Lookout®

GOVERNMENT SOLUTIONS WHITEPAPER

Putting the **trust** in zero trust: Post-perimeter security for a new age of work

There are three key statements agencies must consider in order to move forward in protecting government 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

Government work has fundamentally changed. Critical data needed for employees to be productive has moved to the cloud, and needs to be accessible from any device, wherever employees are located. Spurred by recent federal legislative and administrative activity, government agencies are launching significant modernizations of their cybersecurity systems, getting offensive with hackers and taking a more strategic approach to risk. Prominent among these are the NIST Cybersecurity Framework and the Modernizing Government Technology (MGT) Act.

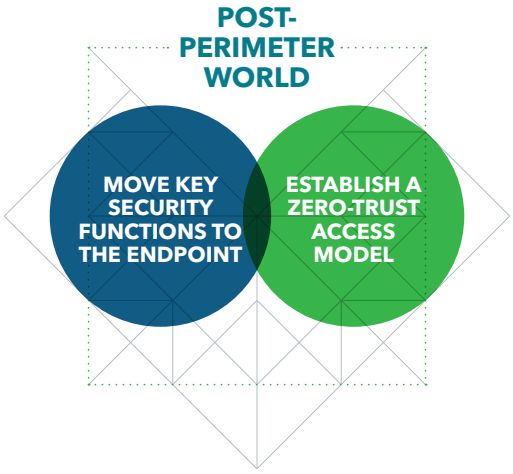
However, none of these necessary initiatives will ultimately be successful without recognizing the fact that the perimeter has failed. Attacks like phishing have also evolved to take advantage of the fact that existing perimeter protections no longer have visibility into user traffic. Work devices are now personal as well. Social media apps, messaging apps, and others create an environment where employees can be phished and agency credentials can be stolen through personal activities. A report published by Lookout early in 2018 laid out the extent to which employee mobile devices and productivity are intertwined:

> **"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

47% report their employees send work documents to unsecured personal email accounts

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

The reality is, there no longer is any "there" anymore when it comes to where government data lives. Data now is 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

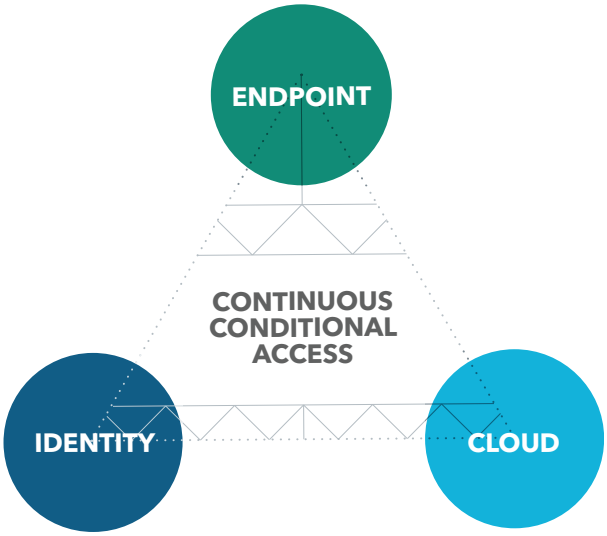
Federal CIO Suzette Kent has stated that zero trust network pilots were well underway, and that these changes go hand in hand with a forthcoming update to the Trusted Internet Connections (TIC) Initiative, TIC 3.0. Simply put, even with security residing on the endpoint the agency should never assume the device is innocent until proven guilty.

> "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 and access management



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 a 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) (e.g., for managed applications).

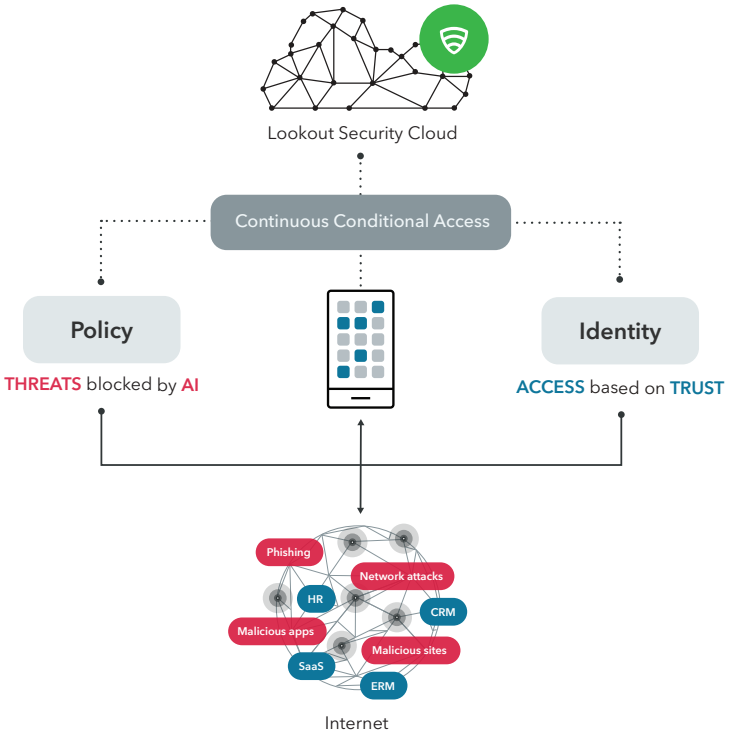
Continuous Conditional Access

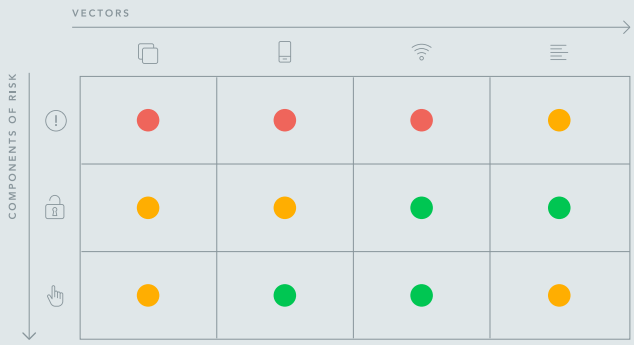
We refer to the continuous assessment of risk and using that assessment to control access to resources as "continuous conditional access." This means that together, the three pillars of post-perimeter security are always watching to ensure that your agency risk levels are not crossed. When they are,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

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

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

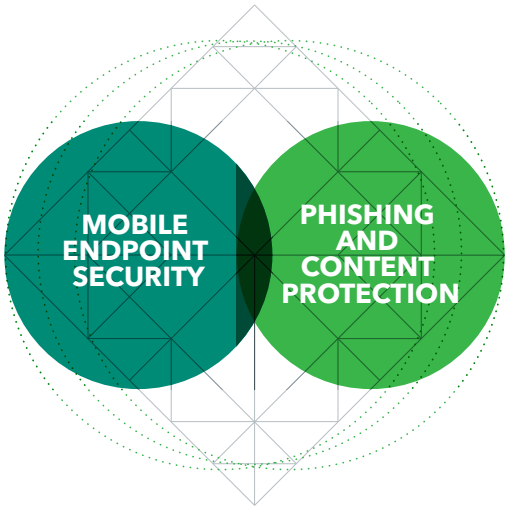
It starts with our dataset of security telemetry from over 170 million devices worldwide and the analysis of over 70 million apps. This gives Lookout an unprecedented depth of insight into the full spectrum of risk, including device, web, app, and content threats and risks. Because of this, we are able 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 agency. Learn what's on it and how to use the Mobile Risk Matrix to inform your agency's risk tolerance.

GET THE DETAILS



Through Mobile Endpoint Security

Current mobile security efforts are falling short. People are bringing their devices into work whether their agency allows them to or not. Agencies are not only facing how their employees use their GFE phones, they're tackling the issue of personal device usage as well. Any effective security solution needs to work with – not against – this fundamental premise.

Using Lookout Mobile Endpoint Security, agencies can deploy continuous conditional access to their employee endpoints. This ensures that two things happen: policies are enforced at all times and device health checks are happening before authentication to agency resources. This is critical, because some of the most flagrant government data breaches happened because once a malicious actor gained access inside the firewall, they were able to move laterally through the network without resistance.

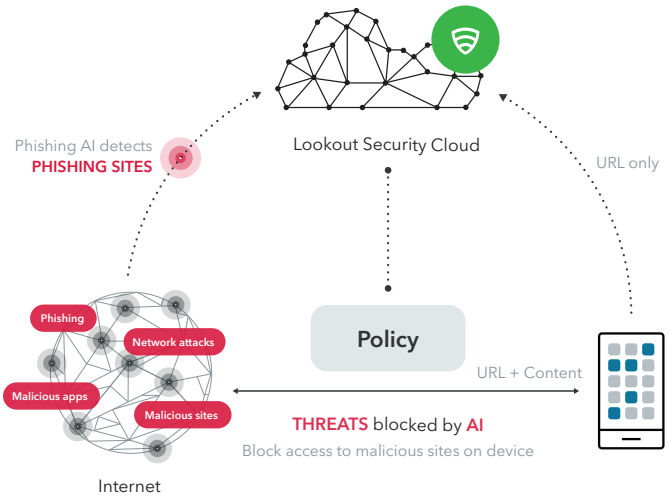
Agencies have the opportunity to select, based on their risk tolerance, policies that help ensure devices stay compliant with internal and external mandates. If a device exceeds the acceptable level of risk, as defined by the agency, Lookout will send a remediation message to the employee, flag the issue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

Once the device returns to an acceptable risk level – which can happen 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 agency resources in the cloud.

Through Phishing and Content Protection

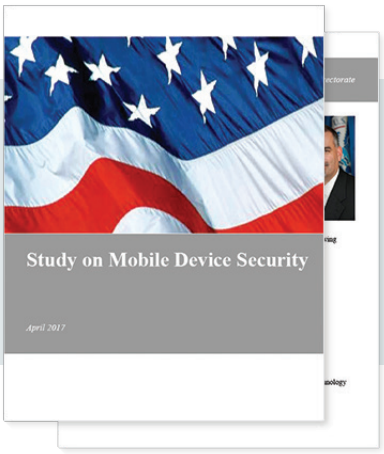
Email is the entry point for 90 percent of successful cyber attacks, and was the start of the massive OMB breach in 2015. Traditionally, attackers have used email as the avenue for attack on desktop, but on mobile you must also take into account social media apps, messaging apps, personal email accounts, and SMS. In August 2018, DHS' Science & Technology Directorate announced that it will make use of Lookout Mobile Endpoint Security to counter such threats.

Security must move to the endpoint itself. Lookout Phishing and Content Protection lives on the device, monitoring for phishing attacks across many vectors including social media apps, messaging apps, SMS, and more.



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 at @PhishingAI.

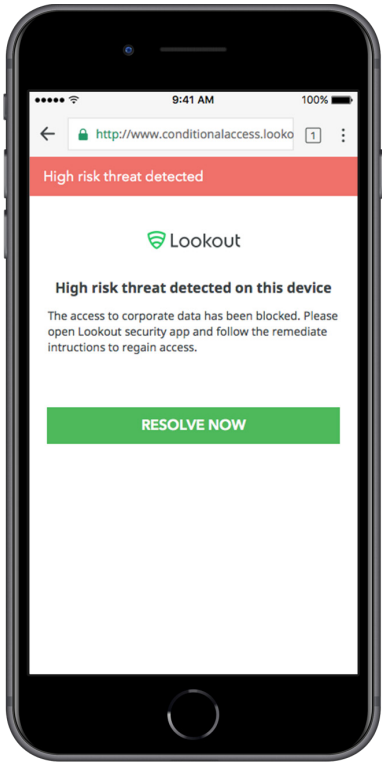
> "The stakes for government users are high. Government mobile devices – despite being a minor share of the overall market – represent an avenue to attack back-end systems containing data on millions of Americans in addition to sensitive information relevant to government functions."
>
> **– DHS Study on Mobile Device Security - April 2017**



DHS Study on Mobile Device Security

DOWNLOAD THE REPORT

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



The way data is stored, the way employees move around, the myriad of devices connecting to agency resources all contribute to a rapidly changing digital transformation that government must embrace to accomplish the mission. "Mobile endpoints" is quickly becoming a name for any device through which employees do work.

Recent survey results from a poll conducted by the Government Business Council, and sponsored by Lookout, bear this out. The poll focused on employee use of mobile devices accessing government databases:

- 45% of respondents accessed work data when connected to external networks – i.e. not the agency network.
- The number was even higher for state and local employees – 75%.
- 47% of respondents have encountered a phishing attack while conducting work via a mobile device.
- Of that 47%, 29% received the phishing attempt via text, and 15% via social media.

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