

“If one of your servers gets compromised, how would you know?”

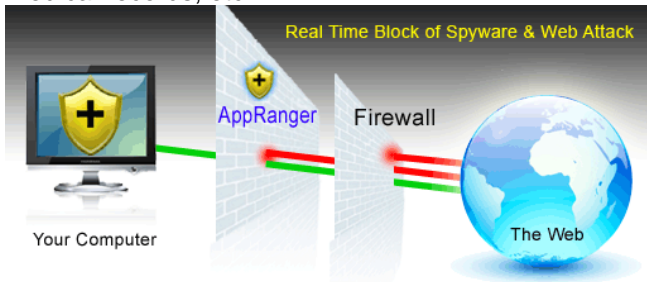
Servers are Extremely Vulnerable

Application servers are the backbone of corporate network. They are also the prime targets of hackers.

Hackers break into application servers such as web server, e-mail servers, database servers etc. by exploiting vulnerabilities in applications that run on them.

For example, a hacker can exploit flaws in Microsoft exchange server software to take control of the server. Now the hacker has access to all corporate e-mail. That information can be used to send more SPAM. Compromised server may be used to run an illegal website that shares porn and music.

Application servers are targeted because these servers have significant amount of disk space, bandwidth, and computer power available. These servers also act as aggregation point for corporate data and that gives hackers access to potentially very confidential and valuable data, such as credit card numbers, bank accounts, social security numbers, medical records, etc.



Gartner states that 75% of today's hacks occur at the application level. This number is expected to rise and by 2009, 80% of companies will have suffered an application security incident.

If a server is hacked, how do you know that it got hacked?

When a server gets hacked, the compromise may go undetected for a long time. Often the hacks are discovered when the server performance degrades significantly, e.g. running out of disk space, excessive

CPU or bandwidth usage etc. By that time, significant damage has already been done.

What makes these hacks difficult to detect is the stealthy nature of malware. Polymorphic malware change signatures frequently to evade signature-based detection methods. Advanced heuristics based detections are also ineffective as malware are using intractable problems like the NP-complete problem to obfuscating code.

Rootkits go a step further. They subvert the operating system and very frequently anti-virus software fails to detect any trace of their presence.

In many cases, hackers only change the configuration of the server, e.g. runs a web server. Because there is no malicious software installed, a scan will not indicate that the server has been compromised.

Stealthy malware and malicious use of good applications present very significant hurdles in detecting server compromise.

Cleaning the Servers

Even if malware has been detected and identified, cleaning servers is an extremely difficult task.

Malware such as SmitFraud, Aurora, Look2Me etc. cannot be cleaned by anti-virus products because they regenerate themselves. Often anti-virus products will not be able to clean the server and one has to resort to rebuilding the computer.

This is not an acceptable solution for servers because unlike desktop computers, servers can't be rebuilt frequently. Therefore, the ability to clean them and to keep them clean is crucial.

AppRanger uses two unique technologies to unmask and remove malware. **AppRanger's** "Kernel Heal" technology unmarks all rootkits. Then **AppRanger** uses "Malware Freeze" technology to prevent malware from regenerating and removes them. **AppRanger** authenticates all software running on the server and therefore one can have complete confidence that the server has been cleaned thoroughly.

Zero-day worm attacks can be rapidly brought under control by **AppRanger** even if a patch for the zero-day exploit is not be available. To defeat such worms, **AppRanger** enforces a lockdown after cleaning the servers. The servers do not get re-infected and can continue to perform their designated tasks.

Locking Down the Servers

AppRanger uses a two pronged strategy to prevent servers from getting infected.

First, **AppRanger** sandboxes applications that are exposed to outside world and hackers.

The sandbox protects applications against exploits targeted towards server applications. Any attack coming in via the application will be contained and neutralized by the sandbox. **AppRanger** automatically detects and protects common server applications such as IIS, Apache, Exchange, etc.

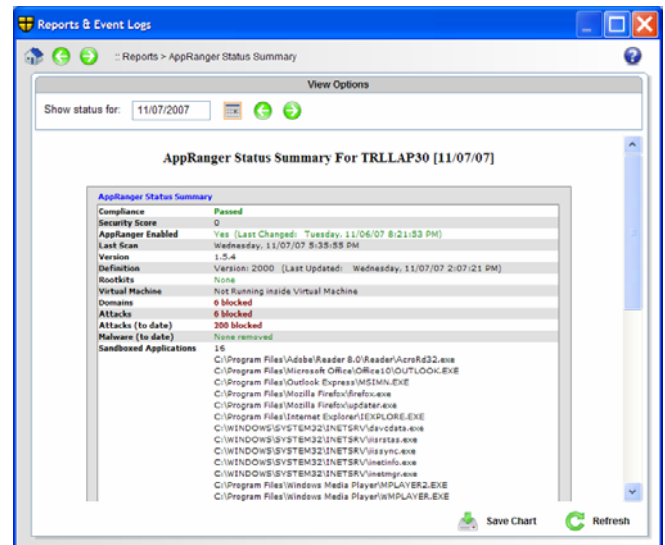
Second, **AppRanger** enforces full lockdown on the server.

When the lockdown is enforced, only authorized application can be executed and system changes are blocked. Any unauthorized application will neither be able to start nor will it be able to damage the computer. For example, during a worm attack, enforcing the lockdown will prevent the worm from re-infecting the servers even if the patches are not up to date.

Even if the lockdown is not enforced, **AppRanger** tracks daily changes to the servers. Tracking changes coupled with application behavior monitoring can pinpoint the time and date of hack.

Achieving Compliance

AppRanger helps in meeting compliance requirement like PCI, HIPPA, etc. Report generated by **AppRanger** directly answers some of the main issues that must be addressed to meet compliance requirements. **AppRanger** also serves the dual purpose of "risk assessment" and "protection."



System Requirements

32-bit operating systems

Windows 2000, Windows 2000 server, XP, Windows server 2003, and Vista.

For a **FREE** trial version of **AppRanger** email us at Support@appranger.com

Or visit

www.appranger.com

AppRanger

602 E. Huntington Drive, Suite F
Monrovia, CA 91016

USA

Tel: 626-357-3706

www.appranger.com