phishing link.

**50.8%** of Lookout users with Safe Browsing turned on encountered a phishing link, year-to-date in 2018

Enabling mobility and the ability to access data seamlessly is a great development 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. With this ecosystem shift, two new security necessities emerge:




### Move key security functions to the endpoint

First, instead of stashing endpoints behind traditional perimeter security, security itself must move to the endpoint. 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.

### Establish a zero trust access model

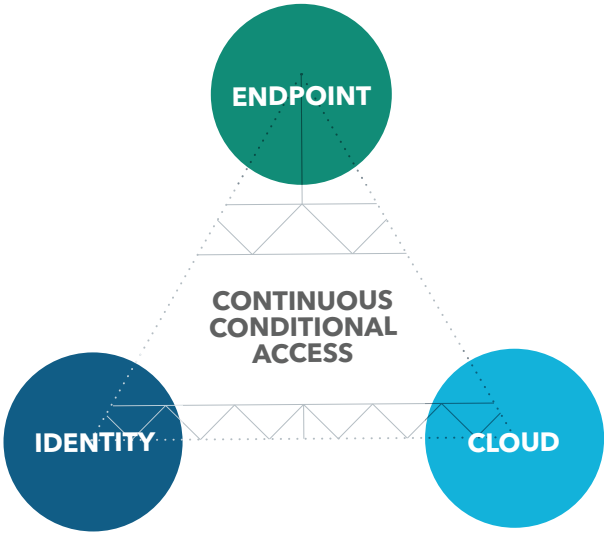
Even with security residing on the endpoint, the enterprise should never assume the device is innocent until proven guilty. This new world demands that all device health must be routinely checked in order to allow access to corporate data.

> "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-perimiterization done by the Jerricho Forum beginning in 2004."

## THE NEW SECURITY ARCHITECTURE: Post-perimeter security

In practice, this necessitates a new security architecture concept we call "post-perimeter security." At its core, post-perimeter security 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 the post-perimeter security architecture. This protection provides continuous visibility into any threats or risks on the device. The solution then decides 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.

Protecting access to the corporate cloud, and the internet as a whole, without relying on perimeter defense is another crucial aspect of this architecture. To make this possible, some of those critical security functions must move to the endpoint. Monitoring for malicious links and websites – and preventing employees from accessing dangerous content – is a primary function that must move.

These two aspects work together with an identity solution, such as an Single Sign-on (SSO) provider, to either allow an employee to authenticate and access corporate resources or be denied even the ability to authenticate. Once authenticated, the endpoint risk is continuously assessed, with access revoked any time a new risk is detected. In certain scenarios, access may be managed via an Enterprise Mobility Management (EMM) (e.g., for managed devices) or Mobile Application Management (MAM) in lieu of identity.

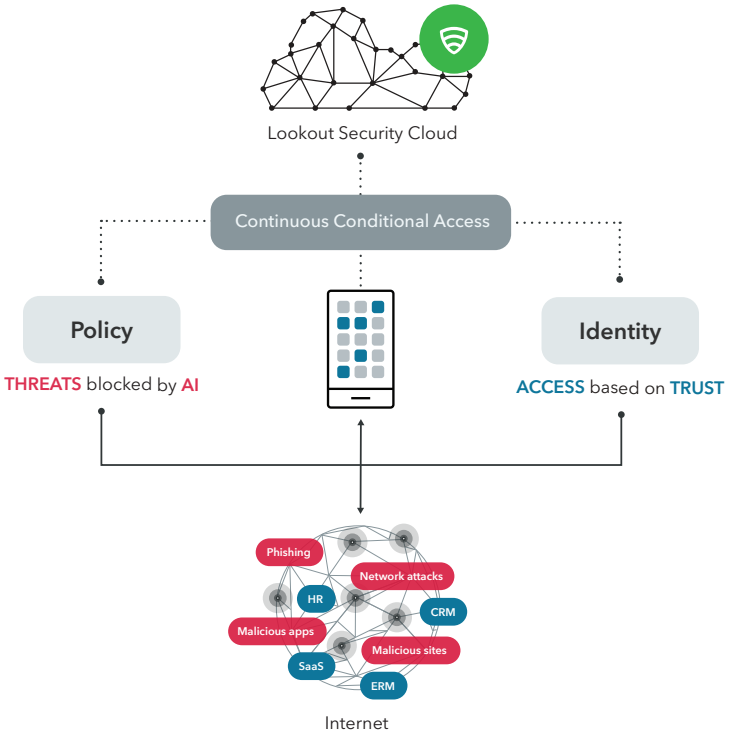
## Continuous Conditional Access

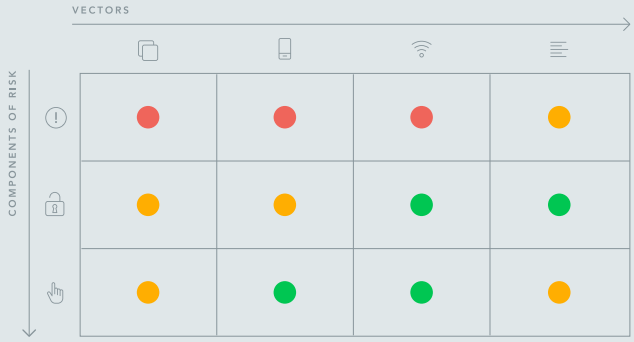
We refer to the continuous assessment of risk and using that assessment to control access to resources as "continuous conditional access." This means that together, the three pillars of post-perimeter security are always watching to ensure that your enterprise risk levels are not crossed. When they are, access is denied, thereby protecting your corporate resources.

# SOLUTION: How Lookout allows you to embrace post-perimeter security

Lookout has specifically designed our platform to give enterprises a tangible way to bring post-perimeter security to their workforce.

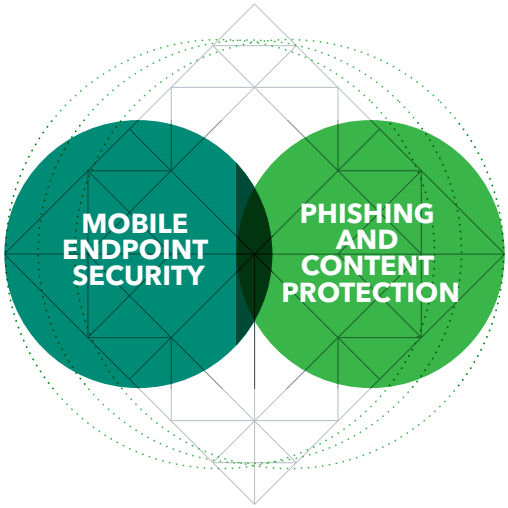
It starts with our dataset of security telemetry from over 170 million devices worldwide and 70 million apps. This gives us an unprecedented depth of insight into the full spectrum of risk, including device, network, app, and content threats and risks. Because of this, we are able to provide enterprises with immediate visibility into potentially harmful scenarios happening on employee devices, at any given point in time.




The Spectrum of Mobile Risk impacts every enterprise. Learn what's on it and how to use the Mobile Risk Matrix to inform your company's risk tolerance.

**GET THE DETAILS**




## 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 resources.

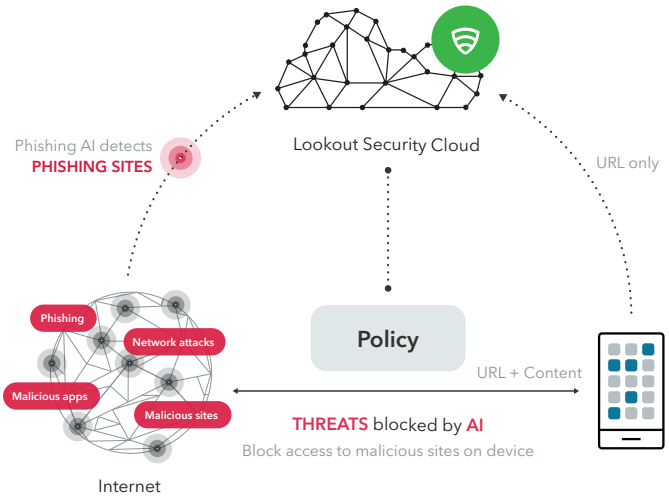
Once the device returns to an acceptable risk level – usually through employee self-remediation – the employee is only then allowed to authenticate to the corporate resources.

As long as the device remains healthy, employees will be able to freely access corporate resources.

## Through Phishing and Content Protection

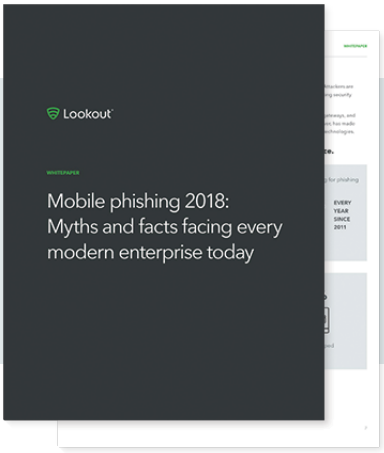
Traditionally, enterprises have relied on email security and gateways in the perimeter to mitigate phishing risk. While email security continues to have a place in the modern security architecture, a problem remains. As employees access data using applications beyond email from devices that do not live behind the perimeter, these technologies are no longer sufficient.

This is one of the main reasons security must move to the endpoint. Lookout Phishing and Content Protection lives on the device, monitoring for phishing attacks across many vectors including social media apps, messaging apps, SMS, and any app that makes a network connection.




The Lookout artificial intelligence detection engine proactively determines the reputation of sites on the internet. With an always-on approach, Lookout Phishing AI detects phishing kits as they are being built, before any user is targeted and an attack is executed. We share select findings with the world here @PhishingAI.

> "Securing mobile endpoints is definitely a priority for us. We see Lookout as a critical layer of protection, both to prevent compromise of our corporate data, and to maintain compliance with all privacy laws."
>
> Christian Jösch, Network administrator, Simon Hegele




Mobile phishing 2018: Myths and facts facing every modern enterprise today

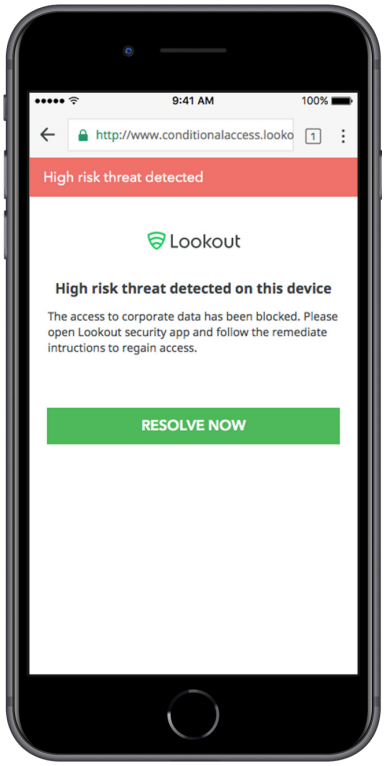
**DOWNLOAD THE REPORT**

## RESULTS:
## The new world is secure, whether managed or unmanaged

The way people work has changed. According to IDC (International Data Corporation), "the percentage of employees considered 'mobile' by large US enterprises is expected to grow to from 35% today to 43% in the next 12-18 months."[1]

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 endpoints" is quickly becoming a name for any device through which employees do work.

The perimeter, as we know is, has disappeared. Legacy security technologies just don't work anymore. The devices themselves cannot be trusted, but there is a way secure corporate resources despite this new fluidity. Post-perimeter security is the necessary and central architecture for a new world of work.




[1] Source: IDC, The State of Mobile Enterprise Devices in 2018: An IDC Survey of Devices, Decisions, and Deployments, forthcoming October 2018