2 FACTOR + 2 WAY Authentication

Deepnet DualShield is an open, unified authentication platform that enables multi-factor strong authentication across diverse applications, users and security tokens.

DUALSHIELD
UNIFIED AUTHENTICATION

SC MAGAZINE

5 Star Award 2010

"A good value for the money and a nice enterprise solution."

★★★★★ **SC Magazine**

Introduction to DualShield

Deepnet DualShield™ is an open, unified strong authentication platform that enables multi-factor authentication across diverse applications, users and security tokens.

Authenticators

- One-Time Password (OTP)
  - OTP on Mobile Phones
  - OTP on USB Drives
  - OTP on ID Cards
  - OTP on-Demand
- Digital Certificate (PKI)
- Digital DNA
- Biometrics

Solutions

- VPN/RADIUS Authentication
- Windows/Linux Authentication
- Web Authentication
- Outlook
  - Outlook Anywhere
  - Outlook Web Access
  - Outlook Mobile Access
- Citrix
- 2X

DualShield is a complete solution for strong user authentication that is extremely user-friendly, cost-effective and easy to integrate into your existing IT infrastructure. The server software supports both MS Windows Server and Linux operating systems.

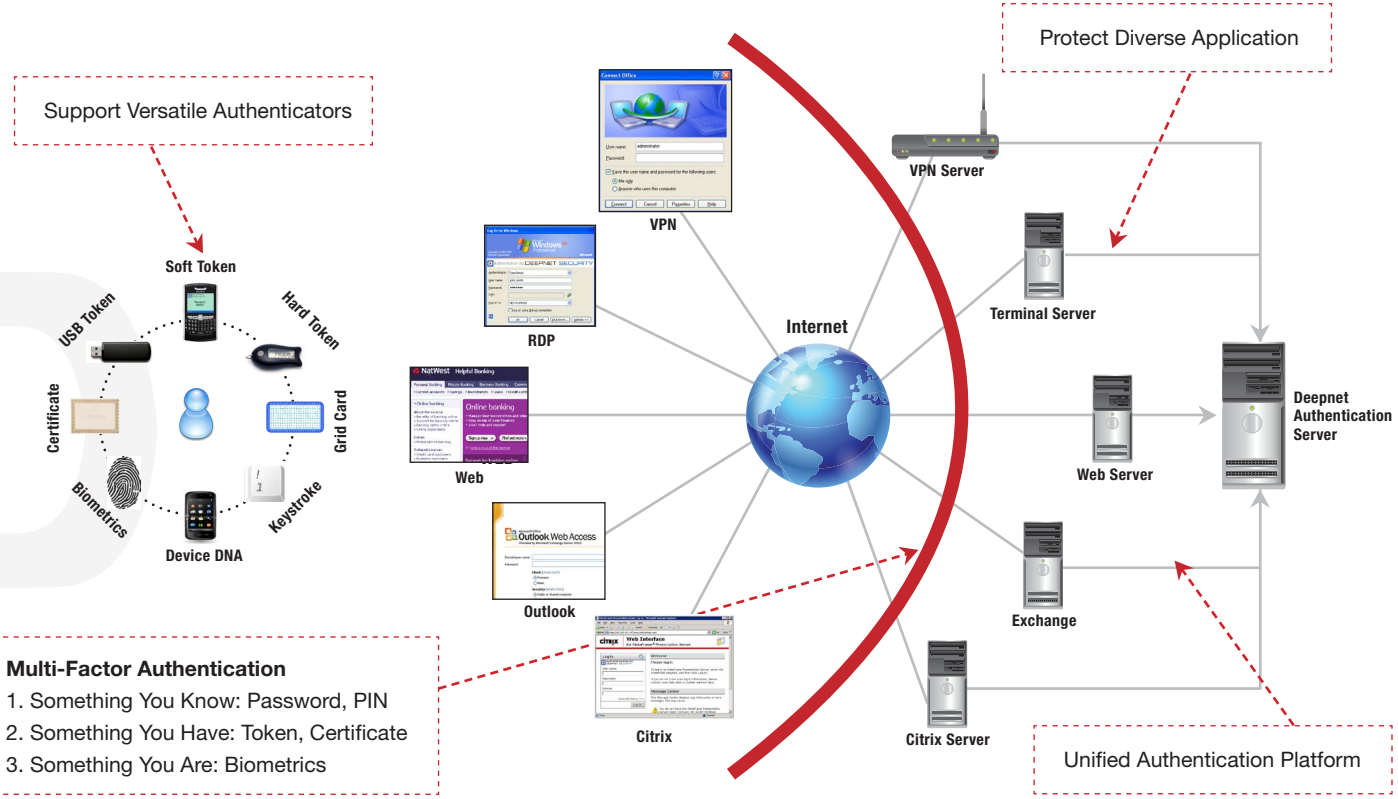
Key Features

- Web based management console
- Native LDAP/AD integration
- Centralized user management
- Role based access control
- Policy based administration
- Enhanced audit trail and reporting
- Extended RADIUS support
- Self-service web portal

DUALSHIELD
UNIFIED AUTHENTICATION

Copyright © Deepnet Security

Architecture of DualShield



Multi-Factor Authentication

1. Something You Know: Password, PIN
2. Something You Have: Token, Certificate
3. Something You Are: Biometrics

Copyright © Deepnet Security

MobileID

MobileID transforms mobile phones, USB drives, PDAs and PCs into One-Time Password (OTP) token devices, providing enterprises, banks, online service providers and retailers with a cost-effective means to provide strong authentication protection to their customers, business partners and employees without deploying additional, dedicated hardware tokens.

Key Features

- Two-Factor Authentication
- Two-Way Authentication
- Challenge & Response
- Data Signing
- OATH Compliant
- Dual Algorithms (HOTP, TOTP)
- PIN Protected
- Multi-Token Support

MobileID supports

- Mobile phones
  - JAVA enabled phones
  - Windows Mobile phones
  - iPhones
  - Blackberry
- USB flash drives
- PCs (Windows XP/Vista/7)

MobileID / Flash

MobileID / PC

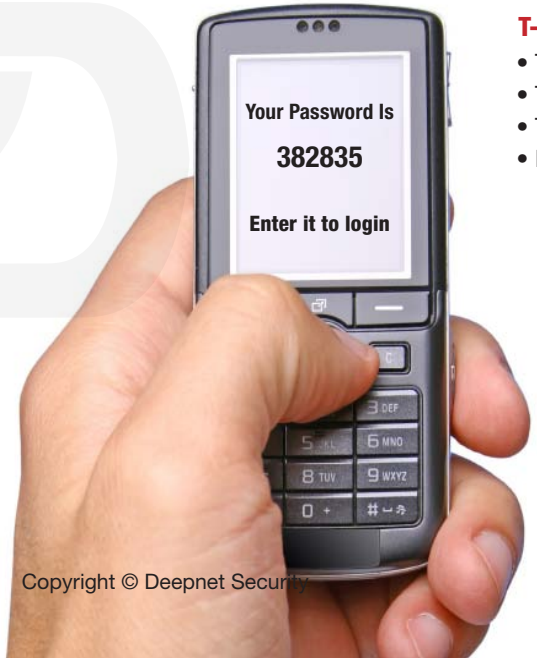
DUALSHIELD
UNIFIED AUTHENTICATION

Copyright © Deepnet Security

Mobile T-Pass

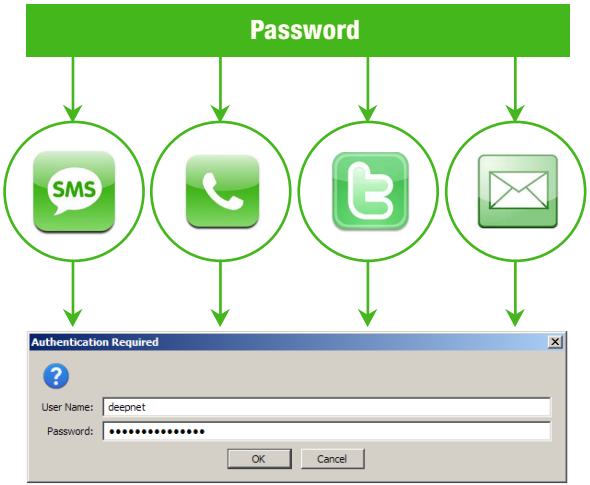
T is for Text, Telephone and Twitter. Mobile T-Pass is a token-less, on-demand one-time password authentication solution that delivers passwords to your phones via SMS text, voice, twitter or email messages.

T-Pass is one of the most user friendly and cost effective two-factor authentication solutions. It does not require any hardware deployment or software installation, therefore saves business customers the cost of administration, user education and technical support.



T-Pass supports

- Text (SMS)
- Telephone (Voice)
- Twitter
- Email



Copyright © Deepnet Security

SafeID

SafeID is a compact security device that generates one-time passwords with a single press on a button. It is available in various form factors.

SafeID 100

Event based. A “green”, life-time token with a renewable battery.

- OATH Compliant (HOTP)
- Size: 54 x 28 x 15 mm
- Battery: Replaceable

SafeID 200

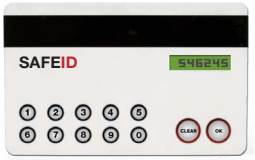
OATH TOTP compliant, time based. A compact, durable security token.

- OATH Compliant (TOTP)
- Size: 61 x 28 x 12 mm
- Battery: 3-5 Years

SafeID C100

OATH HOTP compliant, event based. In the credit-card or ID card form factor with an e-ink display window.

- OATH Compliant (HOTP)
- Size: Credit Card
- Battery: 3 years



SafeID C112

OATH HOTP compliant, event based. In the credit-card or ID card form factor with a 12-button PIN pad.

- OATH Compliant (HOTP)
- Size: Credit Card
- Battery: 2 Years

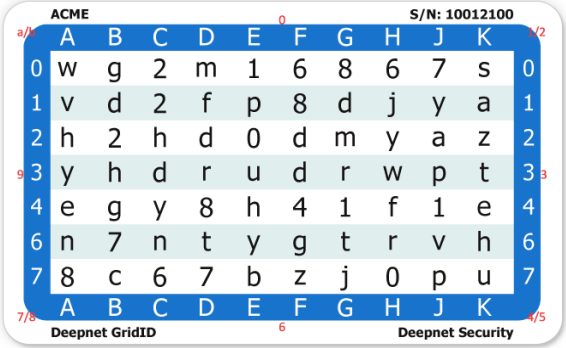
DUALSHIELD
UNIFIED AUTHENTICATION

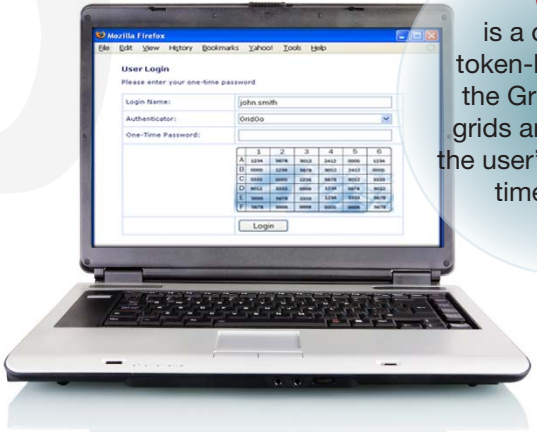
Copyright © Deepnet Security

GridID & GridGo

GridID is a simple, effective two-factor authentication method based on security grids. A security grid contains a matrix of numbers and letters in easily marked columns and rows. These security grids are typically printed on credit card-sized cards that can be easily carried in user's wallets, or they can be printed on the back of employee access badges, credit cards or ATM cards.

To perform strong user authentication with a security grid, users are required to provide a one-time password generated from their security grid.





GridGo is a on-demand, token-less version of the GridID. Security grids are delivered to the user's screen in real time at logon.

PIN Protected

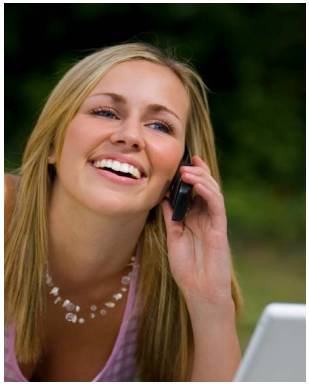
Users can protect their security grid cards with a PIN or password. At each logon, users generate a one-time password by randomly selecting a start point in the grid and navigate in the grid on a secret path that is only known to the users. The secret navigation path is encoded and easily memorized as a PIN or password. This unique, patent-pending technology protects users' credentials even when their security grid cards have been lost or stolen.

Copyright © Deepnet Security

TypeSense - VoiceSense - FaceSense

TypeSense is a software-only authentication solution based on typeprint recognition that uses keystroke dynamics to accurately identify a user by the way they type characters across a keyboard. TypeSense does not need to install any new hardware – it works with the standard computer keyboard. TypeSense is the only biometric authentication that:

- can be changed or reset
- is completely transparent to the user
- does not require special hardware
- can be quickly deployed to millions of users



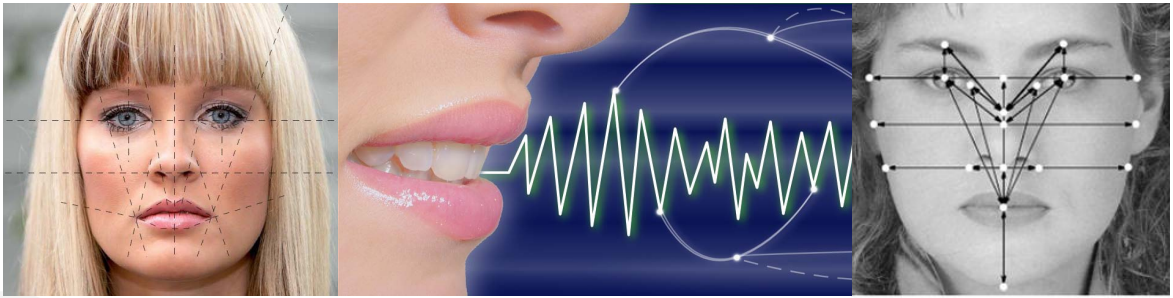
VoiceSense is a text and language independent biometric speaker verification system that verifies the speaker's identity in real time using a simple spoken phrase. VoiceSense is also totally independent of the language and accent that the user speaks in.

Voice authentication is an easy-to-use, versatile yet non-intrusive technology. It is highly accurate and doesn't require specific equipment. The ubiquitousness of PC microphones and mobile phones makes the voice authentication an ideal two-factor authentication system for enterprise, online banking and telecom applications.

FaceSense is a state-of-the-art authentication solution based on facial recognition technology. It is probably the most natural way of verifying the identity of a person. FaceSense does not require any advanced hardware, as it uses existing image capture devices such as webcams and mobile phones with a built-in camera.

Copyright © Deepnet Security

MultiSense



MultiSense is a Multi-Biometrics authentication solution that combines and fuses 3 different biometric technologies: face, voice and speech recognition, into one system. The use of Multi-Biometrics takes advantages of the capabilities of each individual biometrics while overcoming some of the limitations of a single biometrics, therefore improves accuracy, system robustness and fault tolerance.

MultiSense is a Multi-Factor authentication solution by itself and yet simple and easy to use. Users can logon to applications by simply looking at the camera and speaking a single phrase.

- **User Friendly:** Use a single device, webcams or mobile phones with cameras, to capture samples of multiple biometric traits, ie. Face images and voice samples.

- **Resistant to Spoofing:** Request the user to recite a random pass phrase, thereby ensuring that a 'live' user is indeed present at the point of logon

Copyright © Deepnet Security

DevicePass & FlashPass

Each computer device has its own unique characteristics. DevicePass creates a unique “deviceprint”, a digital fingerprint of the device, using the device’s characteristics including hard disk ID, CPU serial number and network MAC address etc. Combining the deviceprint with a user name and password, web and enterprise applications can restrict access to only trusted devices and authenticated users.

DevicePass provides a token-less, transparent way to achieve strong, two-factor authentication.

FlashPass transforms a standard USB flash drive into a security token, binds the user’s identity to the USB drive’s hardware fingerprint.

FlashPass does not require end users to install any software onto their PCs or laptops. Users can simply plug their USB keys into any computer, and will be immediately authenticated.

DUALSHIELD
UNIFIED AUTHENTICATION

Copyright © Deepnet Security

VPN/RADIUS Authentication

User Authentication is the weak link in VPN security. VPN technology is secure but only on the level of data transmission. VPNs typically verify users with only a static password, an approach that offers minimal security as passwords can be easily compromised. Strong user authentication is the only proven method for making VPN remote access secure. Deepnet Authentication for VPN, utilizing one-time passwords generated by portable authentication tokens in a variety of form factors, offers the ultimate security for VPN remote access without compromising the user's experience.

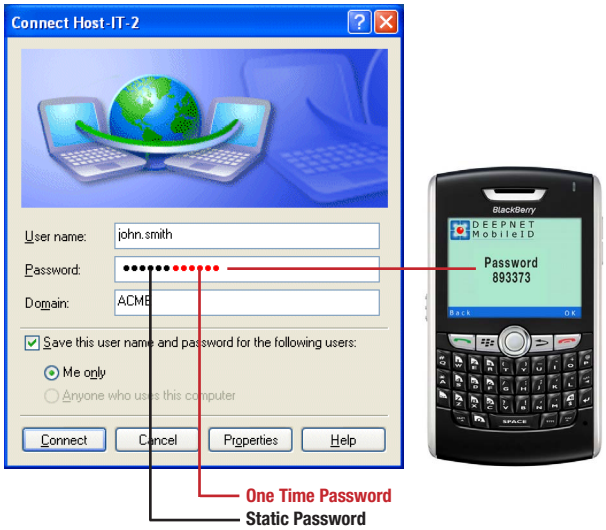
Deepnet DualShield provides a built-in, RFC 2865 compliant RADIUS server. It supports any Network Access Server (NAS) or application that employs RADIUS authentication protocol.

Seamless VPN Integration

Deepnet Authentication for VPN integrates with any IPSec and SSL VPN that supports RADIUS, including:

- Cisco
- Nortel
- Checkpoint
- Juniper
- WatchGuard
- Aventail
- SonicWave
- AEP
- Whale
- F5

Using one-time password, the end-users do not need to install any new software. They will use the same VPN client as they're using now, and simply enter a one-time password or a combination of their static password and one-time password in the place where the password is required.



Copyright © Deepnet Security

Windows/Linux Authentication

Deepnet Authentication for Windows is designed to help enterprise customers ensure that network resources are accessible only by authorized users, whether working locally inside the firewall or remotely via remote desktop. It is a complete solution that reinforces the Windows network domain logon as well as workstation logon with two-factor authentication.

Support:

- Local Access
- Remote Desktop
- Terminal Server
- Active Directory
- Windows 2000, XP, Vista, Windows 7
- Windows 32-bit and 64-bit
- Online and offline logon

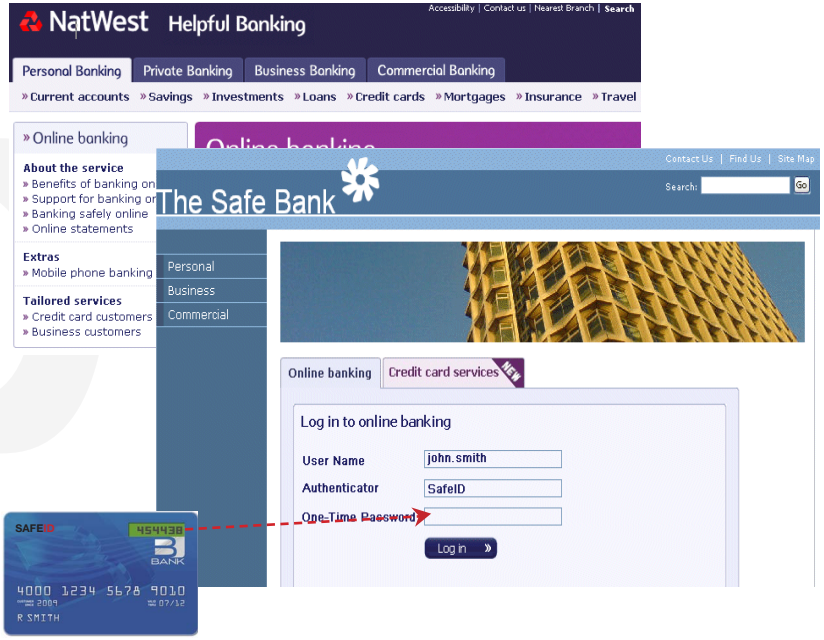
Linux systems and applications that support PAM can also authenticate against DualShield

DUALSHIELD
UNIFIED AUTHENTICATION

Copyright © Deepnet Security

Web Authentication

Deepnet Authentication for Web is designed to help e-commerce and enterprise customers control the access to restricted areas and contents on web sites. It allows access only to those users who provide two-factor authentication using a variety of strong authentication tokens provided by Deepnet and/or third-party vendors.



DualShield provides an SDK/API that allows third-party developers to seamlessly integrate two-factor authentication into custom web applications

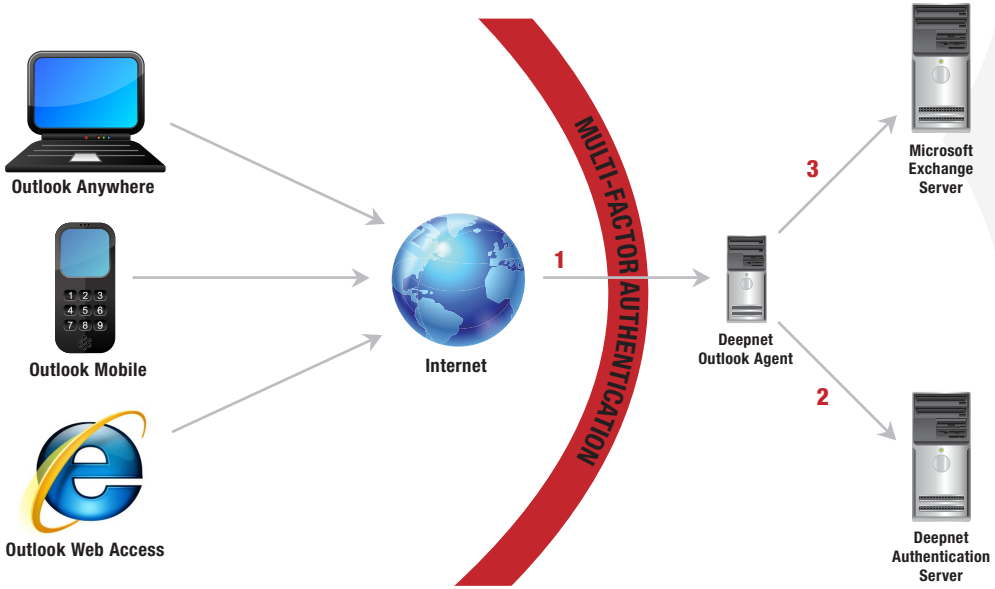
WEB

Copyright © Deepnet Security

Outlook Authentication

Deepnet Authentication for Outlook helps enable secure access to the following Outlook solutions:

- Outlook Web Interface
- Outlook Anywhere
- Outlook Mobile with Exchange ActiveSync



DUALSHIELD
UNIFIED AUTHENTICATION

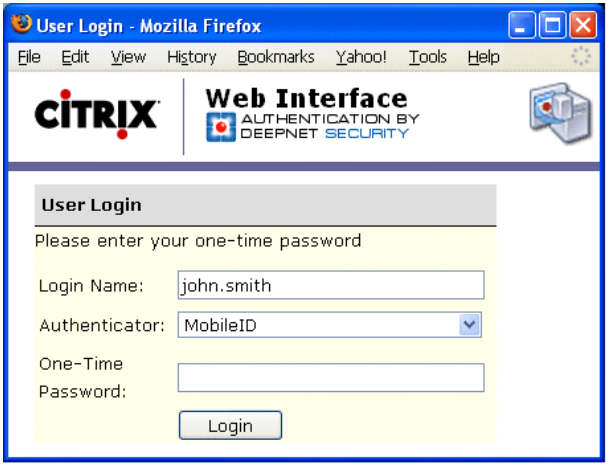
Copyright © Deepnet Security

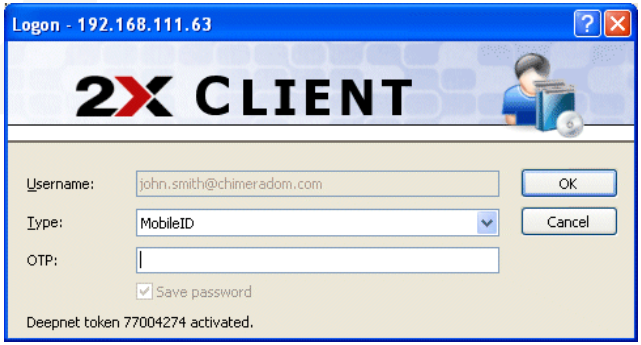
Citrix & 2X

While the Citrix solutions have made it easier for users to access critical information, simply using passwords to authenticate users can put a company at risk. Deepnet DualShield enhances security for Citrix solutions by authenticating users with a strong two-factor authentication system.

Deepnet DualShield helps enable secure access to the following Citrix solutions:

- Citrix Web Interface for Presentation Server
- Citrix Access Gateway with Advanced Access Control
- NetScaler SSL VPN





2X provides a family of enterprise server based computing software that allows desktop virtualization and application streaming on standard PCs and thin client devices.

Natively integrated into the core of 2X system, Deepnet Authentication enhances security for all 2X solutions by authenticating users with a strong two-factor authentication platform.

Copyright © Deepnet Security

"The solution was easy to install and manage, easy to use and provided good support for token and authentication options. The price is very attractive for environments large or small." – ***SC Magazine***

"Of all the different two factor authentication methods we've researched, this is by far the best…" – ***CoinCo Inc***

"We began a process of trialling and reviewing the various options; this included Deepnet, RSA and other major competitors. During these trials we found that the flexibility and ease of use offered by the Deepnet Unified Authentication Platform met our requirements far better than the competition…" – ***Teign Housing***

"We looked at a number of solutions including Secure Computing, RSA and Swivel. Deepnet provided the most flexibility with the number of applications that could be secured and the amount of ways a user could authenticate…" - ***NHS***

DEEPNET SECURITY

Partners

TELESIGN

2X ...oath... initiative for open authentication

Customers

NHS, Telefonica, Redbanc, flybe.com, Ladbrokes, MetroGAS, Imperial College London, American Safety Council, connexions, COINCO, TeignCare, Fulton Hogan

and hundreds more...

Deepnet Security
www.deepnetsecurity.com
info@deepnetsecurity.com
US: +1 714 937 2051
UK: +44 208 343 9663