ZIMPERIUM®
ADVANCED MOBILE SECURITY

Zimperium zIPS with Ping Identity

Enhanced Zero Trust Controls on Mobile Endpoints

The established perimeters around corporate devices have faded away, replaced by a mobile distributed workforce with global access into enterprise assets. Increased connectivity and data availability enable organizations to grow and evolve beyond a physical location's confines while minimizing the friction an employee would typically experience in this new, spread-out workspace.

With an ever-increasingly mobile workforce, enterprises changed their approach to mobile data access, endpoint security, and how it all integrates into existing architecture. To support the changing work environment and enable mobile productivity and authentication, organizations must have device attestation and understand their mobile risk posture. If left unchecked, the 'always verify, never trust' model of Zero Trust falls apart.

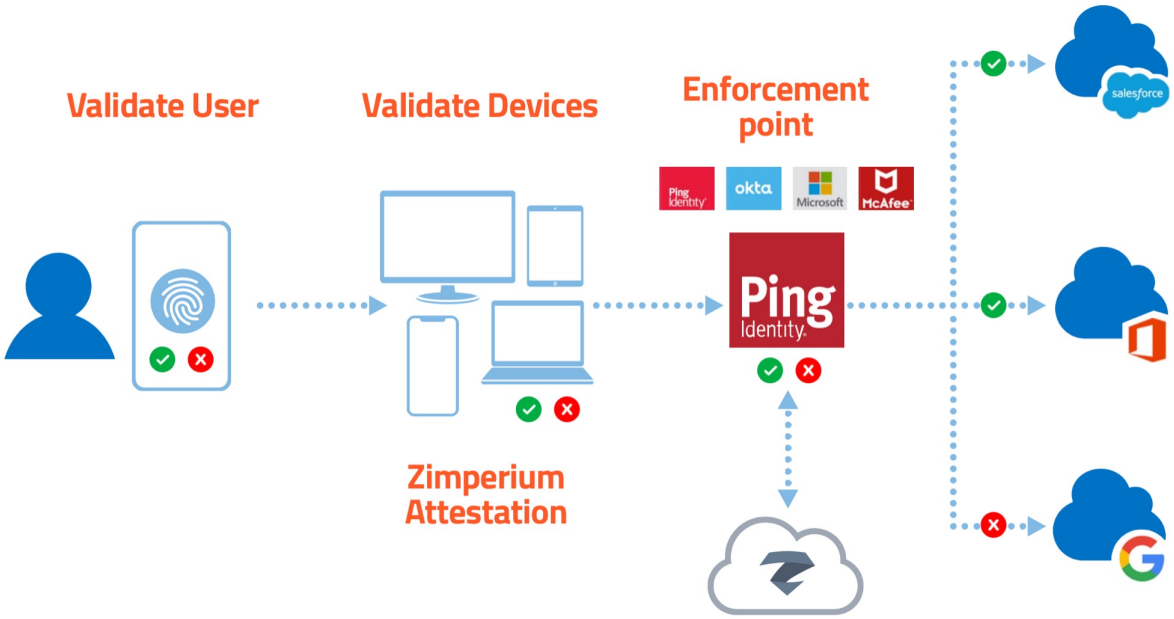
For enterprises to securely enable employees to access the data they need on the devices they use the most, **Zero Trust must be enabled with advanced mobile threat defense.**

Zimperium zIPS with Ping Identity: Complete Mobile Zero Touch Capabilities

As organizations scale to include mobile endpoints into their corporate ecosystem with both corporate-owned and bring your own device (BYOD) policies, they must also increase the existing security infrastructure. These devices have the same level of access and rights as traditional endpoints but are used more. But security for mobile endpoints is often sacrificed for convenience. And these mobile endpoints are exposed to increased attack vectors that organizations have no visibility into, much less the ability to prevent, leaving gaps in the enterprise Zero Trust architecture.

In order to securely enable employees to access the data they need on the devices they use the most, Zero Trust is critical, and mobile threat defense is a core component for that enablement.

With Zimperium zIPS and Ping Identity, enterprises are able to enhance existing mobile endpoint identity management and access controls, bringing all their mobile endpoints into the security perimeter. The two advanced security technologies provide security operations teams the visibility, access control, and device security they need to secure both corporate-owned and BYOD endpoints. And with a cohesive Zero Trust architecture with mobile devices, enterprises can raise their mobile security confidence on managed and unmanaged mobile devices.



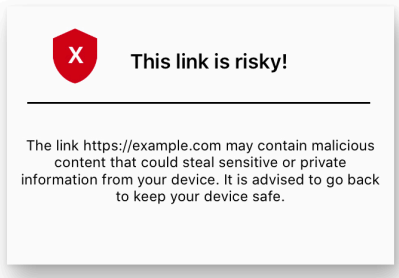
This integration between Zimperium and Ping Identity enables enterprises to evolve and scale without sacrificing their security posture. By enhancing existing mobile endpoint identity management and access tools, security operations teams can understand their whole risk posture and raise their mobile security confidence on managed and unmanaged mobile devices.

Real-time Conditional Access Across All Mobile Devices and Accounts Across a Broad Range of Apps and Services

Zimperium zIPS with Ping Identity provides granular controls and capabilities, enabling security and IT administrators to secure enterprise applications against mobile risks. Based on the customizable policies, if a mobile device is found to have an non-compliant application, from sideloaded to unapproved, admins can prevent access to critical enterprise applications and services until the risk is mitigated. Administrators have the granular control to determine if an account needs to be locked on the device directly or across the complete enterprise.

Direct User Feedback on Detected Risks Within the Protected App

Zimperium zIPS provides clear, full screen alert messaging to the end user when a mobile risk is detected. This message can be modified and adjusted by the administrator, allowing them to tailor the look and feel of the alert to best suit their security needs and policies. The end user is provided with the recommendations or guidance they need to mitigate the mobile risk, from the violated mobile policy, the application causing the alert, and the actions Zimperium zIPS with Ping Identity has taken to protect the mobile endpoint.



Defined Access Policies Best Suited for the Environment

Zimperium and Ping Identity understand that not every environment is created equal and granular control is necessary to enable IT and security administrators to protect their mobile endpoints. With the integration of both products, administrators are able create a policy contract for the authentication policy. Administrators can also alternatively use a Local Identity Mapping or Data Store depending on their needs.

> *"Identity is the new perimeter that enterprises need to secure, and the best way to effectively do that is to leverage a zero trust approach that unifies mobile threat defense with strong authentication. Our integration with Zimperium will make zero trust implementation easy for security teams to deliver a more seamless and secure user experience."*
>
> – Loren Russon, Vice President of Product Management, Ping Identity

Zimperium zIPS with Ping Identity in Action

If you are interested in learning more about the ways Zimperium with Ping Identity can help you enhance your mobile Zero Trust architecture, please contact us.

About Ping Identity

The Ping Intelligent Identity™ platform provides a comprehensive suite of identity services that work in any cloud, hybrid and on-premise environment. From multi-factor authentication and single sign-on to data governance and intelligent API cybersecurity, our platform helps you optimize both security and convenience simultaneously. We'll help you build a centralized control point for security so your customers, employees and partners have secure access to resources from anywhere.

About Zimperium

Zimperium, the global leader in mobile security, offers the only real-time, on-device, machine learning-based protection against Android, iOS and Chromebooks threats. Powered by z9, Zimperium provides protection against device, network, phishing and malicious app attacks. For more information, visit www.zimperium.com