NEXTLABS®

Application Enforcer for Network File Shares

Secure Supply Chain Planning Ecosystem

THE SITUATION

Ensuring zero trust principle using attribute-based access control and mandatory access control across file stores is extremely difficult in today's enterprise: servers are distributed, housed onpremises and in the cloud, and often managed by different administrators. IT must have the ability to update controls in response to frequently changing user job responsibilities, project assignments, and shifting requirements, as well as maintain visibility into access control events for auditing and troubleshooting.

The existing discretionary access control model simply can't keep pace with these requirements, which leaves over-burdened IT teams struggling to meet compliance, governance, and risk management objectives.

THE SOLUTION

NextLabs Entitlement Manager for Network File Shares supports Server Message Block and Common Internet File System (SMB/CIFS), Samba, and Windows servers in providing fine grained, unified access control, and audit capabilities across file stores and other applications. The solution is easily deployed with no change to network infrastructure and zero-perceptible latency to end-users.

THE RESULTS

Unify Access Control Across All File Stores and Azure Files

- Control access across file stores, monitor user activities in real-time with summary dashboards, event details, and alerts, track behavior over time

Control Access by Mobile Users and Unmanaged Hosts

- Prevent unauthorized file store access by mobile users on unmanaged hosts from unknown locations or devices

Protect Data with Advanced Access Control

- Provide granular access control for file stores based on a variety of variables, including user, location, network connection, requesting host, and data classification or content

Centrally Manage Enterprise-wide Access Control and Audit

- Reduce management and compliance cost with centralized access control administration and access auditing across all file stores

Support for Any CIFS/SMB and Samba Compatible File Store

- Deploy as an integrated component of an enterprise entitlement management solution encompassing file stores, Microsoft SharePoint, enterprise applications, and data protection

DYNAMIC AUTHORIZATION ACROSS FILE STORES

Traditional file store access controls are container-based and discretionary. As a result, system administrators need to grant permissions, control target-specific network locations, and trust end users to be both informed and compliant (by storing information in correct locations to prevent wrongful disclosures or data breaches. Administering these container-based controls (user groups and permissions can be both cumbersome and expensive especially when teams try to implement complex requirements across multiple systems. Dynamic authorization is an approach that complements and extends container-based controls by controlling access based on metadata, user attributes, and other factors— across all file stores at once. Data is protected no matter where it is stored, and there is no need to maintain multiple sets of cumbersome, container-based controls.

STANDARDS-BASED APPROACH

Entitlement Manager for Network File Shares is based on eXtensible Access Control Markup Language (XACML, the industry standard for Attribute Based Access Control (ABAC. A single set of digital policies can be deployed across all CIFS/ Samba and Samba-compatible file stores, Microsoft SharePoint, and enterprise Line of Business (LOB applications.

INTEGRATION WITH EXISTING INFRASTRUCTURE

NextLabs' Attribute Based Access Control can extend native Permissions and Security Groups already maintained in Active Directory, so IT teams do not need to overhaul its security infrastructure in order to complement their existing security with dynamic authorization. The Entitlement Manager for Network File Shares also integrates with Microsoft Active Directory (AD), Azure AD, Azure Access Control Service (ACS), Microsoft Purview, and File Classification Infrastructure (FCI), allowing IT to control access based on user and device claims and resource properties.

CENTRALIZED AUDIT AND REPORTING

Policy compliance and end user activity are collected in a central Activity Journal for reporting by NextLabs Reporter, a graphical analysis, charting, and reporting application.

ENTITLEMENTS FOR MOBILE USERS AND UNMANAGED HOSTS

The Entitlement Manager for Network File Shares can manage access by mobile users and unmanaged hosts using intelligent host recognition which dynamically controls access based on host name, domain, platform, country, or site location. This can be done without installing any software on the client. Example controls can include:

- Prevent file store access from unmanaged hosts, such as visitor and contractor laptops
- Restrict access to select shared folders from internal network or from a specified office branch or location
- Prevent mobile users from downloading document via remote connections

SPECIFICATIONS

Feature	Support
File Stores Supported	CIFS, SMB, Samba
Cloud Platforms Supported	Azure, AWS
Operating Systems Supported	Windows Server 2016 Windows Server 2019 Windows Server 2022

ABOUT NEXTLABS

NextLabs®, Inc. provides zero trust data-centric security software to protect business critical data and applications. Our patented dynamic authorization technology and industry leading attribute-based zero trust policy platform helps enterprises identify and protect sensitive data, monitor and control access to the data, and prevent regulatory violations – whether in the cloud or on premises. The software automates enforcement of security controls and compliance policies to enable secure information sharing across the extended enterprise. NextLabs has some of the largest global enterprises as customers and has strategic relationships with industry leaders such as SAP, Siemens, Microsoft, AWS, Accenture, Deloitte, Infosys, and IBM. For more information on NextLabs, please visit http://www.nextlabs.com.