Auth Shield
Multi Factor Authentication

An Authentication Security Organization

Case Study | GatewayRail

Protecting Windows Logon (Remote Desktop and Local Logon) with AuthShield Multi-Factor Authentication

Auth Shield
Multi Factor Authentication

Contents

Auth Shield
Multi Factor Authentication

Overview

We all know that Windows-based systems have plenty of potential security risks. However, access to Windows-based systems is commonly protected only by primary credentials - just a username and password. Compromise of primary credentials puts not just individual workstations but entire ecosystems of servers and workstations at risk.

Analysis of data breaches show that compromised primary credentials continue to play a primary role in data breaches: 95% of breaches involve the use of stolen credentials, according to the Verizon 2015 Data Breach Investigations Report.

Some of the weaknesses of Windows Based Systems:

- File and share permissions that give up everything to everyone
- Lack of malware protection
- Lack of personal firewall protection
- Weak or nonexistent drive encryption
- No minimum security standards
- Missing patches in Windows as well as third-party software
- Weak Windows security policy settings
- Weak or nonexistent passwords

Adding Two-factor authentication to the Windows Logon process helps secure Windows workstations and servers from unauthorized access.

GatewayRail has deployed AuthShield Two-factor Authentication on the Windows Logon to secure access to systems. AuthShield two-factor authentication is based something the user knows (a password or PIN) and something the user has (an authenticator).

About Organization

GatewayRail provides inter-modal logistics and operates its own rail-linked Inland Container Depots (ICD) at Gurgaon, Faridabad, Ludhiana, and Sanand. It also operates a domestic terminal at Mumbai. The company operates a fleet of 23 trains and 265+ owned road trailers at its terminals. GatewayRail operates regular container train services from these ICDs to the Nhava Sheva, Mundra and Pipavav ports, transporting EXIM as well as domestic containers. All major shipping lines operate from these terminals.

The Challenge

Client faced various challenges with respect to its critical information. They have many large implementations used for business-critical processes, deployed across the entire organization. With recent attacks on their systems, it has become essential to protect the credentials of users logging into Windows Login systems. They needed an efficient way to detect such threats as specific vulnerabilities are difficult to detect in their critical environment.

Need of Client

Objective

Client wanted to implement a security solution enabling employees to securely access the organization's systems and its applications as it contains organization's most sensitive data.

Requirement

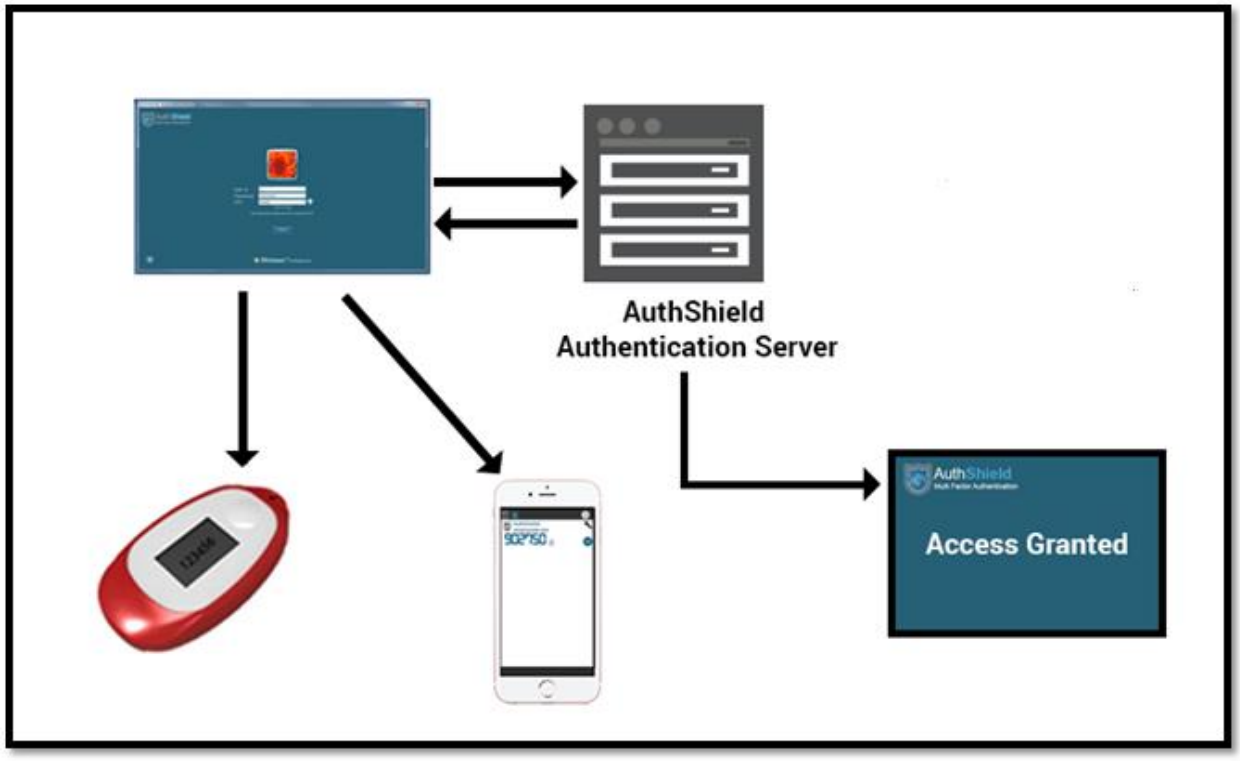
They needed a solution in which no additional hardware is required in their environment. Also, require a scalable and proven high-security solution without compromising on user friendliness.

Auth Shield
Multi Factor Authentication

Two-Factor Authentication for Window Login

AuthShield integration for Windows Remote Desktop Protocol (RDP) protects both RDP and local console logins for versions of Windows from Vista to Windows 10 clients, and Windows server operating systems from 2008 to 2012 R2.

Technical Architecture



Process

- AuthShield Authentication Plugin needs to be installed at the user's system.
- Enter OTP generated from Hard Token or Mobile Token
- Entered Password gets validated from Local Database/ AD/ LDAP whereas OTP gets validated from the Authentication Server
- Once validated, User shall be granted access to the Windows.

Protecting the system

When your organization banks on you, what do you bank on?

Prevention is always better than cure. It is truer today than ever before when the theft is conducted on the net with no physical threats and with less cost to the perpetrator of the crime. The only challenge that remains is to cover ones tracks and considering the massive flow of information on the net almost on a daily basis, it is not much difficult either.

Multi-Factor Authentication: why do you need it?

Phishers try to obtain personal information such as your password or PIN-code by pretending to be a legitimate entity.

Using Phishing, static passwords can be easily hacked providing fraudsters easy access your personal accounts, files and confidential information.

AuthShield - Multi Factor Authentication maps the physical identity of the user to the server and increases the security of financial and other critical systems. Integrating Stronger User Authentication system not only helps prevent Online Credit Card fraud, Card Cloning, Identity theft but also helps in the capture of habitual cyber criminals.

AuthShield authenticates and verifies the user based on –

- something only the user has (mobile phone/ land line/ hard token)
- something only the user knows (user id and password)
- something the user is (Biometrics)

AuthShield technology uses a dual mode of identification where along with the user id and password, verification is done through a secure randomly generated through One- time password (OTP). This is provided to the user through –

Auth Shield
Multi Factor Authentication

Hard Token

AuthShield's Hard token is a security device given to authorized users who keep them in their possession. To verify a transaction using second factor of authentication, the device displays a changing number that is typed in as a password. The new number is based on a pre-defined unbreakable randomized algorithm. Thereby, the hard token enables the server to authenticate the digital identity of the sender using a hardware device apart from his user name and password.

Auth Shield
Multi Factor Authentication

Mobile Token

AuthShield's mobile token is an application installed on smart phones which generates an OTP for the user on the phone itself.

The architecture remains similar to a Hard Token except that the user only has to carry his mobile phone. Thereby, the device enables the server to authenticate the digital identity of the sender using a mobile phone apart from his user name and password.

Auth Shield
Multi Factor Authentication

Why our Solution was chosen over other Solutions

- Only organization providing Multifactor Authentication Security at **Protocol Layer.**
- Seamless integration with any application whether it supports or doesn't support Multi-factor Authentication.
- Robust and Proven Technology
- Competitive Prices
- Flexible Network and Time Policies
- Simple Deployment Model and Unparalleled Support

Features

- OS Independent Authentication Mechanism
- Seamless Integration with the current business and security architecture
- Increases the log on security for Mails
- 99% security from Phishing attacks and identity thefts
- Unbreakable encryption on the lines of those used by US Government
- Logs are maintained to fix responsibility in case of an unlawful event.

About Us

The world today revolves around information. Information today is the energy that plays a critical role in our personal lives and drives our businesses. As we move further into this digital age, it has become imperative to not just protect our information from outsiders but to also draw intelligence from the vast amount information available to us.

AuthShield is an Authentication Security solution with a patented technology on implementing Multifactor Authentication at a protocol level. This makes it an application independent technology and needs no changes at the application. As an advantage of working at protocol rather than application level, an organization can use AuthShield to implement Multifactor Authentication in any and every technology such as **Downloading mails on phones / desktops,** SAP, Database queries, Internet of Things, or any other enterprise or cloud technology in a matter of minutes.

Contact Us

@ authshield2FA

+91-11-47065866/ 45272272

info@auth-shield.com

www.innefu.com / www.auth-shield.com