

SphereShield for ADFS

Enhanced ADFS protection for securing cloud services



AUTHORIZED USERS CAN CONTINUE USING ADFS EVEN WHILE UNDER AN ATTACK

ADFS - an enterprise security risk

Active Directory Federation Services (ADFS) is an authentication service developed by Microsoft that allows the secure sharing of identity information between trusted business partners across an extranet and the company's local Active Directory.

Enterprises utilizing cloud services, such as Office 365, typically use ADFS to extend their end users' single sign-on (SSO) access to applications and systems outside the corporate firewall. Allowing an external service to authenticate against your local Active Directory (AD) presents a security challenge, and puts ADFS at risk for Distributed-Denial-of-Service (DDoS) attacks. Even without the password, an attacker can easily lock an account simply by sending failed login attempts with the employee's user name, a value that is easily exposed.

Microsoft Windows 2012 Extranet Lockout protection limitations

Traditional solutions such as the built-in Windows 2012 Extranet Lockout protection – a part of the Windows 2012 server – fail to provide a workable solution for most enterprises. Once the software detects an attack, the Extranet Lockout is activated and ALL external access is denied, with no exceptions. This means that while the internal account remains

FEATURES AND BENEFITS

- Ability for authorized users to continue using ADFS even while under an attack
- Enhanced ADFS security against automated/human attacks
- Account lockout (DDoS) protection
- Security auditing logs and reports
- Mitigation of ADFS Extranet Lockout Protection's vulnerability
- Live Geo location map
- Geo fencing rules
- IP based restrictions
- Security auditing and reports
- Authentication risk engine
- Simple and transparent deployment
- No end user training required



secure, legitimate users are still unable to access the account through ADFS, causing significant disruption to business operations. As more and more services depend on ADFS, the impact of DDoS is more significant. In addition, Windows 2012 Extranet Lockout fails to fully protect the AD account from all lockouts. AGAT has identified and demonstrated the

ability to lock Active Directory accounts even when the ADFS Extranet Lockout feature was configured to block account lockout. SphereShield for ADFS' robust solution addresses this vulnerability, ensuring the enterprise extranet is secured in all scenarios.

Enhanced ADFS protection

SphereShield for ADFS is a proprietary security solution that allows legitimate users to continue accessing their cloud-based services even when their account is under attack. Developed by AGAT Software, an innovative security provider specializing in external access, authentication and data protection solutions, SphereShield for ADFS delivers new-generation ADFS protection against automated attacks/bots and human-based attacks.

Security for business critical applications

Utilizing adaptive authentication options based on real time data analysis, SphereShield for ADFS offers more robust protection than Windows 2012 Extranet Lockout Protection. An advanced management portal enables proactive analysis, detection and auditing of security incidents. SphereShield for ADFS provides enterprises with peace of mind of knowing that their business critical applications are well secured.

- **Account lockout protection**

AGAT Software's authentication and data protection solutions are widely deployed and successfully securing global enterprise applications across a range of industries. The new-generation SphereShield for ADFS builds on AGAT's proven ADFS security solution by solving the issue of extranet lockout that prevents legitimate users from being able to sign in while their account is under attack.

- **Multi-factor security features**

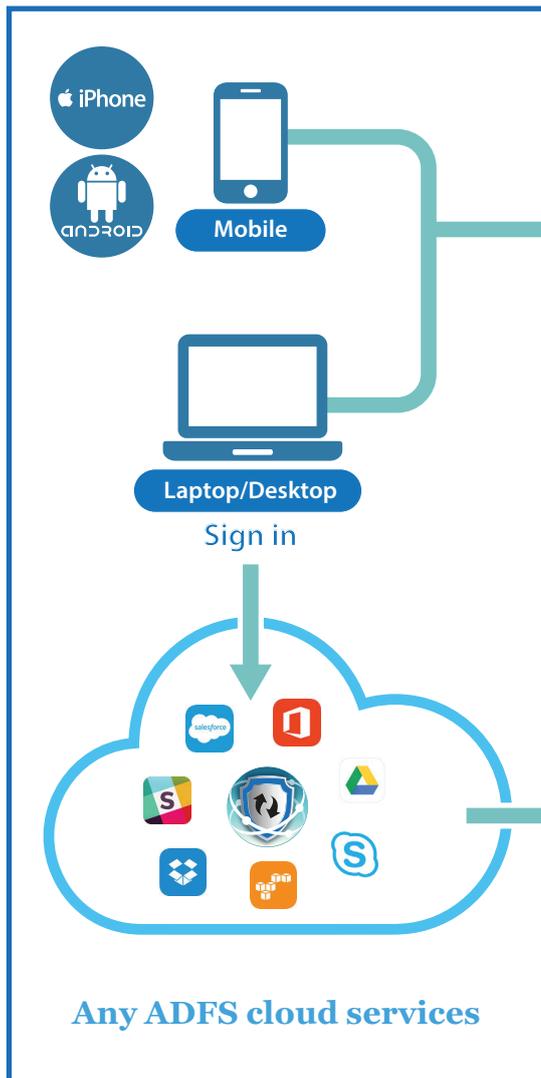
Using a range of parameters to identify authorized user authentication, SphereShield for ADFS offers adaptive authentication methods based on real-time risk assessment. Threats can be identified based on geolocation, device identifiers and behavior profiling.

- **Security dashboard**

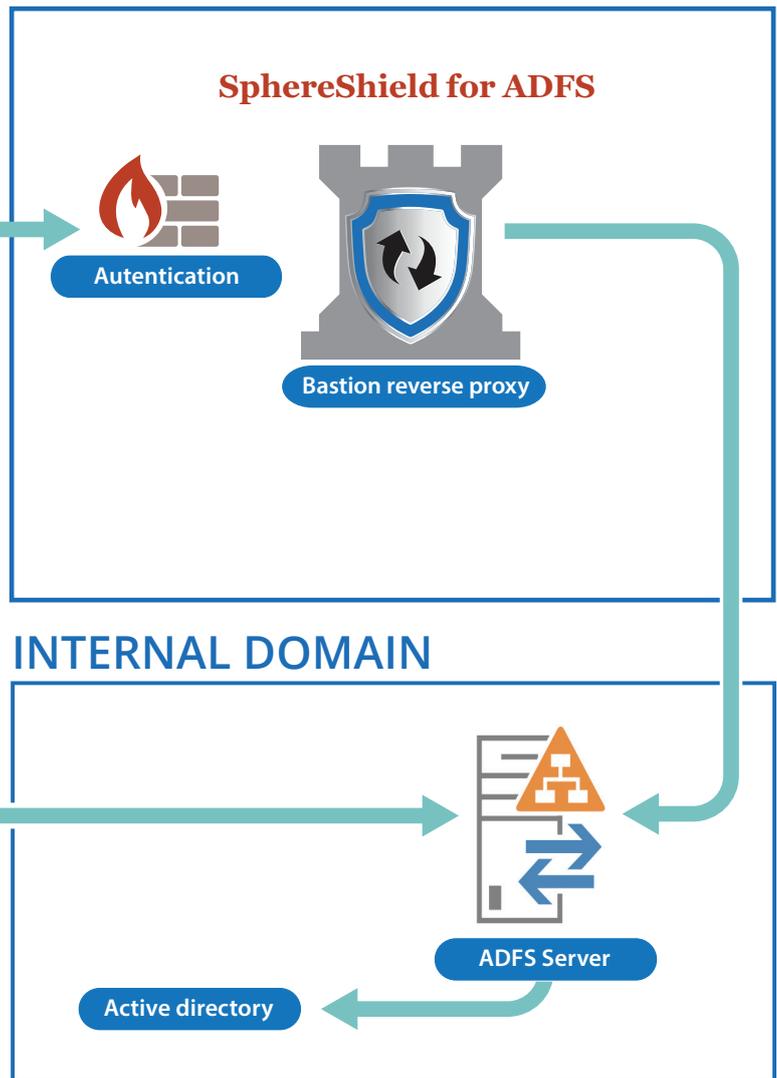
SphereShield for ADFS offers enterprises an advanced tool for real-time monitoring and data collection of security events, failed login monitoring, data auditing including information such as user, device, IP, geo-location, as well as reports analyzing user behavior and data.



WORLD



DMZ



ABOUT AGAT

AGAT Software is an innovative security provider specializing in external access authentication and data protection solutions.

SphereShield - AGAT's product suite handles security threats related to password and identity theft as well as data and network protection.

Utilizing this expertise, AGAT developed solutions to secure Microsoft Skype for Business external connectivity. with specific unified communication (UC) and solutions for securing ADFS

AGAT's client base consists of government offices, banks, insurance companies and large industrial global corporations, including Fortune 500 companies.

For more information, please visit our site:

www.AGATSoftware.com