WHITESWAN
IDENTITY SECURITY

Whiteswan Datasheet

Eliminating Identity & Access Blind Spots

Identity & unauthorized access based cyberattacks remain the top culprit for Security breaches in 2022. An alarming 84% of organizations experienced an identity-related breach in 2022, according to a recent survey by Identity Defined Security Alliance.

Advanced attacks are bypassing critical identity controls placed on applications and infrastructure. These attacks are challenging to prevent because traditional identity solutions don’t monitor insiders once they are admitted. Once the attackers are admitted either via stolen identities, tokens etc. they can move about in the network as a legitimate user. The only way to prevent the attacker masquerading as an insider from achieving their goal is to have granular Just-in-time controls around the devices and connections.

Key Benefits

» **Protects Active Directory** sensitive accounts with MFA and Passwordless authentication. Grant Just-in-time privileges for sensitive operations

» **Protects internal & legacy endpoints and servers** with continuous MFA

» **Protects legacy web applications** by ensuring that only authorized devices and users can connect

» **Eliminates dwell time** by applying MFA on system utilities to prevent lateral movement & payload detonation

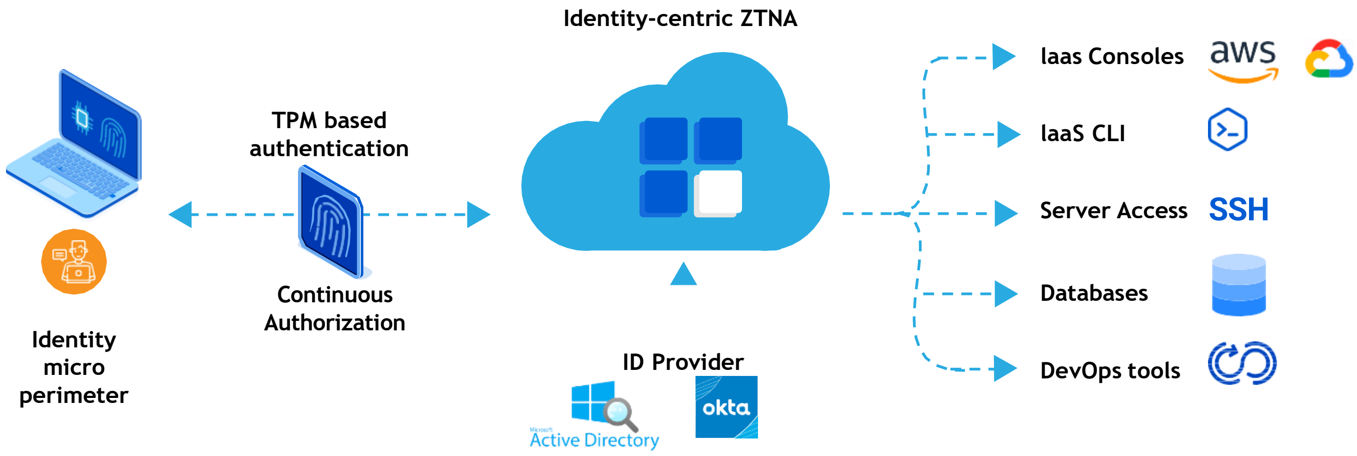
» **Reduces operational complexity** with no-gateway, no-secret management approach

» **Effectively hardens endpoints** against known and unknown vulnerabilities without patching Precise results reduce analyst costs

**for on-prem/Active directory onboarded computers*

Zero-standing privileges

Whiteswan Identity Security Platform is the only solution that implements complete zero-standing privileges for your endpoints and workloads by combining secure remote access, application control and permissions assurance to secure workloads and endpoints from identity attacks.



Whiteswan achieves zero-standing privileges for your applications and cloud infrastructure by deploying the following modules:

Identity protection for Local Admin, Service accounts and Privilege accounts

» Discovers Local Admin, Service Accounts and Privilege accounts across your endpoints and servers
» Constantly monitors any newly added local administrators; Ability to remove Local Admins on Endpoints
» Enrolls end-users, privilege users and devices into MFA via Trusted Platform Module/passkeys
» Challenges users to provide MFA when the commands/applications deviate from the norm
» Works across Windows, Linux and Mac's Operating Systems
» PAM features – Follow the user Screen recording, Detailed Session auditing on server, termination of session on unsafe commands, Privilege user MFA enrollment

Identity-centric Trusted Access w/ built-in JIT workflows

» UDP based Peer to Peer Network establishment without gateways. Direct connect from Remote end-user to OT server.
» Continuous monitoring of privilege operations and connections
» Works across Windows, Debian and Linux Operating systems
» Instant access and revocation to RDP, SSH and VNC ports on remote server
» Ability to place restrictions around Time/Geo etc. when personnel are accessing sensitive servers

Features and Capabilities	
Endpoint Privilege Management	Just-in-time controls and privilege rightsizing for local admins and users
Application Control	Just-in-time controls at a Publisher/executable granularity
DLP control	Just-in-time controls on network folder access
Secure Remote Access to Corporate Applications and Infrastructure	Automated Point-to-Point (p2p) VPN overlays utilizing the noise protocol framework
MFA enrollment	Device and user enrollment in portal, Trusted Platform Module (TPM)
Identity Providers	Active Directory, Okta, SAML support
Visualization | Reporting | Monitoring	
Real-time dashboard reporting	charts, reports and alerts around Privilege creep, insider activity etc.
Attack Attribution reporting	Real-time logging
Application Environments Supports	
Operating Systems	Endpoints: Windows 7 – Windows 11 Servers: Windows 2003 – Windows 2022 RHEL: RHEL 6.x – RHEL 9.x Ubuntu: Ubuntu 12.04 – 20.04 Mac OS: Yosemite and above