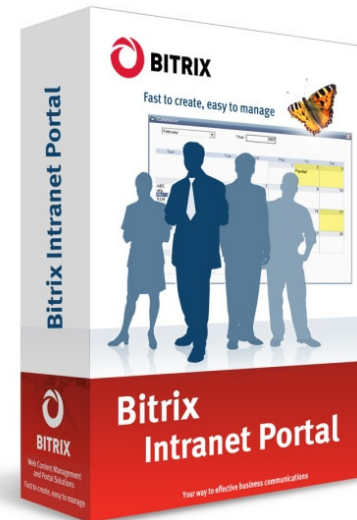




INTRANET PORTAL AND CONTENT MANAGEMENT SOLUTIONS

Bitrix Software Security

Powerful content management with advanced security features





INTRANET PORTAL AND CONTENT MANAGEMENT SOLUTIONS

Internet Security 2009 Quick Facts*

- **210,000** websites are attacked every month on the Internet
- **\$234,244** is your approx. loss count if your website is shut down by hacks
- The number of hacker attack attempts sky-rocketed **671%** in 2009
- **41%** of companies are not satisfied with their web security

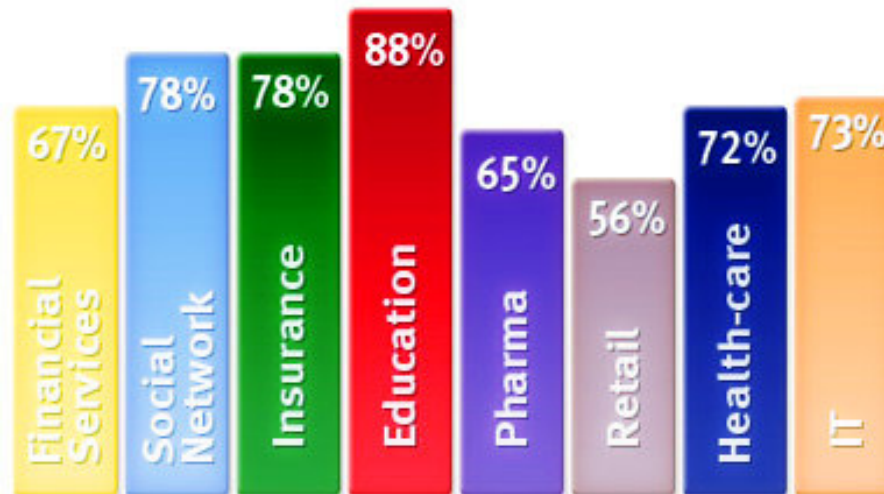
*According to Dasient, White paper "Drive-by-Downloads, Web Malware Threats, and Protecting Your Website and Your Users", <https://wam.dasient.com/wam/info?prod=18>



INTRANET PORTAL AND CONTENT MANAGEMENT SOLUTIONS

Is Your Company Vulnerable to Hacker Attacks?

Every day your website or corporate portal could be attacked many times, damaging the integrity of your web project. Data leaks, phishing and unauthorized access to your website pose a real threat to your company, making up-to-date security mechanisms mandatory. Here's a look at the industry vulnerability chart:



Industry Vulnerability Chart

Percentage of websites susceptible to security threats, by industry.
Source: White Hat Security, "Website Security Statistics" by Trey Ford.



INTRANET PORTAL AND CONTENT MANAGEMENT SOLUTIONS

Main Reasons for Data Leak / Data Loss:

Data leak due to

- Inappropriate access permission distribution
- Unauthorized user account registration
- Weak or inflexible moderation policy
- Phishing attempts from within
- Weak protection from external threats
- Lack of internal dataflow monitoring techniques
- Delay in virus and web threat security updates

Data loss and data damage due to

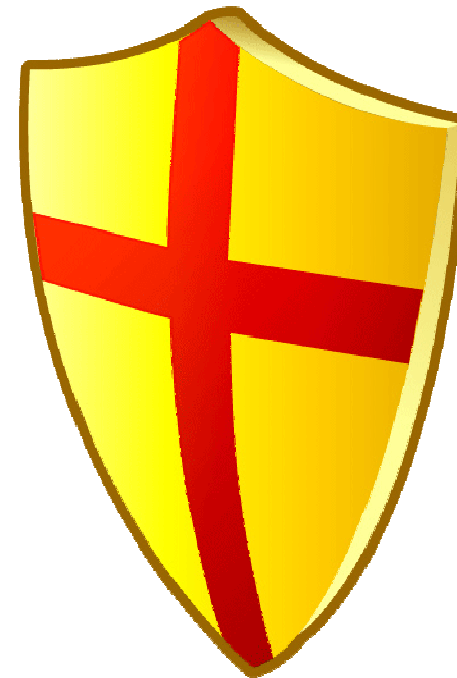
- Weak login/password protection
- Inflexible authorization policy
- Non-adjustable session lifetime
- Easy access to the website root
- Harmful web-code implants
- Inappropriate notification system
- Incoherence of web-code elements



INTRANET PORTAL AND CONTENT MANAGEMENT SOLUTIONS

How Can Bitrix Products Protect My Web Presence?

Bitrix Site Manager and Bitrix Intranet Portal include the **PRO+PRO™** Security Framework that provides maximum protection from thousands of threats that can be encountered on the Internet or originate locally because of inappropriate web project security policies.





INTRANET PORTAL AND CONTENT MANAGEMENT SOLUTIONS

PRO+PRO™ Framework Highlights:

The PRO+PRO™ framework incorporates a number of technically advanced security technologies. It uses multiple security levels, allowing you detect and combat almost all known hacking techniques. The PRO+PRO module features:

- Security Dashboard
- Proactive Filter / FireWall Web Application
- One Time Password technology support
- Protection of authorized sessions
- Activity Control and Intrusion Log
- IP-based Protection Mechanism
- Script Integrity Control
- Stop Lists and Security Logs



INTRANET PORTAL AND CONTENT MANAGEMENT SOLUTIONS

PRO+PRO™ Offers Preconfigured Protection Levels:

Basic Level

assigned to all web projects running without the Proactive Protection module; only basic security features are provided.

High Level

customized for projects conforming to higher security requirements (standard level + kernel module event logging, storing sessions in the database, etc.)

Standard Level

uses most common proactive protection features (everything offered by the basic level + proactive web filter, intrusion log, activity control, CAPTCHA, error log, etc.)

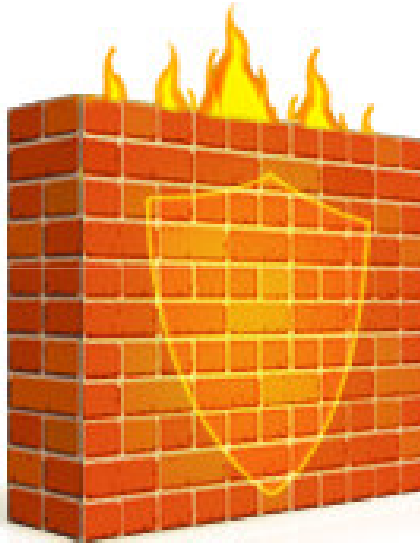
Highest Level

assigned to all projects requiring maximum protection from internal/external threats (all high level security features + OTP support, control script integrity verification, etc.)



INTRANET PORTAL AND CONTENT MANAGEMENT SOLUTIONS

Web Application Firewall



The firewall filters incoming website requests for malicious code, hacker attacks and suspicious activity like buffer overflow. Protects against XSS, CSRF, SQL injection and File Include attacks.



INTRANET PORTAL AND CONTENT MANAGEMENT SOLUTIONS

Web Anti-Virus



- An elaborate web antivirus system
- Shields websites against harmful HTML-implants
- Detects 90% of potential infection threats
- Notifies administrator upon location of dangerous code
- Detects and reports incoherent code elements
- Includes a "white list" to reduce false positive alerts



INTRANET PORTAL AND CONTENT MANAGEMENT SOLUTIONS

One-Time Passwords (OTP)



A hardware token generates a series of digits which the user adds to his password at each log in. This means that the password will be different with every new session. Even if a third-party illegally acquires your password, it will not be possible to use to authorize on your website.



File Integrity Log



This feature allows you to detect any changes that could have been made to the system files. Administrators can verify the integrity of the system kernel, system files or public files anytime. The File Integrity Log helps you identify unauthorized changes, thus preventing intrusion attempts.



Script Integrity Monitor

File integrity control

- Tracks file system changes
- Verifies kernel integrity
- Verifies system area integrity
- Verifies public files integrity

Verification of the file integrity control script

- Verifies the file integrity control script for changes
- Protects the script using the keyword and password pair



Intelligent System Backup



This backup feature protects the website from a range of risks from server hardware failure to malware infection. When a website gets infected, it is nearly impossible to eliminate all the bits of malicious code. They are usually spread over all the site content and manual eradication would require too much time. With a backup in place, you can simply restore the original non-infected version.



Anti-Phishing Protection



Phishing – an illegal attempt to acquire private information (usernames, passwords, credit card details, etc.) that is made through a routine activity performed on a website that is thought to be trustworthy. The PRO+PRO module allows you to stop redirection to potentially dangerous websites, offering your website visitors even more safety.



INTRANET PORTAL AND CONTENT MANAGEMENT SOLUTIONS

Flexible Access Management



PRO+PRO Security Framework leverages the power of a variety of mechanisms for protection from the external threats and an advanced user permission management system. These features combine to allow customized access permission to sections, pages and even page objects in a most flexible manner.



INTRANET PORTAL AND CONTENT MANAGEMENT SOLUTIONS

Automatic Updates



Bitrix products offer click-away security updates with real-time notifications about new patches and bug-fixes available. All updates affect only the system core and will not cause any data change in the public view part (front-end) of your web project.



INTRANET PORTAL AND CONTENT MANAGEMENT SOLUTIONS

PRO+PRO Crash Test 2009



More than six hundred Russian hackers tried to invade the brand-new Bitrix PRO+PRO™ security framework as part of the "Bitrix Real-Time Hack Competition". The test was organized during the "Chaos Constructions CC9 Festival" in August 2009. During the competition, more than 25.000 attacks on the Proactive Protection security mechanism were repulsed, proving its superb reliability!



INTRANET PORTAL AND CONTENT MANAGEMENT SOLUTIONS

More Information about PRO+PRO Framework:

Bitrix PRO+PRO Security Framework Overview:

<http://www.bitrixsoft.com/products/intranet/security.php>

Bitrix Web Anti-Virus Main Features:

<http://www.bitrixsoft.com/products/intranet/security.php#tab-antivirus-link>

Bitrix Proactive Protection Guide:

http://www.bitrixsoft.com/download/manuals/en/security_tutorial.pdf

Bitrix SiteUpdate System Overview:

<http://www.bitrixsoft.com/products/intranet/siteupdate.php>



INTRANET PORTAL AND CONTENT MANAGEMENT SOLUTIONS

Thank you!



Sales Department: sales@bitrixsoft.com

Website: <http://www.bitrixsoft.com>



www.bitrixsoft.com