Lookout®

WHITEPAPER

How to secure your post-perimeter world

WHAT IS THE POST-PERIMETER WORLD?

In an increasingly cloud and mobile-focused world, there are three key realities that 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 are not enough.
3. Devices cannot be trusted.

As employees continue to use a mix of managed and unmanaged devices to access corporate resources, it sets up the need for a new security architecture: **post-perimeter security.**

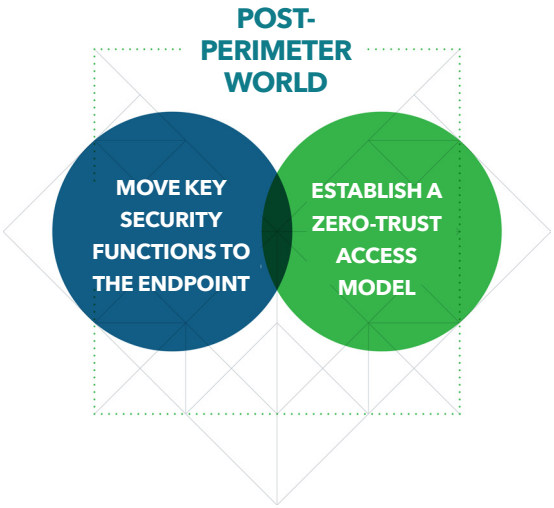
THE PROBLEM:
Your perimeter has disappeared

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.

Attacks like phishing have also evolved to take advantage of the fact that existing perimeter protections no longer have visibility into user traffic. Corporate devices are personal now, as well. Social media and messaging apps create an environment where employees can be phished and corporate credentials stolen through personal activities.

Enabling mobility and the ability to access data seamlessly is a great development for enterprise productivity, but it presents 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 any more. 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, or relying on VPNs to bring traffic into the perimeter, security itself must move to the endpoint. Security needs to be everywhere the data is accessed without impacting end-user privacy.

Establish a zero-trust access model

Even with security provisions on the endpoint, the enterprise should never assume the device is innocent until proven guilty. This new world demands that device health must be continuously checked in order to allow access to corporate data, again, without impacting end-user privacy.

THE NEW SECURITY ARCHITECTURE: Post-perimeter security

In practice, this necessitates a new security architecture concept we call "post-perimeter security".[1] 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. Only then can it be determined 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 defence 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 Enterprise Mobility Management (EMM) (e.g. for managed devices) or Mobile Application Management (MAM) (e.g. for managed applications).

WHY THE WORLD IS MOVING TO POST-PERIMETER SECURITY

Corporate data is increasingly hosted in the cloud, and at the same time is increasingly accessed by endpoints that are connected to networks beyond the control of IT – wide area cellular networks and public WiFi. Corporate data no longer moves between a server and an endpoint on networks managed by IT. Instead, a significant portion of enterprise data doesn't even enter or go through the physical enterprise. Today's enterprise data must move across any network and be accessible on any device.

> **"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

The rise of cloud-based productivity tools

Today many core office productivity applications are consumed through a software as a service (SaaS) delivery model, backed by an identity and access management solution. No longer limited to a single device, the licensing model for SaaS apps are assigned to a user identity. This means that users can access these applications on any device, whether a laptop or mobile device, to best suit their needs, any time, anywhere. The flip side of this, is that organisations can no longer depend on traditional approaches to security to control access and movement of corporate data.

NEED FOR SOPHISTICATED MANAGEMENT AND CONTROL

In the post-perimeter world, employees have greater control over the tools they use for work, and often leverage consumer tools in place of corporate apps and services assigned to them by IT, in the interest of productivity and user experience. The challenge for IT is to provide secure access to corporate data without getting in the way of the user. This is compounded by the rise of bring your own device (BYOD), which in most cases limits the ability of IT to impose control on the device itself. In addition to managing devices and applications where possible (e.g. using a mobile device management or a mobile application management solution, respectively), the focus must now include protecting access to corporate data using identity and SaaS application controls.

Post-perimeter security builds on existing strategies

Granting access to data automatically when a user or endpoint connects to a corporate network no longer works in a mobile and cloud world. This led to the development of the Zero Trust security framework by Forrester Research analyst Jon Kindervag in 2009[2]. The goal of Zero Trust is to treat all endpoints connecting to enterprise data as untrusted, and instead focus on inspecting and logging all traffic to verify that users are doing the right thing.

In 2011, Google created an enterprise security model, BeyondCorp[3]. BeyondCorp began as an internal Google initiative to enable every employee to work from untrusted networks without the use of a VPN. Access requirements are organised into trust tiers representing levels of increasing sensitivity. With BeyondCorp, mobile devices are treated as first-class platforms that must have the same levels of access and ability to perform tasks.

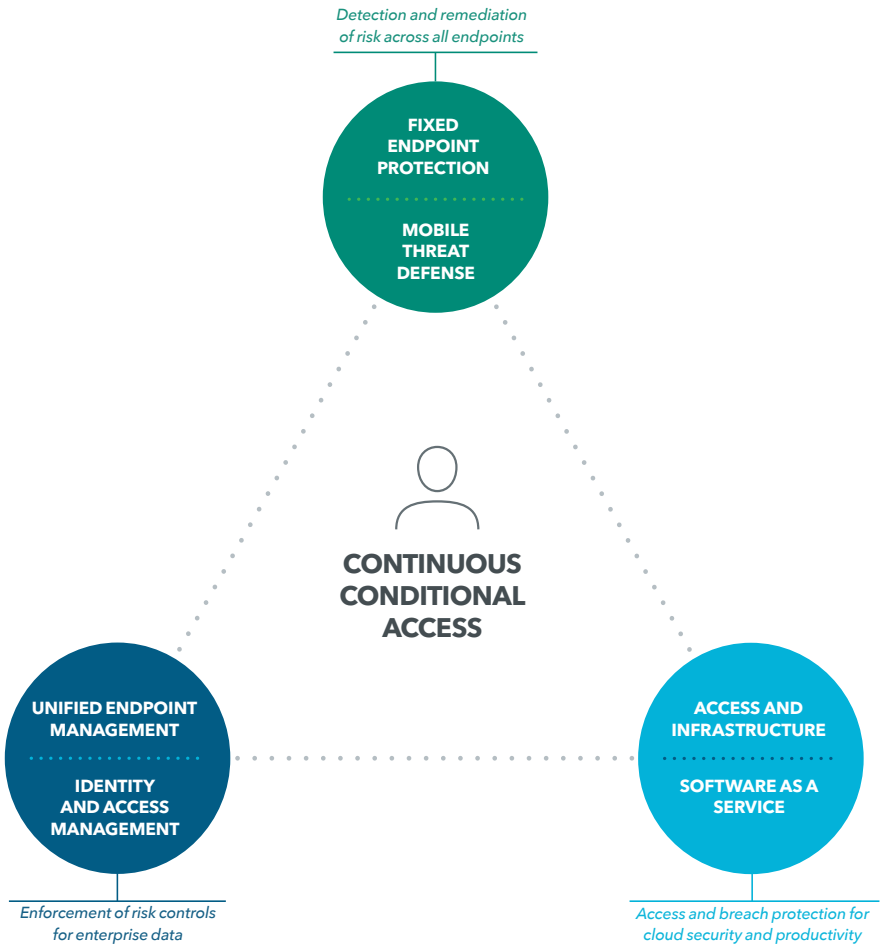
In 2017, Gartner's CARTA (Continuous Adaptive Risk and Trust Assessment) framework expanded on Zero Trust and BeyondCorp. According to Gartner, initial one-time block/allow security assessments (e.g. during login) for access and protection are flawed, leaving the enterprise open to zero-day and targeted attacks, credential theft and insider threats[4]. Key to the CARTA framework is that trust (and risk) of digital business entities and their actions must be dynamic, not static, and assessed continuously as interactions take place and additional context is gained.

Building on these key tenets of modern security in a mobile and cloud-first world, post-perimeter security provides an architecture for enterprises to establish continuous conditional access to corporate resources based on the dynamic risk posed by untrusted endpoints and to add key protections for users, who are often the starting point for most cyber attacks.

HOW TO MAKE POST-PERIMETER SECURITY A REALITY

With apps, devices, and networks outside the reach of perimeter based security controls, adopting Zero Trust, BeyondCorp, and CARTA is now the goal for many IT organisations. For many organisations, making post-perimeter security a reality is about expanding and integrating existing services that are already in place.

What you need to get post-perimeter security



Endpoint protection for all endpoints

The role of endpoint protection is to continuously determine and establish the risk posed by user actions and devices, all of which are untrusted in this new architecture, such protection must span fixed and mobile devices as corporate applications are seamlessly accessed by users across devices. Furthermore, endpoint protection must integrate with access arbiters such as identity and access management solutions and/or the cloud-based applications themselves in order to take remedial action in the presence of unacceptable risk. In certain scenarios, remedial action may be achieved via integrations with controls provided by enterprise mobility management.

Cloud security and productivity

As reliance on cloud services and infrastructure grows, the need to provide secure access to hosted applications and data becomes paramount. Cloud security solutions provide independent access and breach protection for the hosted data and services. In addition, cloud service providers must integrate with identity and access management and endpoint protection in order to incorporate the potential risk associated with access requests. To protect users from malicious sites masquerading as corporate access, adequate provisions must be included in the endpoint itself.

Identity and access management

Identity has been recognised as the "new perimeter" and the foundation for granting access to corporate data. Identity platforms streamline access with capabilities like single sign-on, making it easier for users to work across multiple apps and services. While identity and access management vendors leverage key security capabilities like multi-factor authentication to protect access to cloud and on-premises data, they must integrate with endpoint protection to continuously determine the risk posed by untrusted devices. Combining identity with endpoint protection allows organisations to provide a continuous assessment of trust for both users and the devices.

THE POST-PERIMETER ALLIANCE

The Post-Perimeter Security Alliance includes leading enterprise vendors with a common vision to provide security and productivity for the modern, perimeter-less, cloud-delivered, and privacy-focused world. Today, it is difficult to achieve end-to-end post-perimeter security from a one-stop shop. Instead, with integrated security capabilities across endpoint, cloud, and identity, this alliance delivers productivity enablement and protection for access to corporate data. Together, the solutions offered by the Post-Perimeter Security Alliance provide continuous assessment of risk to corporate data, as well as remediation and controls in the presence of such risks.

Members of the Post-Perimeter Security Alliance include mobile threat detection, endpoint protection, identity and access management, enterprise mobility management and cloud-based productivity vendors. As market leaders in their respective markets, it's likely that an organisation has one or more of these vendors already in their environment. Whether they know it or not, many organisations are well on their way to a post-perimeter security strategy.

Learn more about making post-perimeter security a reality within your organisation here.

> **"A cross-industry effort like the Post-Perimeter Security Alliance makes a lot of sense right now, and can help guide enterprises who want to implement a post-perimeter architecture, but aren't sure how all the pieces fit together."**
>
> – Phil Hochmuth, Program Director, Enterprise Mobility at IDC

[1] Putting the "trust" in zero trust: Post-perimeter security for a new age of work (1 November 2018)
Retrieved from: https://www.lookout.com/info/lookout-post-perimeter-lp

[2] Getting Started with Zero Trust: Never trust, always verify
Retrieved from: https://drive.google.com/file/d/1y_bexOduIUAr8M9wZxTqAGv21T3Vchor/view?ts=5c361c31

[3] Barclay Osborn, Justin McWilliams, Betsy Beyer and Max Saltonstall. (Spring 2016) BeyondCorp, Design to Deployment at Google
Retrieved from: https://storage.googleapis.com/pub-tools-public-publication-data/pdf/44860.pdf

[4] Gartner Seven Imperatives to Adopt a CARTA Strategic Approach (10 April 2018)
Retrieved from [subscription required]: https://www.gartner.com/doc/3871363/seven-imperatives-adopt-carta-strategic