PASSWORD BOUNCER™

ADVANCED PASSWORD POLICY ENFORCEMENT

Prevent the costs of security breaches by eliminating vulnerable passwords

Overview

The reality of hackers, compliance legislation, and recent world events are forcing organizations to make their environments more secure through password strengthening policies. Preventing vulnerable user passwords significantly reduces the chance of security breaches that inevitably result in costing your organization time, money, privacy, and reputation. Password Bouncer eliminates all weak passwords from being used by your end users as old passwords expire and new ones are entered.

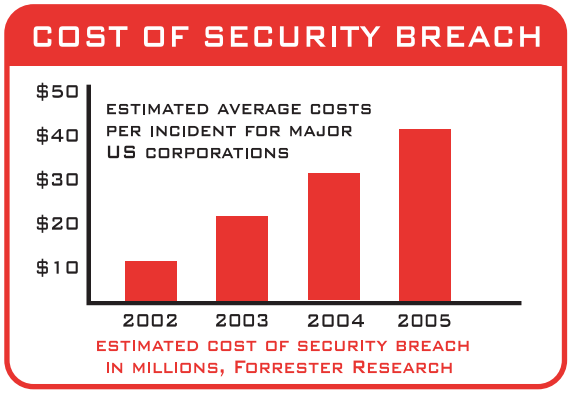
How Password Attacks Occur

The security industry has determined that 70% of all deployed firewalls are not effectively protecting the networks behind them. More telling is that 70% of all network compromises occur behind the firewall by a user or hacker attacking other user accounts.

Most users are prone to selecting simple, easy-to-remember passwords that contain only letters or digits. Simple human behavior innocently reduces the effort required to compromise a password. A smart hacker can simply apply guesswork to gain unauthorized network access by using spouse and child names, birthdays, anniversaries, etc.

More insidious are freely available utilities that automate what is commonly known as a Dictionary attack. These programs compare common words from several dictionaries to compromise a user's password. Should a hacker gain access to an administrative password and the Domain Controller's SAM, all passwords on the network are threatened -- from the mailroom to the boardroom.

Using these methods, the hacker can crack virtually any password given enough processing power and time. The key is to harden the password, so that by the time it can be compromised, it has already changed due to a globally enforced password policy.



Lower Costs Today

The cost of a security breach can be calculated based on estimates of lost business due to unavailability of the breached information resources; lost productivity while the IT staff tries to contain and repair the breach; labor and material costs associated with the IT staff's detection, containment, repair and reconstitution of the breached resources; plus labor costs and legal costs associated with the collection of forensic evidence and the prosecution of an attacker. Password Bouncer can prevent even the most minor network compromise and will immediately result in savings that far offset the total cost of the product.

Strategic Benefits

Improve security

User account passwords are the network's principal line of defense against intrusion. Studies have repeatedly shown that 70-80% of all network damage is done with a user that has been authenticated inside a network. Password Bouncer prevents the use of vulnerable passwords on your network, which eliminates the threat of a compromised account being exploited.

Improve total cost of ownership

Password Bouncer delivers enhanced password security without requiring any modification to the user's desktop. Password Bouncer eliminates the cost, time, and support overhead of intrusive desktop solutions by managing passwords at the domain controller. Users access the native password change window, which eliminates the need for any additional training or costly deployment tasks.

Rapid return on investment

Preventing even the most minor network compromise will immediately result in savings that offset the cost of Password Bouncer, which is the most effective insurance a company can buy. Password Bouncer eliminates the need to constantly audit and discipline users with weak passwords, which saves hundreds of hours of administrative time each year.

Provides continuous network protection

Passwords are proactively screened at the time they are changed and when new users are created.

Enhances existing security

Password Bouncer™ provides additional password policy rules not found in the native operating system, which allows administrators to significantly harden password choices.

Delivers immediate enterprise protection

Password Bouncer's rapid installation and policy distribution engine provides immediate password strength and cross-platform support.

Reduce help desk costs

Password Bouncer Deluxe Edition includes Policy Publication™, which allows current password policy settings to be published to an Intranet site for access by the user community. Updates to Password Bouncer policies are immediately reflected in the Policy Page, so users are able to view current policies when creating their new password.

Installs in minutes

Password Bouncer seamlessly integrates with Microsoft Security technologies and can be installed, configured, and deployed in under an hour regardless of the size of your organization.

AVATIER™

PASSWORD BOUNCER

Feature Comparison Matrix

Features	Native Windows NT/2000's Strictest Rules	Password Bouncer Deluxe Edition
System Password Policies		
Set Password Expiration Length	✓	✓
Set Minimum Password Age	✓	✓
Set Minimum/Maximum Password Length	✓	✓
Set Password Uniqueness	✓	✓
Password Strength		
Force Mixed Case	✓	✓
Do Not Allow NT User ID	✓	✓
Do Not Allow Any Part of User's Full Name	✓	✓
Do Not Allow Palindromes		✓
Do Not Allow Repeating Sequences		✓
Do Not Allow Alpha or Numeric Sequences		✓
Require a Number in a Specific Location		✓
Do Not Allow a Number at the Beginning or End		✓
Must contain one or more Numbers		✓
Require a Special Character in a Specific Location		✓
Do Not Allow a Special Character at the Beginning or End		✓
Must contain one or more Special Characters		✓
Supports Authorized Special Character List		✓
Policy Scope		
Manage Multiple Domain Password Policies from Single Console		✓
Exclude Specific Users from the Password Policy		✓
Apply Password Policy Only to Specific Users		✓
Dictionary Policies		
English Wordlist Filters - 300,000 words		✓
Custom Wordlist Filters with Wildcard support		✓
Proper Wordlist Filters - 4,000 - names		✓
Spanish, German, French, Italian Wordlist Filters - 483,000 words		✓
System Features		
Automatic Password Policy Domain Controller Distribution		✓
Automatic Password Policy Web Publication		✓
Transparent Password Synchronization with Password Station		✓
Cross-Platform Support with Password Station		✓

AVATIER™ IDENTITY MANAGEMENT SERVER

Design Advantages

- **Pre-Integrated into AIMS™ - Avatier's Identity Management Server (AIMS™)** has **Password Bouncer™** pre-integrated and available for license activation to enforce strong passwords from **AIMS™** web interfaces. This cross-platform server is a centralized solution with modules for account creation, self-service password management, and account termination. Organizations can institute a stronger password policy within the **AIMS™** platform, but can also enforce the same policy on any active directory account password change made from the users desktop.

- **Highly configurable - Password Bouncer™** includes very granular password policy rules that allow for highly configurable combinations of required password complexity.

- **Enforce strong password policies -** Extend existing security policies by allowing administrators to establish stronger password policies that:
  - Reject passwords that contain common words using language specific dictionaries
  - Reject passwords that contain proper names using a 4,000 name wordlist
  - Enforce additional custom wordlists with wildcard support
  - Enforce the use of upper and lower case characters (mixed case)
  - Enforce the use and position of special characters
  - Enforce the use and position of numeric characters
  - Reject passwords that contain palindromes
  - Enforce password length: minimum and maximum
  - Reject passwords with repeating sequences or characters

- **Automatic password policy publication -** whenever you establish or modify your password policies, **Password Bouncer™** will automatically generate a publishable internal HTML page that clearly explains the policy and requirements.

- **Eliminates common words - Password Bouncer™** has the ability to filter out the use of over a million common words, names from five languages, and from a custom word list. By eliminating the use of common words and names from passwords, **Password Bouncer™** will have taken the single most effective step forward to improving password security.

- **User feedback to prompt compliance and policy understanding - Password Bouncer™** will notify the **AIMS™** web interface user of what is needed to create a strong password should the one they enter fail the policy. This feedback is detailed and gives the user the necessary information to create their password to meet the network policy.

- **Achieve ease of use -** Password screening is automatic and invisible to the user. The optional change password applet alerts the user to the first rule their rejected password violated and links them to the published password policy for reference.

- **Maximize scalability -** By operating as a function at the domain controller and with the ability to filter for over a million words in less then 0.5 seconds, **Password Bouncer™** accommodates the largest environments. Multiple domains may be managed from a single console of **Password Bouncer™**.

- **Decrease frustration -** Secure password policy does not need to be a source of constant frustration for users or management. Following the **Password Bouncer™** Implementation Guidelines will ease your user community into the routine of selecting secure passwords while eliminating the individual conflicts with those who have repeatedly struggled to follow the written corporate policy.

Security Advantages

- **Act proactively -** Passwords are proactively screened at the time they are changed by the user. Unlike password scanning tools that only let you know after the doors have been left open, **Password Bouncer™** bars those doors against security breaches due to vulnerable passwords.

- **Make network security a priority for everyone -** Protecting the investment that organizations spend on securing the perimeter of their networks, the internal security on the network ("the user's password") is of paramount importance and requires the cooperation of everyone from the CEO to the temporary employee.

- **Improve security -** User account passwords are the network's last line of defense against intrusion. Studies have repeatedly shown that 70-80% of all network damage is done by users who are already inside the firewall. **Password Bouncer™** prevents the use of vulnerable passwords on your network, which eliminates the threat of a compromised account being exploited.

- **Overcome human nature -** Users will trade network security for convenience by choosing simple and easy-to-remember passwords, even if a strong written policy is in place. **Password Bouncer™** takes the decisions about your network security out of the hands of the users and puts it back with security management where it belongs.

Lower Operational Costs

- **Realize rapid return on investment -** Preventing even the most minor network compromise will immediately result in savings that offset the cost of **Password Bouncer™**, which is the most effective insurance a company can buy. By ensuring that ALL the passwords on your network are secure, **Password Bouncer™** eliminates the need to constantly audit and discipline users with weak passwords, which saves hundreds of administrative hours each year.

- **Eliminate desktop deployment costs -** Enhanced network password security can be instantly achieved without requiring any modification to the users' desktop. **Password Bouncer™** eliminates the cost, time, and support overhead of altering the user experience by screening passwords at the domain controller. Users access the same familiar native password change window, which eliminates the need for any additional training.

"Password Bouncer enabled us to immediately strengthen our password policy and protect our company's vital assets..."
Denny Goldberg
Senior Network Analyst
5,000+ Employee Insurance Provider

Customer Showcase

Platforms Supported

Password Bouncer seamlessly integrates with Password Station to deliver password protection for the following platforms:

Platforms		Supported Versions
Operating Systems		
	Microsoft Windows NT/AD	4.0, 2000, 2003
	Microsoft Windows Server	4.0, 2000, XP, 2003
	Sun Solaris	2.6 and above
hp	HP/UX	11 and above
AIX L	IBM AIX	4.3 and above
	Redhat Linux	7.1 and above
	SUSE & Other Linux	All Versions
IBM	iSeries (IBM AS/400)	V4R5 and above
IBM	zSeries (IBM OS/390)	V2R8 and above
hp	Digital VMS and Tru64	7.3-1, 5.1 and above
Directories		
RSA	RSA SecurID ACE/Server	5.2 and above
	Sun Java System Directory	4.2 and above
N	Novell NDS	4.01 and above
N	Novell eDirectory	6x and above
9i	Oracle Internet Directory	All Versions
	Microsoft ADAM	All Versions
IBM	IBM Directory Server	3.x, 4.x, and 5.x
	OpenLDAP	2.1 and above
Databases		
	Microsoft SQL Server	7.0 and above
9i	Oracle	8.x and above
	Sybase	10.x, 11.x, 12.x
IBM	IBM DB2/UDB	6.x, 7.x, and 8.1
IBM	Informix	7.x, and 9.x
Applications		
Lotus.	IBM Lotus Notes	R4 and above
9i	Oracle E-Business Suite	8.x and above
PEOPLE Soft	PeopleSoft	8.x and above
SAP	SAP	4.5B, 4.6C, and 4.7

Minimum Requirements

Hardware

Password Bouncer Administration Server:

- 400 MHz CPU speed or higher
- 256 MB RAM
- 10 MB for program files and auditing database
- Monitor capable of displaying 16-bit color or greater and a resolution of 800 x 600 or higher

Software

Password Bouncer Administration Server:

- Microsoft XP Professional, Windows NT 4.0 Server, Windows 2000 Server, Windows 2003 Server Standard Edition. When managing either a Microsoft Windows NT or Active Directory domain, we recommend making the Password Bouncer Administration Server a member in at least one of the managed domains.
- Can run on domain controllers
- Live Internet connection is required to register the product
- A component gets installed on each PDC of all domains where Password Bouncer enforces password policies. Microsoft Active Directory requires a component to be installed on every Domain Controller
- The Password Bouncer Service must have access to the Admin$ share on every Domain Controller
- The Password Bouncer Service must have read/write access to System32 and the Registry of each Domain Controller
- Microsoft Windows NT 4.0 requires a reboot of the NT 4.0 Primary Domain Controller.
- Microsoft Active Directory requires a reboot of each Domain Controller

Password Bouncer Client:

- Microsoft Windows 2000 Workstation or Server
- Microsoft Windows XP Professional
- Microsoft Windows 2003 Workstation or Server

Contact

Worldwide Headquarters
Avatier Corporation
12647 Alcosta Blvd, Suite 400
San Ramon, CA 94583

925-217-5170 main
925-275-0853 fax
800-609-8610 sales

info@avatier.com
www.avatier.com
www.passwordbouncer.com

powered by AVATIER IDENTITY MANAGEMENT SERVER