PRISMA
BY PALO ALTO NETWORKS

BeyondCorp
A STEP TOWARD ZERO TRUST FOR THE CLOUD

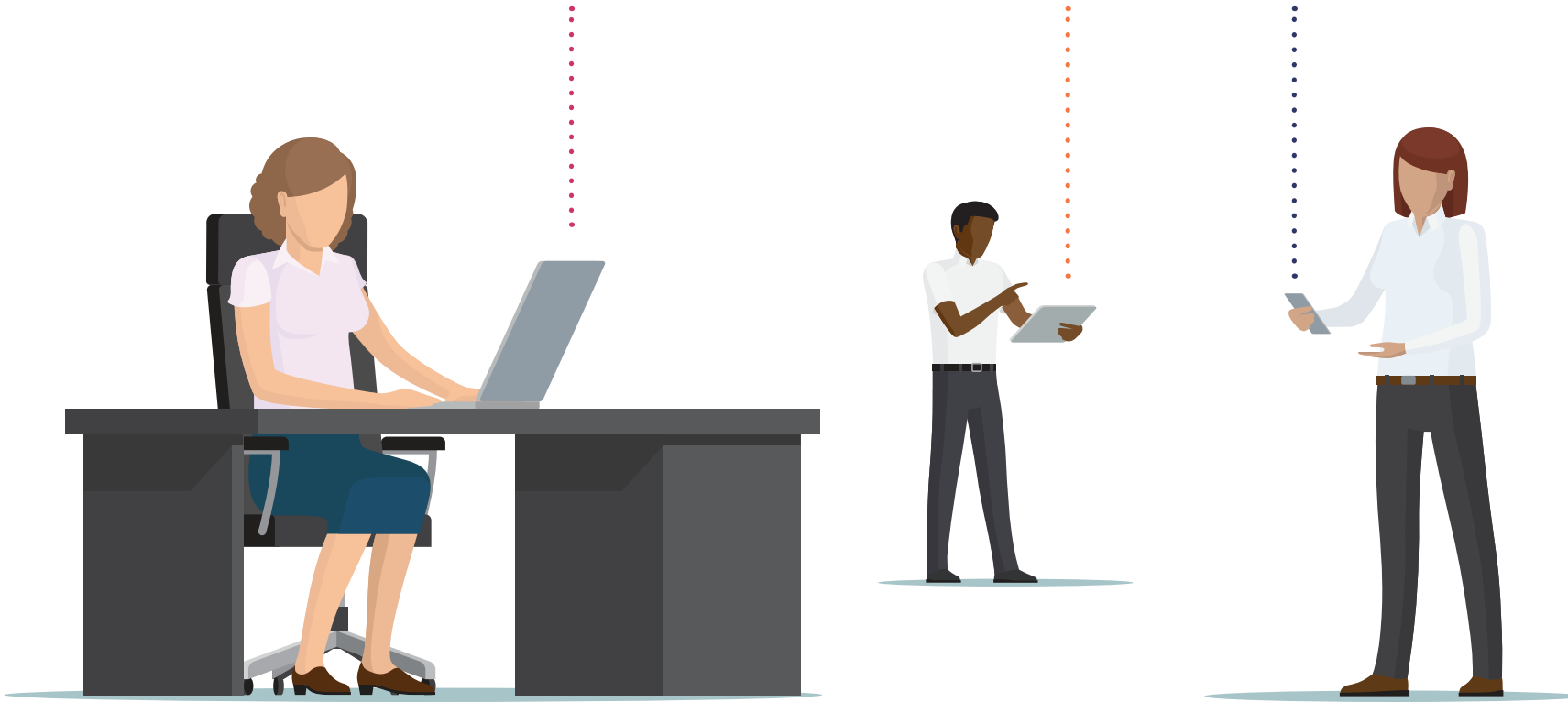


TABLE OF CONTENTS

Introduction

Organizations are increasingly moving toward a Zero Trust approach to security in order to bolster their defenses and reduce data breaches. However, as apps and infrastructure move to the cloud, there are questions about how to implement the Zero Trust concept for cloud applications and data. Google researchers have developed an approach called BeyondCorp, which helps organizations apply Zero Trust concepts in the cloud. This e-book looks at BeyondCorp, its key principles, and how it applies to implementing a comprehensive Zero Trust approach in the cloud.

What Is BeyondCorp?

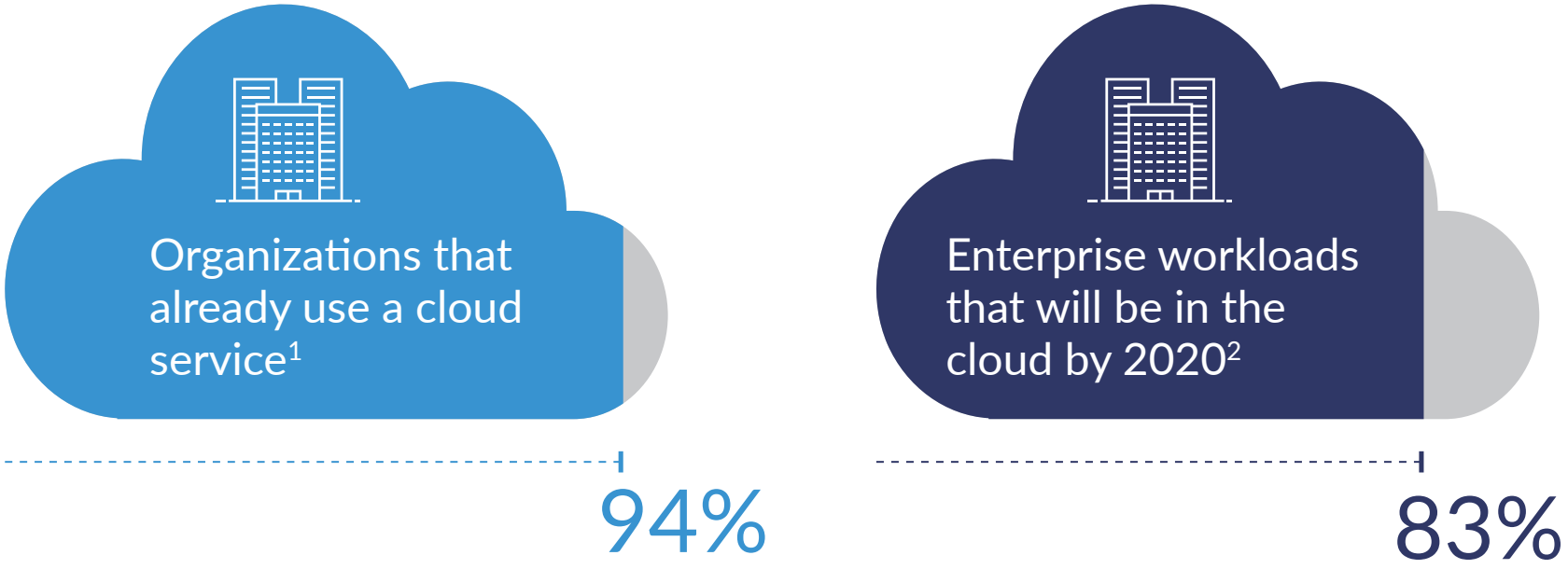
BeyondCorp is an implementation of the Zero Trust concept that shifts access controls from the network perimeter to individual devices and their users, enabling them to work securely anytime, anywhere, and on any device without the need for a VPN. It applies context-aware access that is intended to better secure organizations.

At a baseline, organizations should:

- Define and apply access policies that specify which resources require high levels of trust and which do not.
- Understand the context of user and their requests, such as identity, location, and device information.
- Classify applications and data as sensitive or not to protect them, regardless of whether they are in the cloud, on-premises, or in the data center.

Why BeyondCorp Matters

There was a time when organizations housed their applications and data on-site in a single data center. During that time, they operated on the idea that everything inside their company network could be trusted and that anything outside the walls needed to be verified. As new cloud technologies and mobile devices have been developed, companies have moved more and more of their applications and data to third-party cloud service providers, outside the trusted part of the network.



However, with the move to the cloud, companies have realized they have limited insight into who is accessing and using their applications, and how their data is being used and shared. The traditional perimeter-based security model is no longer effective, requiring a rethink of how to consistently enforce security policies across on-premises data centers, multiple cloud service providers, SaaS, and other environments.

1. RightScale 2019 State of the Cloud Report, Flexera, February 27, 2019.
2. Louis Columbus, "83% Of Enterprise Workloads Will Be In The Cloud By 2020," Forbes, January 7, 2018.

Key Principles of BeyondCorp

A BeyondCorp approach to security is built on three key principles to keep organizations, their users, and data safe.[3] They are:

1. Connecting from a particular network must not determine which services you can access.

In other words, it doesn't matter if the network is trusted or not; access is based on the enforcement of policy rather than the location of the user.

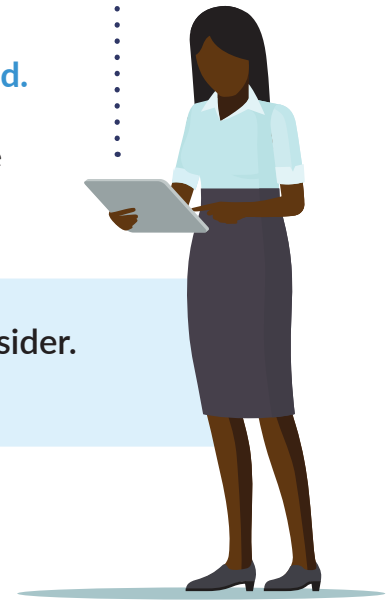
> "The only way to guarantee that every request is legitimate is to look at each request."[4]
>
> Source: BeyondCorp Beyond Google (Cloud Next '18).

2. Access to services is granted based on what we know about you and your device.

Employees with managed devices get immediate, full access to their applications—regardless of whether they're in the data center, cloud, or SaaS—while contractors on non-compliant devices receive different levels of access without bringing the device on network, thus maintaining a least-privileged architecture without disrupting business.

3. All access to services must be authenticated, authorized, and encrypted.

Implement a scalable way to apply rules based on context (e.g., user identity, device, location) of requests to applications, which are classified and secured according to the sensitivity of the data they contain.



If you are thinking about BeyondCorp as part of your security strategy, however, there is more to consider. Let's look at how BeyondCorp relates to Zero Trust.

3. "BeyondCorp: A new approach to enterprise security," Google Cloud, last accessed October 4, 2019.
4. "BeyondCorp Beyond Google," YouTube video, 40:56, posted by Google Cloud Platform, July 25, 2019.

How BeyondCorp Relates to Zero Trust

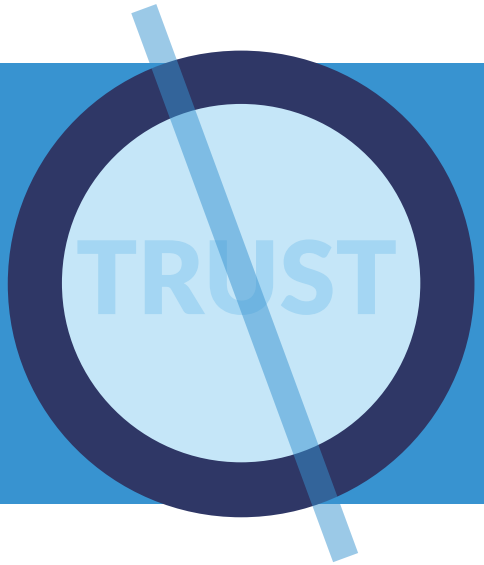
Zero Trust is a security model introduced by Forrester Research that addresses the shortcomings of perimeter-centric strategies by removing the assumption of trust from the equation.

The basic definition of Zero Trust, as defined by Forrester,[5] is:

Ensure all resources are accessed securely regardless of location.

Adopt a least-privileged strategy and strictly enforce access control.

Inspect and log all traffic.



Built on the idea of "never trust, always verify," Zero Trust establishes a demarcation between applications and users for the enforcement of policy, regardless of which devices they use or where they are located. That means everyone—whether inside or outside of the company—is required to go through a formal identity and authorization process before being granted access to the network. Zero Trust is a philosophical shift in protection, meaning that no access at all is permitted without identification.

BeyondCorp does establish a demarcation between apps and users for enforcement of policy, which is part of the foundation of Zero Trust. As organizations think about other security requirements, they may want to think about inspection and logging to control in-line traffic.

5. "No More Chewy Centers: The Zero Trust Model of Information Security," Forrester Research, March 23, 2016.

Expanding Zero Trust in a BeyondCorp Model

To expand Zero Trust in a BeyondCorp model and effectively protect the organization, companies must:

- Separate users and applications in the cloud.
- Identify users and devices as well as enforce policy between users and applications.
- Enforce a Zero Trust policy that inspects traffic based on users, applications, or data.
- Enforce threat prevention and data loss prevention.
- Constantly inspect and log all traffic to proactively stop threat

"In a Zero Trust world, there are no trusted devices, systems or people. This doesn't mean that people are fundamentally untrustworthy; it means that they generate data packets which appear to be coming from them—and sometimes it isn't them. Once every packet has the same trust level, zero, you begin to address the problem."

– John Kindervag, Field CTO, Palo Alto Networks

Source: SecurityRoundtable.org interview.

Building on BeyondCorp

As we've seen, context-aware access is a key tenet of BeyondCorp, but visibility is equally important. To achieve that, once access is established, there should be continuous inspection of the traffic both to ensure that users adhere to application policies which govern the movement of data and to verify that data is not being exfiltrated, used, or shared improperly. Without inspection, it would be alarmingly simple for an attacker to compromise a valid user's endpoint and take control of data available to a rightful user.

That's why identity is only part of Zero Trust. The traffic that the asserted identity generates must be inspected for malicious content and unauthorized activity and logged through Layer 7. Start with reducing the attack surface (the sensitive data you want to protect) and extend across the network to the applications, systems, and users, both on-premises and in the cloud.

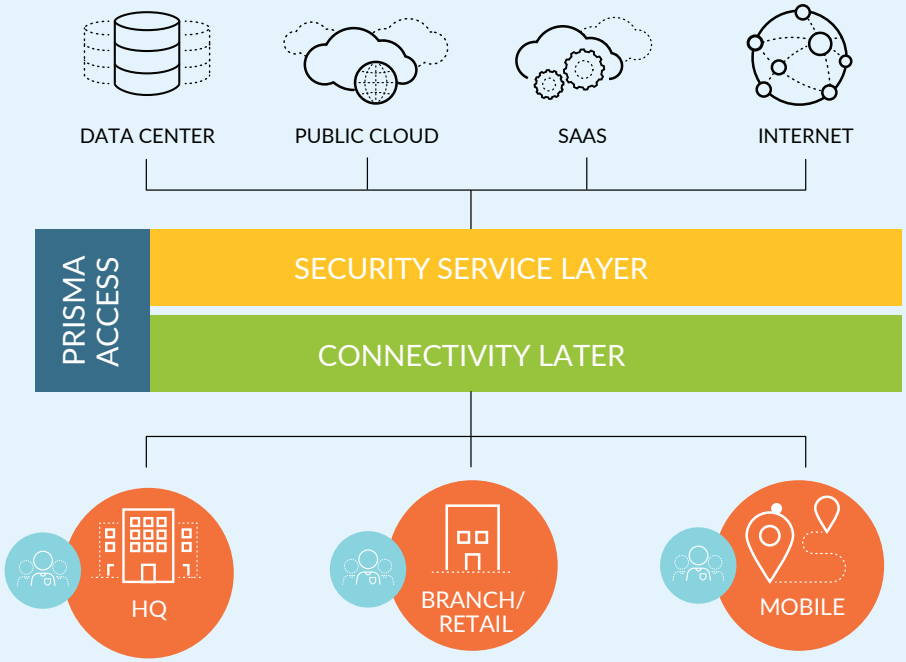
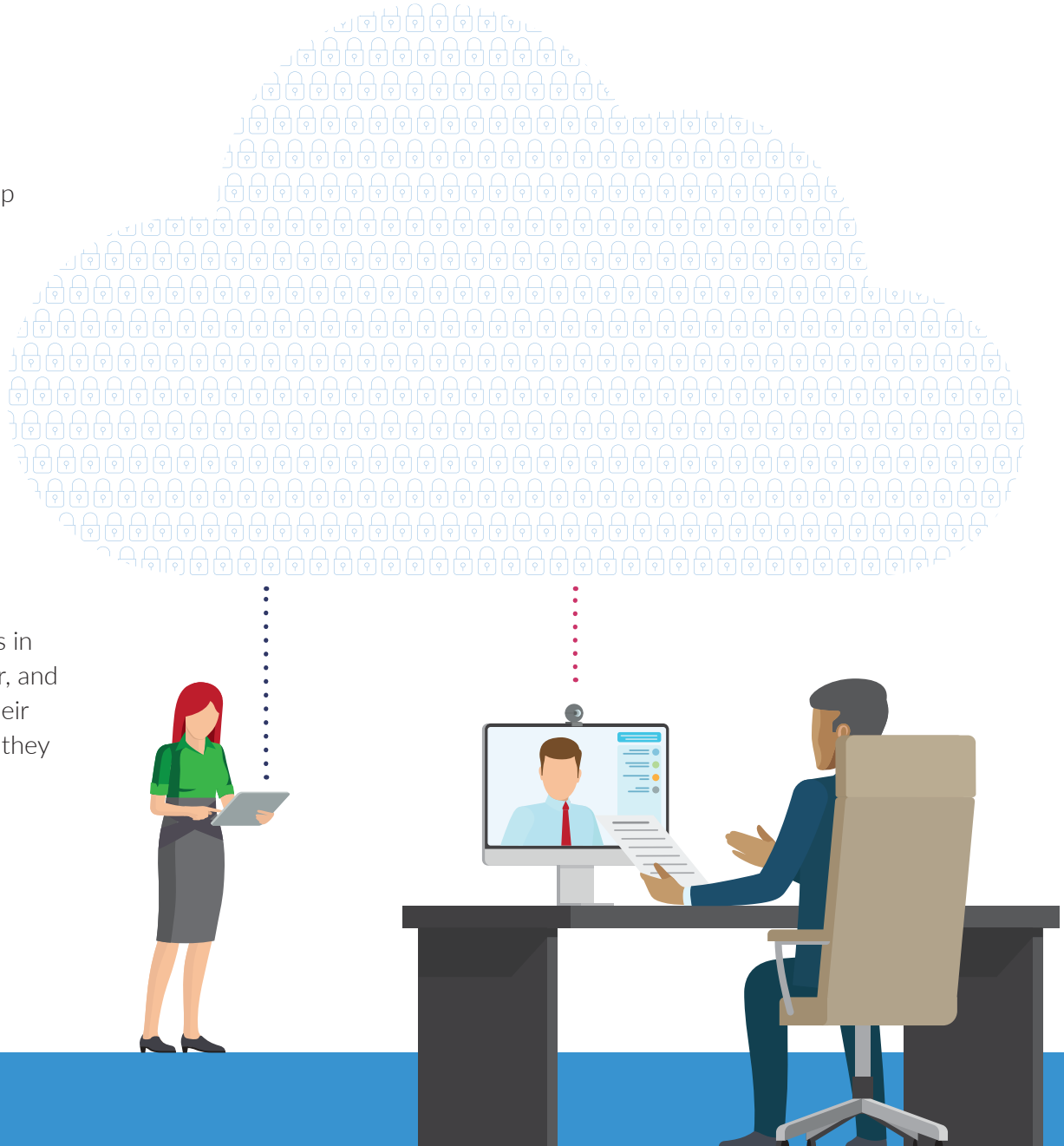


FIGURE 1
Architecture that separates users and applications, applies security policies, and prevents threats

How Palo Alto Networks Can Help

Palo Alto Networks partners with Google to develop integrations that make the implementation of secure cloud applications easier. With respect to BeyondCorp, our mutual customers will benefit from this integration to address implementation challenges with identifying users, maintaining consistent policy, protecting data, and enforcing threat prevention across a diverse landscape of users, workloads, and devices.

Prisma™ Access by Palo Alto Networks is cloud-based security infrastructure that helps you gain control and visibility over the users and applications in the public cloud, SaaS, internet, internal data center, and other locations. Organizations can begin to build their cloud security infrastructure with Prisma Access as they set out on their cloud transformation.



Conclusion

BeyondCorp is a first step in building an effective cybersecurity architecture. As you deploy BeyondCorp, plan to incorporate Zero Trust principles to achieve a complete cloud security strategy for your organization.

Next Steps

Learn how you can apply Zero Trust principles to your cloud environments in our white paper.

Additional Resources

Blog Post: https://blog.paloaltonetworks.com/beyondcorp/