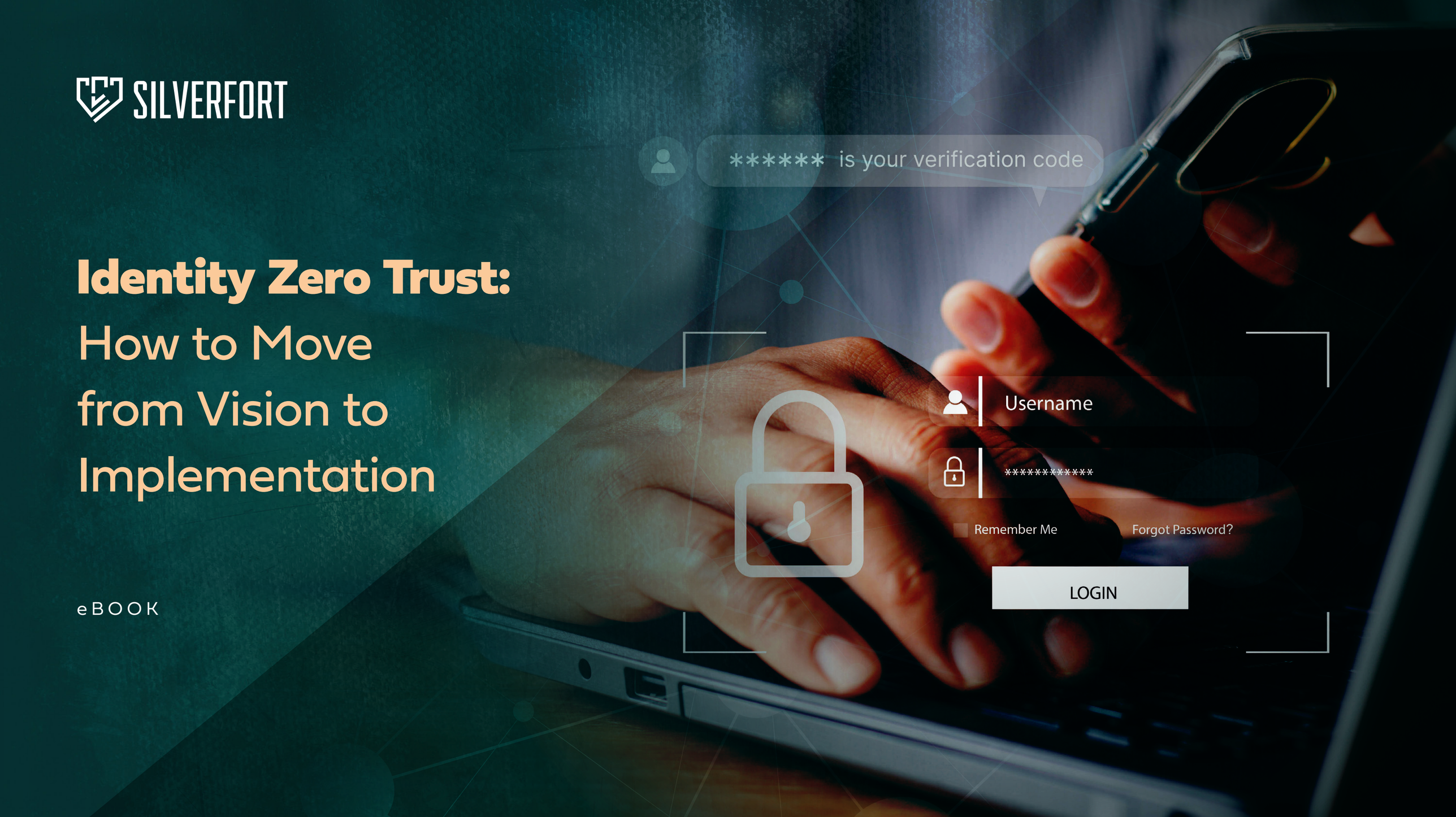
SILVERFORT

Identity Zero Trust: How to Move from Vision to Implementation



eBOOK

Foreword

Zero Trust is often viewed as a project focused on network infrastructure. But the dissolution of the traditional perimeter has led to a surge in users accessing resources outside the corporate network. As a result, organizations today need to implement Zero Trust across the entire identity control plane. This means eliminating any implicit trust in user access – even when correct username and password are provided – as well as analyzing all incoming requests to determine if they can be trusted.

In this eBook, you'll learn about a framework for approaching Identity Zero Trust, including a strategy to help you benchmark your environment and develop capabilities around monitoring, analyzing, and acting on every access attempt. You will then learn how Silverfort can help organizations take a "never trust, always verify" approach to every authentication.

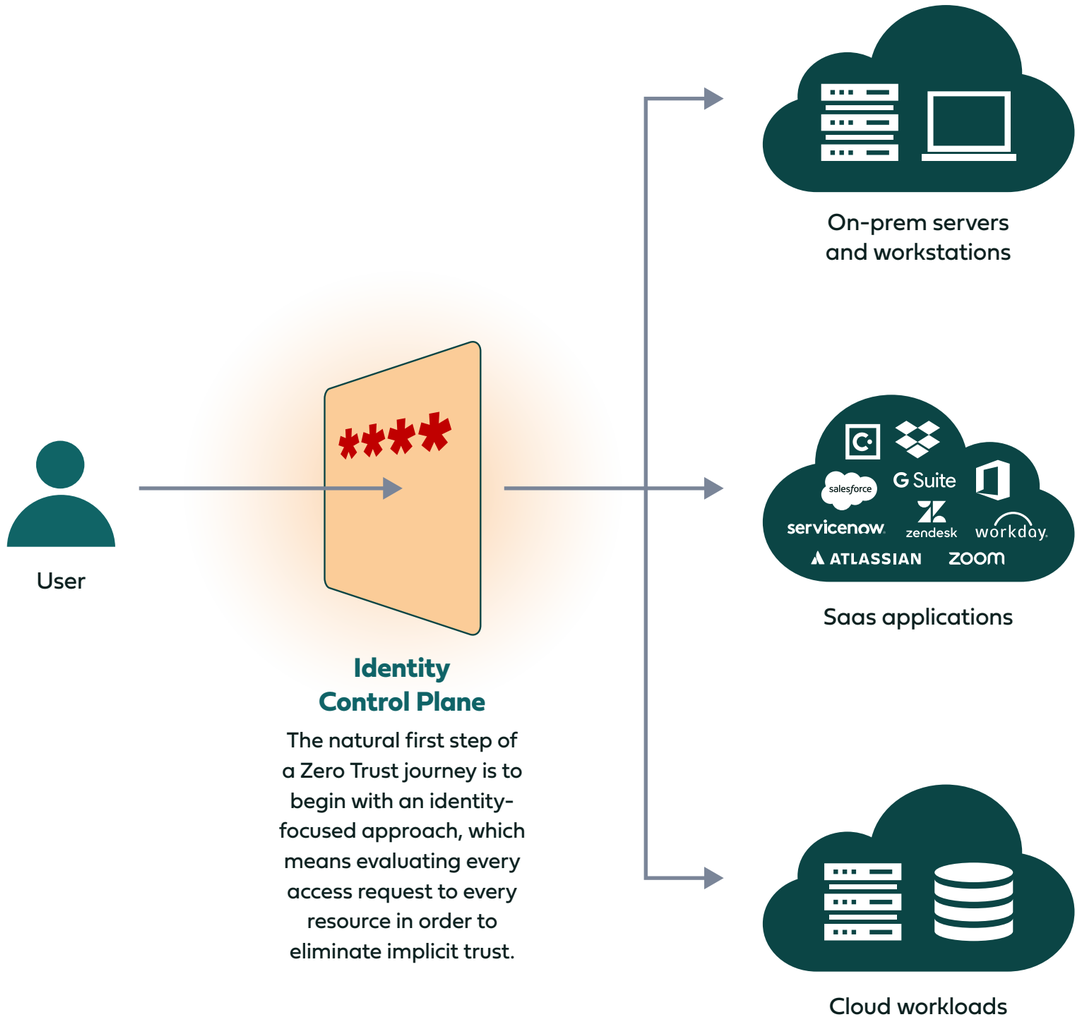
Identity is Where Zero Trust Needs to Begin

Why Start with Identity

Because accessing resources is based on user authentication, the natural place to start is with the identity control plane. This has become an especially urgent concern due to an ever-growing rise in identity-based attacks, where threat actors use stolen credentials to gain access to a company's resources to exfiltrate data and spread ransomware.

The Challenge of Identity Zero Trust

The problem with an identity-focused approach is determining where to begin. For example, how do the products in your current security stack contribute? Should implementing a PAM solution be the top priority or would it be better to instead focus efforts on expanding MFA protection? In the following pages, we lay out **four implementation pillars** to act as guidelines for breaking down Identity Zero Trust into a a set of concrete, actionable steps to help you move forward on the journey.



Pillar 1 – Unification

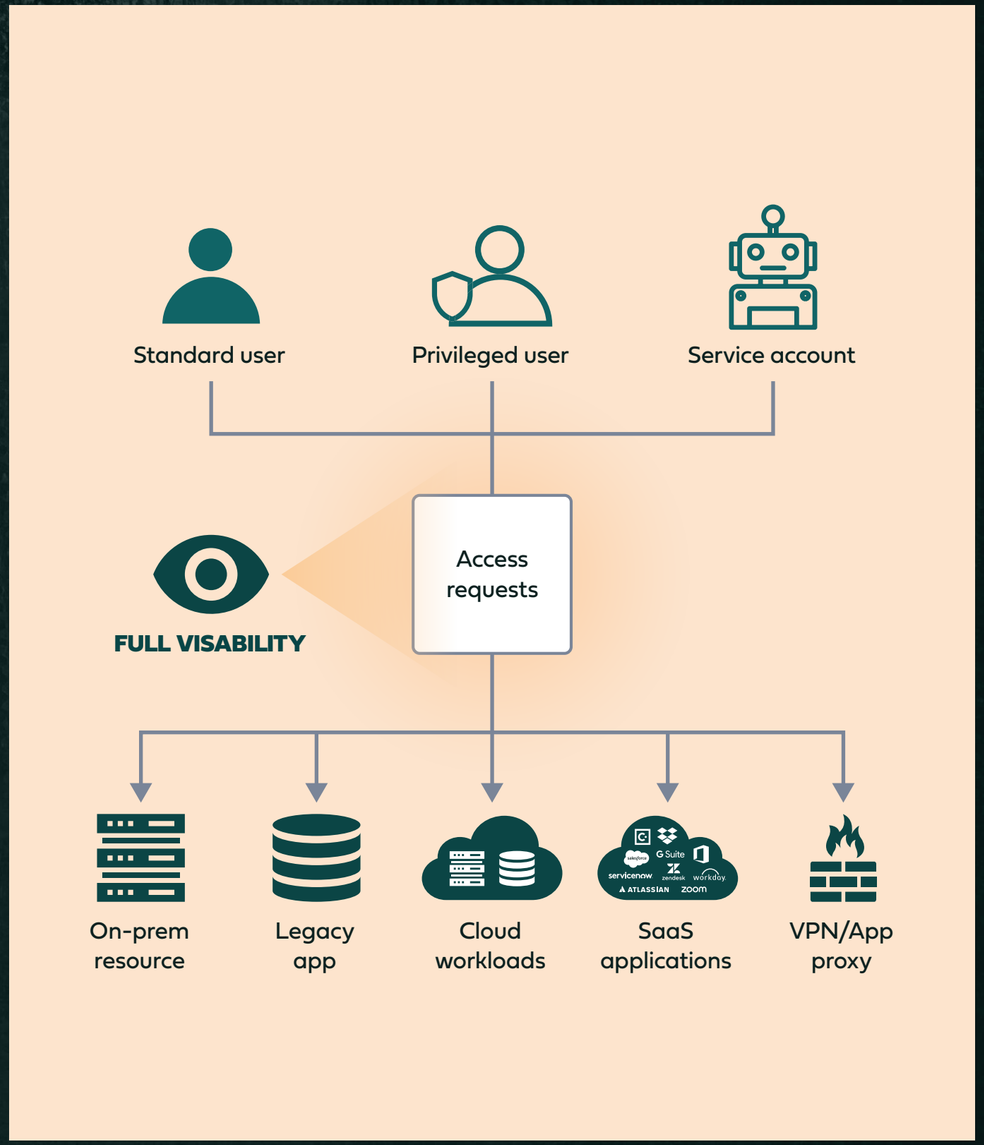
The Need for Centralized Visibility into All Access Requests

HOW TO DEFINE UNIFICATION

Unification means the ability to have real-time visibility into every authentication and access attempt across all resources (whether on-prem or cloud-based) by all users (both human and machine) through any access interface and using any authentication protocol.

THE CHALLENGE OF UNIFICATION

Because most organizations today operate with a hybrid environment, there are multiple places where identity is managed and secured. This means different identity providers for cloud vs. on-prem resources as well as other products that manage identities, such as PAM solutions and VPN connections. As a result, user activity (including standard users, privileged users, third-party users, and service accounts) is distributed among various silos with no easy way to gather all data for a holistic view.



Pillar 2 – Context

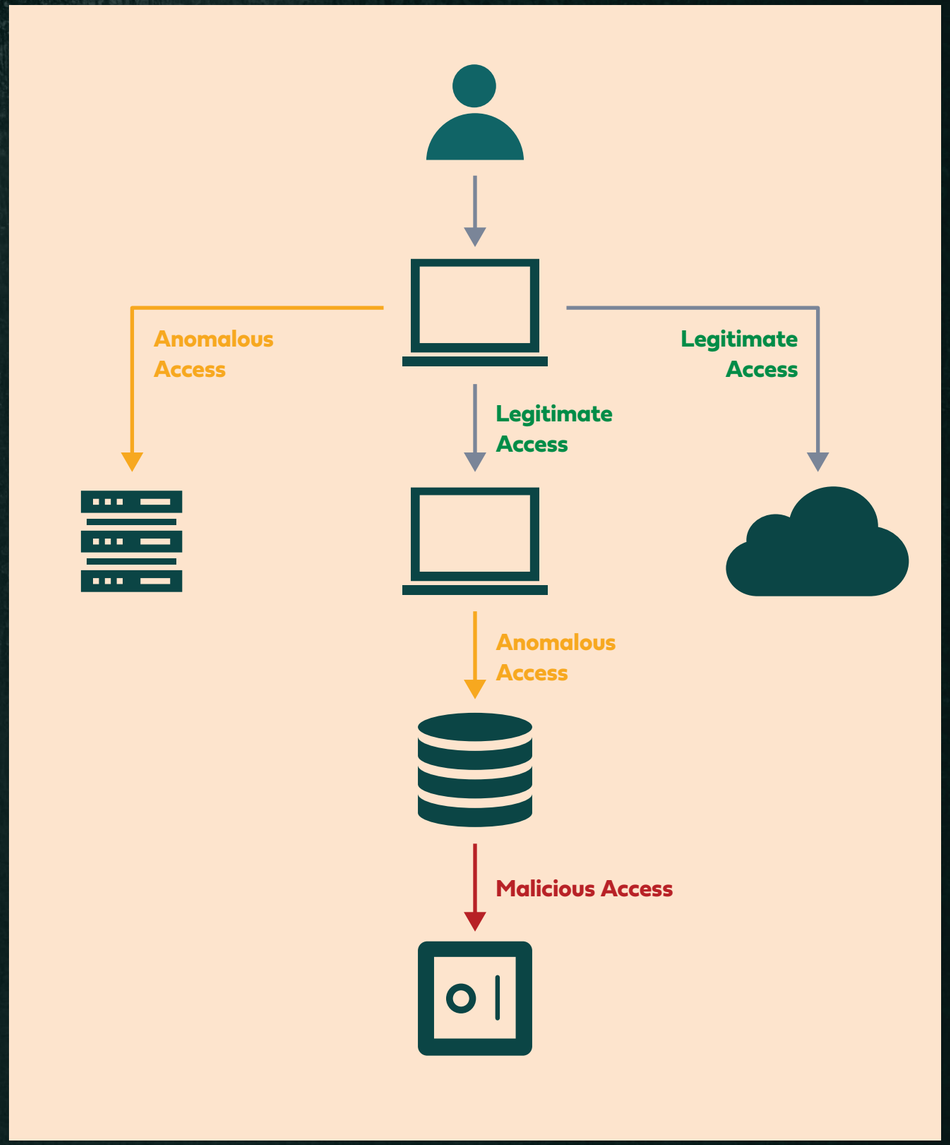
The Ability to Determine Whether Each Access Attempt is Legitimate

HOW TO DEFINE CONTEXT

Context is about continuously assessing risk levels, based on identity, to determine whether the access request was initiated by the actual user or is in fact coming from an adversary using compromised credentials. This is done by analyzing each request to reveal any anomalies that would separate it from a legitimate authentication. Anomalies could be either part of the authentication process itself (as in Pass-the-Hash or Pass-the-Ticket attack) or as a deviation from the user's normal behavior.

THE CHALLENGE OF CONTEXT

The fragmented nature of today's hybrid environment means gathering and processing all data associated with authentication and access requests is a major obstacle, especially due to the difficulty in normalizing the scores being generated by different risk engines. There are few security solutions capable of analyzing the actual authentication packets in order to flag when a malicious modification has taken place. Organizations don't have a complete view of a user's behavior when a request is made and can't accurately assess the risk of granting access.



Pillar 3 – Enforcement

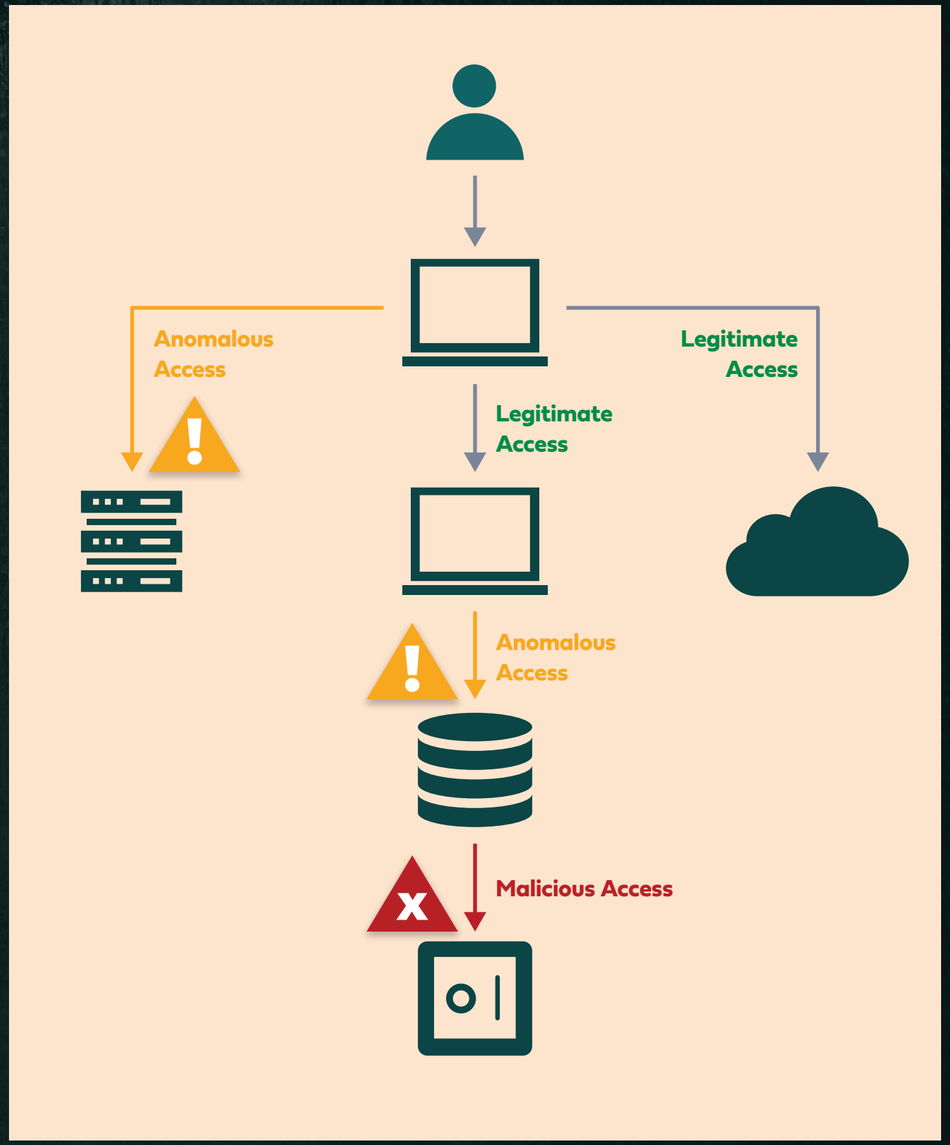
The Ability to Block Malicious Requests in Real Time

HOW TO DEFINE ENFORCEMENT

Enforcement means the ability to actively block an access request when it cannot be trusted. Specifically, this should involve triggering secure access controls via a configured policy across every type of user, access interface, or resource in real time.

THE CHALLENGE OF ENFORCEMENT

Active Directory's main authentication protocols (Kerberos and NTLM) don't support the most effective identity protection control: multifactor authentication (MFA). As a result, there is no way to enforce real-time protection on AD-managed resources — including legacy applications, command-line access tools (such as PsExec and PowerShell), file shares, databases, and others. Many existing security products are focused on detection rather than response (including EDR, CASB, and network traffic analysis tools), making them irrelevant to the core task of determining whether to trust each incoming access request or not. This means organizations don't have a complete view of a user's behavior when a request is made and can't accurately assess the risk of granting access.



Pillar 4 – Granularity

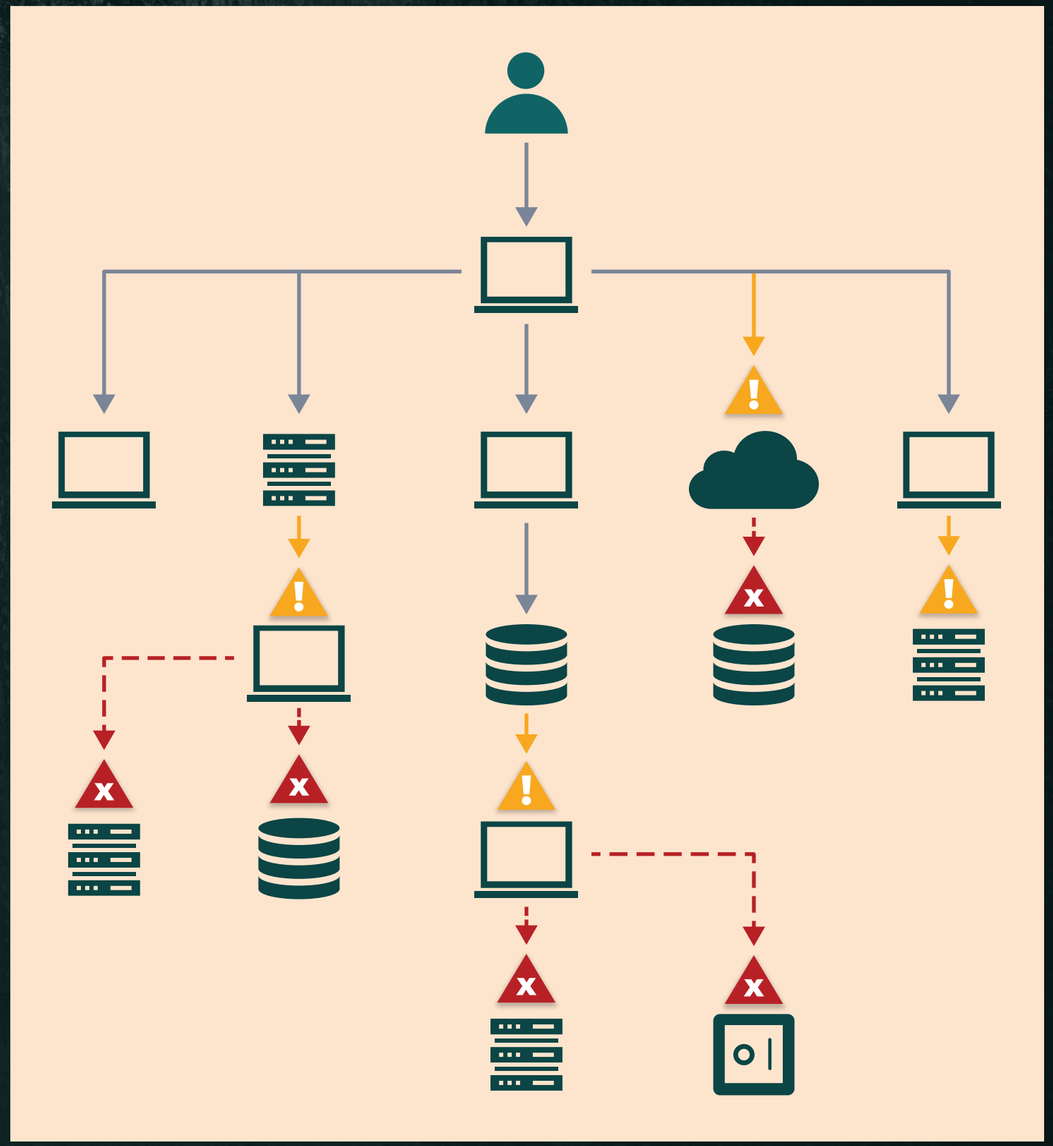
The Need to Apply Context and Enforce Access to Every Resource

HOW TO DEFINE GRANULARITY

Granularity is the ability to apply both context and enforcement to the level of each individual resource access continuously. Once this ability is available, organizations can now make informed decisions on how to apply it in a way that aligns with security while taking into account other considerations including user experience.

WHY GRANULARITY IS IMPORTANT

Granularity is the final step in an Identity Zero Trust implementation, where organizations are able to apply risk analysis and can also take enforcement action at the most granular level of access to every individual resource. For example, applying policies to each resource within a network segment rather than just at a gateway, thus preventing threat actors using compromised credentials from being able to gain access to multiple resources at once.

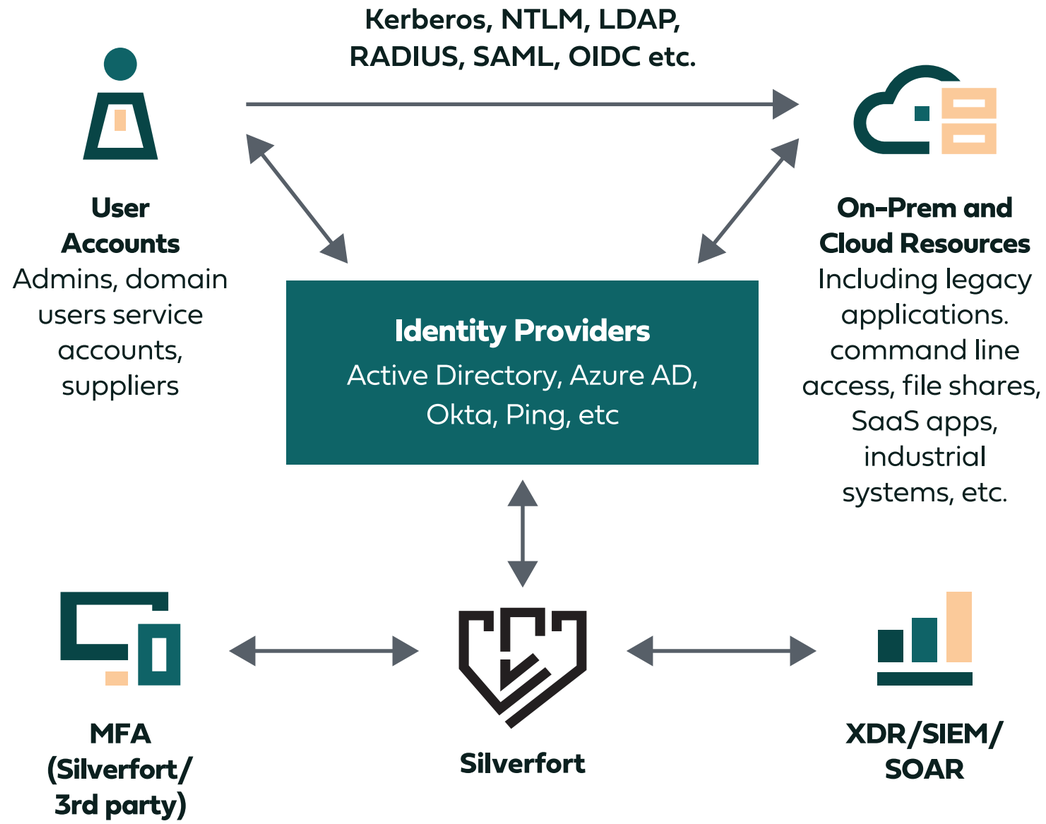


Introducing Silverfort: Unified Identity Protection

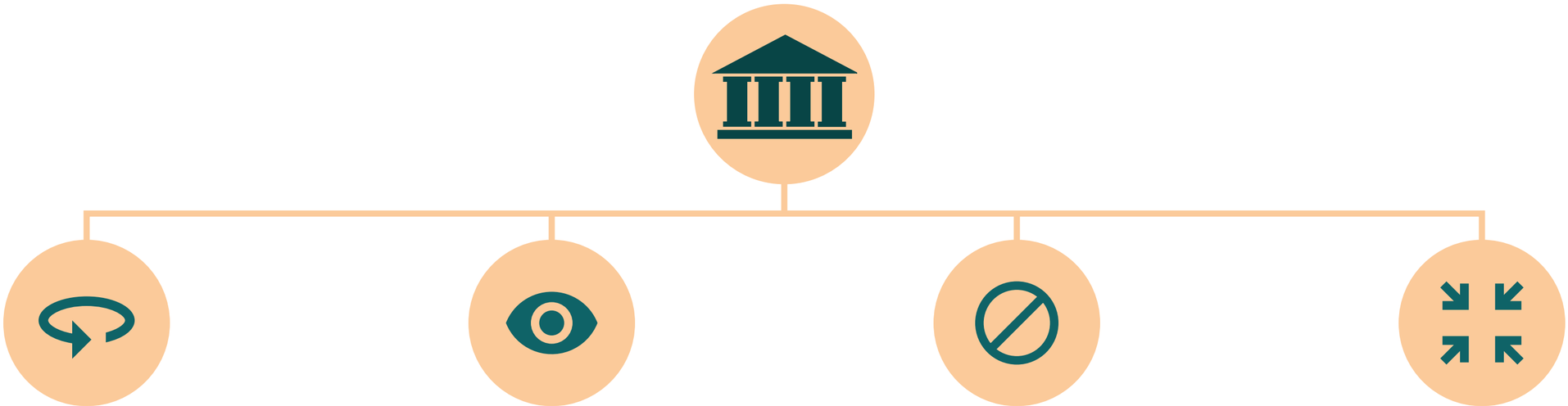
Silverfort enables organizations to monitor and control every authentication taking place within their environment, regardless of user or resource. This means modern identity controls such as MFA can now be applied everywhere, including to legacy systems as well as the command-line interfaces used in the majority of data breaches and ransomware attacks.

Silverfort uses an innovative agentless and proxyless technology that runs in the backend of an existing IAM infrastructure to enforce MFA across the hybrid environment and stop identity threats in real time.

When an identity provider receives an access request (regardless of user, resource, or protocol used), the authentication packet is forwarded to Silverfort for risk analysis and policy enforcement. If MFA is required, the relevant third-party MFA provider triggers the MFA push and – based on user response – Silverfort then passes this verdict back to the identity provider to either allow or deny access.



How Silverfort Implements the Four Pillars



Unification

Silverfort has native integrations with every identity provider, enabling it to log every authentication request, thus providing a unified view of all network activity across every user and any resource.

Context

This ability to see all activity also means Silverfort can evaluate the full context of every authentication and develop a sophisticated risk analysis engine to determine whether every authentication is legitimate or not.

Enforcement

Silverfort can actively enforce policies due to the platform's MFA capabilities and integrations with all third-party MFA solutions.

Granularity

Silverfort integrates with every product in the security stack, including SIEM tools, EDR/XDR solutions, and SOAR software, giving teams the ability to fine-tune access enforcement policies for each resource.

Identity Zero Trust Readiness Self-Assessment

This table includes a series of questions related to each pillar that can act as a readiness assessment to help you take the next step on your Identity Zero Trust journey. For each question, think about not only whether your organization has this capability but also how much effort would be required to achieve it.

Implementation Pillar	Identity Zero Trust Readiness	Capability Y / N	Effort S / M / L	Silverfort
Unification	Do I have real-time visibility into all authentications and access attempts?			✔
	Is this visibility available in a single interface?			✔
	Can I easily discern between standard users and privileged users?			✔
	Can I really discover all existing service accounts?			✔
Context	Do I have a risk engine that can ingest all authentication data?			✔
	Do I have a single engine that can cover all authentications?			✔
	Can my risk engine determine reliably whether any given authentication is legitimate or malicious?			✔
Enforcement	Can I enforce rule-based access policies across all resources?			✔
	Can I enforce risk-based access policies across all resources?			✔
	Can I apply MFA to all resources and access interfaces?			✔
	Can I block malicious authentications in real time?			✔
Granularity	Can I apply Zero Trust to the level of each resource access?			✔
	Can I control additional parameters (such as connection length, etc.)?			✔

About Silverfort

Silverfort has pioneered the first-ever Unified Identity Protection platform, which protects enterprises against identity-based attacks that utilize compromised credentials to access enterprise resources. Using innovative agentless and proxyless technology, Silverfort natively integrates with all existing IAM solutions, to extend secure access controls such as Risk-Based Authentication and MFA across all on-prem and cloud resources. This includes assets that could never have been protected in this way before, such as homegrown/legacy applications, IT infrastructure, file systems, command-line tools, machine-to-machine access, and more. Silverfort continuously monitors all access attempts by users and service accounts, and analyzes risks in real-time using an AI-based engine to enforce adaptive access policies.

For more information, visit silverfort.com