Axidian

WHITE PAPER

Axidian Shield

Comprehensive Identity Protection Over a Corporate Network

Identity Threat Detection and Response

Agentless MFA

Table of contents

Credential Protection and Access Management: The Main Measures for Ensuring Information Security

In recent times, with the development of cloud services and the widespread adoption of remote work, protecting the infrastructure perimeter has ceased to be the primary focus of corporate information security. Credentials (identity) can confidently be called a new perimeter that requires protection, as attackers no longer need to compromise network security assets. To access a company's resources, all they need to do is compromise credentials.

As numerous studies have demonstrated[1], corporate information security departments allocate a significant portion of their budgets to IAM due to the fact that the number of attacks on credentials has been steadily increasing. Compromising and subsequently using credentials to access information systems have become central elements of nearly every cyberattack. This is an inevitable consequence of the fact that attackers seek out and utilize all available new methods to exploit a continually expanding attack surface and the exposure of credentials.

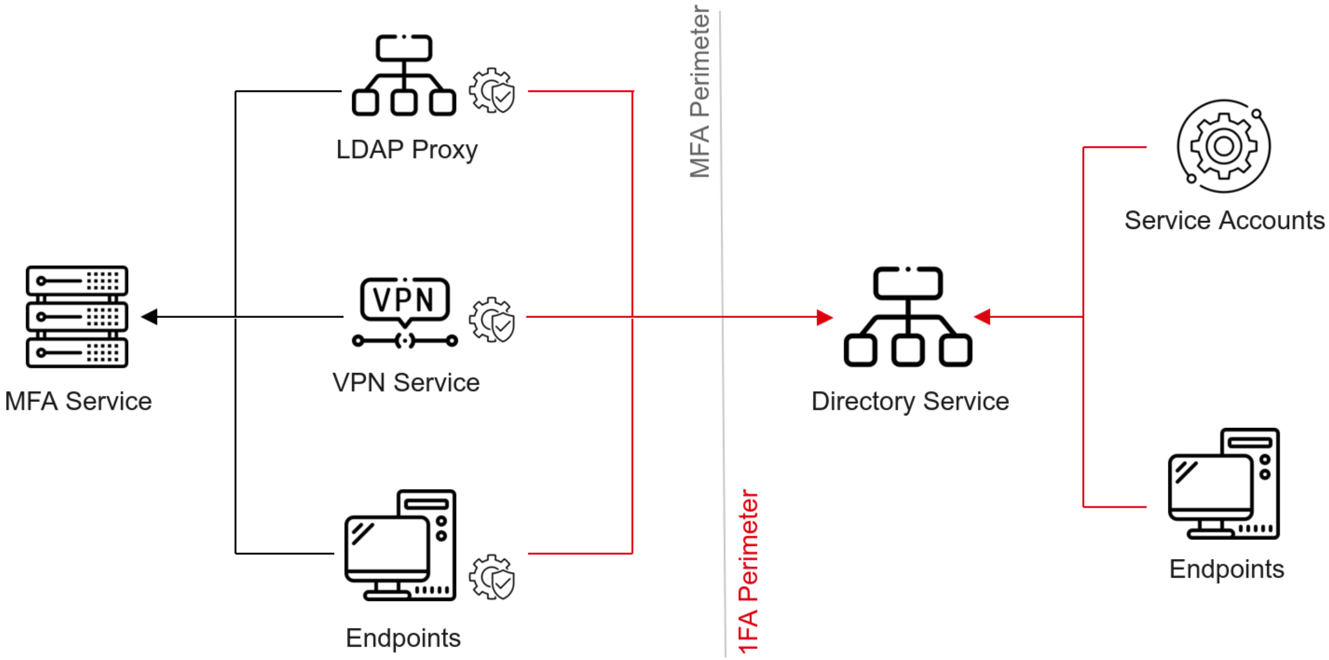
In addition to the already mentioned trends towards the use of cloud services and remote work, one should not forget about the old issues of managing account data and access by means of traditional IAM:

- There are virtually no means of controlling service accounts.
- Disparate products are used to build IAM infrastructure.
- Creating a consolidated system for monitoring events related to access across all possible accounts in all possible systems is simply impossible. Consequently, there’s no way to build an enterprise-level adaptive system that would detect and respond to access-related problems and threats.

Also, it is worth noting that multi-factor authentication is usually implemented in a corporate environment at the client or intermediate component level (Credential Provider, LDAP Proxy, RADIUS Server, etc.), while the authentication provider (KDC and LDAP Server of the domain controller) continues to operate in single-factor mode. Thus, a large number of attack vectors on account credentials remain relevant even if the organization fully utilizes IAM.

Below is a logical diagram of a traditional solution for multi-factor authentication in a corporate network. Authentication requests that remain single-factor are shown as red arrows.

[1] https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bcRe?culture=en-us&country=us https://www.google.com/url?q=https://www.beyondtrust.com/resources/whitepapers/identity-issues-impact-zero-trust-effectiveness&sa=D&source=docs&ust=1712566331659248&usg=AOvVaw19_2unFURLsE7aOA1zC7ar



A diagram of a traditional multi-factor authentication solution

Additionally, while the authentication provider continues to operate in a single-factor mode, transitioning a secured infrastructure component into a single-factor circuit usually only requires reconfiguring the component itself by disabling the MFA agent on it. An important characteristic of identity attacks is that with traditional approaches and tools, it is practically impossible to determine whether the credentials are being used by a legitimate user or an attacker.

Identity Threat Detection and Response – ITDR

The systems included in the ITDR solution continuously monitor the activity of user and service accounts, identifying unusual sequences of events and patterns that indicate the preparation or execution of attacks on user credentials. To assess the ongoing processes in the infrastructure, indicators can be compared both with statically defined values and with basic statistical data that is constantly calculated during the operation of ITDR systems.

Similar to EDR (Endpoint Detection and Response) and NDR (Network Detection and Response) solutions, ITDR systems provide threat detection and identification, as well as offer incident analysis and management, attack containment, and recovery capabilities.

The key functions that a mature ITDR solution should perform include:

- Real-time monitoring of access requests and access provisioning events.
- Continuous collection and aggregation of data from various sources, threat detection, and high-quality data visualization.
- Proactive protection measures.

Depending on how the system classifies a particular threat, entities affected by the incident may have their access to specific services blocked or additional authentication factors may be required.

The system should have access to all authentication and access events, meaning the integration of ITDR into the infrastructure should occur at the level of the central authentication provider, rather than at the level of client components. This enables the development of high-quality, adaptive security policies that take into account all aspects of user behavior, thereby minimizing false detector triggering without weakening protection.

Axidian Shield

Axidian Shield provides multi-factor authentication and protection against attacks on user credentials in any corporate environment without requiring changes to the protected systems or the installation of any agents or proxies. This innovative technology allows for the protection of even those systems that were previously considered impossible to secure, including:

- Systems developed within the organization
- Closed proprietary systems
- Administrative utilities, such as PsExec
- Shared network folders

Axidian Shield performs in-depth analysis of authentication protocols at the network level, thus gaining access to all events involving the use of credentials within the protected perimeter.

In addition to monitoring traffic, the system can exert control directly into the client-provider authentication interaction channel. For example, it can block access or seamlessly introduce a request for a second factor into traditional authentication protocols, regardless of the user's scenario.

The main advantages of this method of integration into the infrastructure are:

- Analyzing logs of IAM system events and corporate authentication providers is no longer necessary. This allows the system to detect threats faster and more efficiently than traditional solutions that analyze logs and infrastructure configurations.
- The method makes it possible to work with a potential maximum amount of input data: in most cases, the data does not need enrichment; all necessary information can be obtained from network exchanges between the client and the authentication provider.
- The integration of MFA at the protocol level does not require the installation of agents and proxies: protection is provided not at the client component level but at the authentication provider level. This ensures that even if an attacker gains control over client and server components of protected systems, it’s not possible to disable MFA.

It's important to note that the system includes built-in mechanisms for detecting service accounts. Administrators can confirm that account is a service account and apply all necessary restrictions to it, such as binding it to a specific host, allowing access only to specific corporate services, prohibiting interactive logins to the system, and so on.

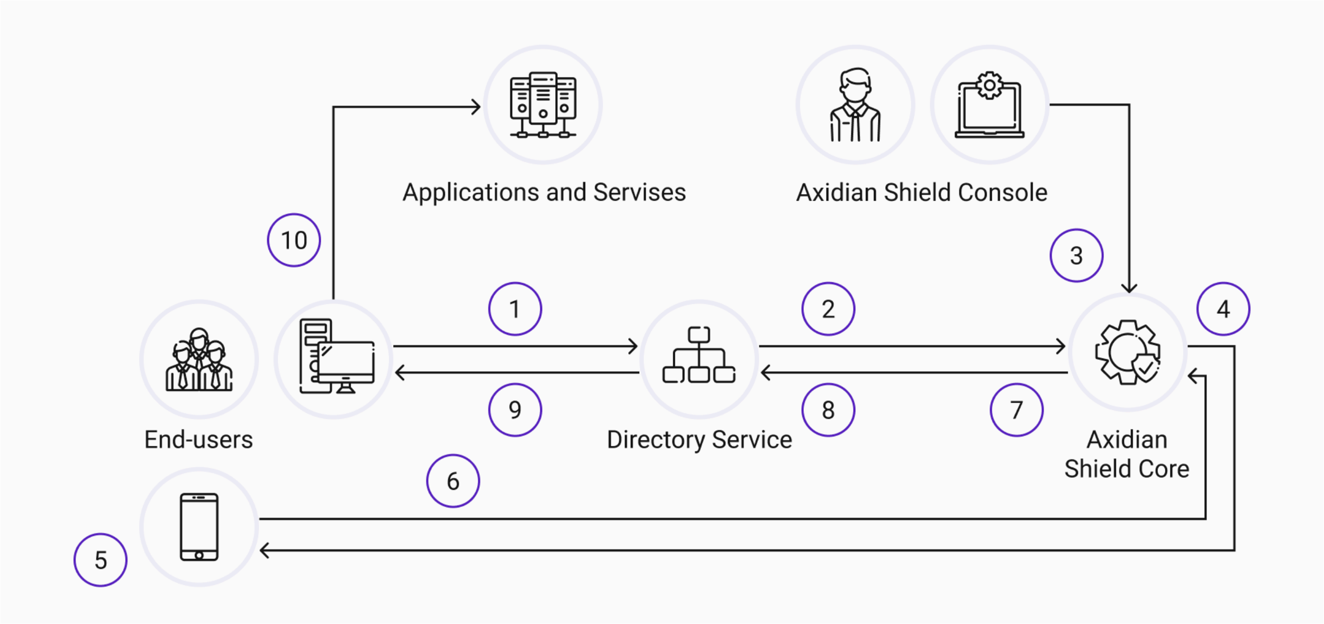
Supported protocols

The first version of Axidian Shield supports the following protocols:

- Kerberos
- NTLM
- LDAP
- LDAPS

Architecture

Unlike most other solutions, Axidian Shield does not require the installation of any agents or proxies, nor does it necessitate reconfiguring target systems on the server side. Integration into the infrastructure is achieved through the configuration of request and response forwarding for authentication protocol traffic from the authentication provider to the core component of Axidian Shield. In this process, standard operating system tools (Windows, Linux) and automation scripts in Bash or PowerShell are used on the authentication provider. There is no need to install or run proprietary closed-source software or compiled executable files on domain controllers.



General architecture and diagram of a typical authentication scenario

1. An authentication request with a domain password is sent to the domain controller. No additional software is installed on the client workstation.
2. The request is redirected to Axidian Shield.
3. Axidian Shield analyzes the request. The system can grant or block access based on specified restrictions and parameters, including requesting user confirmation through a second factor.
4. An optional access confirmation request is sent via push notification to the mobile application of the target user.

5. The user confirms or declines the request.
6. The response from the mobile application is sent to Axidian Shield.
7. If the user confirms the authentication request in the app, the system passes the initial request to the domain controller for standard processing. If the user declines the request, the system generates its own error response and sends it to the user through the domain controller.
8. The domain controller processes the authentication request. Typically, this step involves verifying the Kerberos or LDAP authenticator.
9. The user receives a response from the domain controller, such as a Kerberos ticket.
10. The user gains access to domain-integrated services.

Detected Attacks

With the help of Axidian Shield, the following typical attacks and hacking techniques can be effectively identified and stopped:

- User Enumeration
- Password Spraying
- AS-REP Roasting
- Kerberoasting
- Golden/Diamond Ticket
- Diamond PAC
- Pass-the-Ticket
- Skeleton Key
- Lateral Movement

Integration with External Systems

Axidian Shield can serve as a provider of account behavior data for SOAR and XDR systems. Additionally, the system can be used via an API when developing response playbooks for blocking access or enabling MFA on a target set of managed entities.

Distribution Method

The system is distributed in the form of a Linux OS-based virtual appliance and is fully deployed within the customer's infrastructure.

About Axidian

Axidian is a global IT vendor specializing in Identity Security. We provide a comprehensive approach to managing and securing identities. Our company operates from the United Arabian Emirates and considers itself a part of the local IT security community. Our goal is to contribute to the development of cybersecurity hygiene and culture in the region and globally.

Axidian is where Identity Security finds its Axis.

If you have any questions about our products or are interested in learning more, visit us at axidian.com.

☎ +370 (5) 208 0466

☎ +971 4 540-13-68

☎ +65 3125 8699

✉ sales-europe@axidian.com

✉ sales-mena@axidian.com

✉ sales-asia@axidian.com