PROTECT YOUR APPLICATION SERVERS

Preserve uptime by blocking attacks and unauthorized changes
Preserve uptime by blocking attacks and unauthorized changes

The Situation

How often have you sat through the painstaking process of determining why a mission-critical application server has crashed? Have you scrambled to restore access to applications while fielding phone calls from your user community complaining that a critical SAP, SharePoint, or ERP application is down and they cannot conduct business? Did that server crash because of a rogue application being installed? Did it crash because of a system change that did not go through a change control process? Was it malware that brought down the server?

These are the questions that administrators must answer in order to explain to management why there was downtime, lost productivity, and lost revenue for every hour critical applications were unavailable. These fire alarm situations are occurring more often as the threats, vulnerabilities, and usage modes of application servers evolve. Hackers are willing to work hard today to get at these business assets—to cripple key applications or to use the application server to connect to rich databases. In addition, harried administrators and ever-more-frequent patches have increased the chance of configuration mistakes or the introduction of software before full integration testing has been completed.

Driving Concerns

Application servers can be conduits to sensitive data processing applications such as credit card transactions, regulated and confidential customer information, or health records. Application servers are also financial systems, human resources applications, hosted web applications, and middle tier servers to front end web servers or backend databases.

To many organizations, these servers are mission-critical applications that cannot be down. If your application server environment is seeing an increasing number of outages and application misbehavior, it is time to implement select protections that will help isolate these systems from vulnerabilities, attacks, and unexpected changes. From a security perspective, this progress starts with gaining an understanding of where the threats exist, how they are changing, and what can be done to mitigate them. The following security issues are today’s top causes of downtime for application servers:

• **Vulnerabilities.** Mitigating risk from vulnerabilities through consistent application and server OS patching can be a challenge in any organization. Patches need to be reviewed and tested, and there is usually a brief and rare change management window when patches can be deployed. While this process takes place, application servers remain at risk. Vulnerabilities that exist either within the application or in the operating system running under the application server can leave the application server open to network-based attacks such as eavesdropping or DoS/DDoS attacks. Gateway attacks to front or backend systems exploit SQL or web server vulnerabilities with code injections. These vulnerabilities might be mitigated if appropriate shields were in place at the perimeter, but many firewalls and intrusion detection devices are outdated, or so noisy that their protective capabilities have been neutered.

• **Malware.** Malware can attack a vulnerable system that does not have proper antivirus technologies. Malware can spread through an open port on the server or a vulnerable system service. If an application server is not properly hardened, an attacker or some form of malware can make its way into an unsecured port or vulnerable service and gain access to sensitive data.

• **Application server change management.** Without proper testing prior to implementation, any changes made to an application server can have an adverse effect on the server. Many organizations lack a proper mechanism to monitor changes and prevent unapproved changes.
• **Unauthorized software and processes.** Similarly, new features or patches installed without sufficient testing and validation often upset a previously stable configuration. Malicious executables use this tactic, too.

• **Management complexity and compliance processes.** Application servers come in all flavors. No two organizations are alike and nor are their application server deployments. Application servers can be hosted on various platforms such as Windows, Linux, or Solaris. This could introduce a certain level of complexity from a security perspective, since the administrator will need to ensure that the security technologies they use are multi-platform aware and provide unified auditing, enforcement, and management in a manner where they can ensure compliance across all platforms.

**Solution Description**

To achieve optimal application server security, McAfee recommends a multi-layer security approach that begins with basic security fundamentals and moves up to more advanced security implementations for total security protection. Taking this approach allows for IT security administrators to clearly define what their security strategy should be for application servers and how they can ensure success in mitigating their risk.

• **Protection against vulnerabilities and exploits.** The solution must provide proactive protection against malicious code, buffer overflow attacks, and exploits to give your organization gap protection while the operating system undergoes the patch management lifecycle. At the perimeter, technologies should provide a first line of defense to application servers by inspecting the traffic before it hits the server, mitigating attacks such as DoS/DDoS attacks or man in the middle attacks and shielding against known vulnerabilities.

• **Malware protection.** Antivirus solutions should include proactive protection via signature and heuristic based detections. Heuristics and real-time reputation assessment should provide additional zero day protection for the malware that signature-only detection may not recognize. Malware protection should include access protection functionality for basic firewall, port, and process control over the application server.

• **Enforcing change management.** Change control processes including continuous file integrity monitoring should help your organization meet requirements such as PCI. The solution should identify and alert on violations, such as when a file or registry is modified and then changed back, and capture specific details about every change including the exact time of the change.

• **Preventing unauthorized application and process execution.** To protect the integrity of the application servers, automated systems should block the installation of unauthorized software as well as the execution of malicious or unauthorized code. It should limit execution to an approved list of applications and processes specific to each server. The technology should include the ability to create trusted updaters, so applications installed on the application server can receive product updates without manual intervention.

• **Management complexity and compliance processes.** Security management of multiple application server platforms should be managed under a single management infrastructure. Organizations can benefit from a standardized set of policies and visibility across multiple, disparate application server platforms. Understanding where vulnerabilities, exposed services, and weak passwords exist on an application server can give you a good compliance baseline, helping to focus efforts to get the application server infrastructure up to industry standards. Both administrators and auditors can quickly see where compliance policies are not being followed and take appropriate action.
Technologies Used in the McAfee Solution

McAfee uses reinforcing perimeter and server layers to protect application servers. Intrusion prevention system (IPS) technologies in the McAfee® Network Security Platform act as a first line of defense for traffic that traverses the application servers and other resources that tie in with it, such as web and database servers.

On the server, McAfee VirusScan® Enterprise offers antimalware for common application server platforms. In addition, some applications, such as SAP NetWeaver and Microsoft SharePoint, merit special attention. McAfee offers additional antimalware modules for these technologies through McAfee VirusScan for SAP NetWeaver and McAfee Security for Microsoft SharePoint.

To reduce disruption from accidental or malicious software installation or system changes, McAfee provides advanced memory protection and application whitelisting through McAfee Application Control and completes the protection lifecycle with total change policy enforcement through McAfee Change Control. McAfee Policy Auditor is integrated within the McAfee ePolicy Orchestrator® (McAfee ePO™) management platform to help you assess and monitor compliance as part of centralized management of your server protections.

Network IPS plus strong protection on each file and application server help to prevent downtime and data compromise.
McAfee Network Security Platform (NSP)
As a full-featured, enterprise-class intrusion prevention system, McAfee Network Security Platform can provide protection against a number of vulnerabilities that exist in the common operating systems underlying application servers. Many organizations opt to segment their application server farm on a separate vLAN or subnet. NSP will filter traffic before it reaches these servers, using both signature-based protection against the most common OS vulnerabilities and heuristics protection against zero-day vulnerabilities. This can help administrators prevent attacks that can exploit vulnerabilities on application servers without adding any additional overhead at the operating system level. NSP can accomplish this protection at wire speed without introducing any latency to the application server infrastructure.

McAfee VirusScan Enterprise
McAfee VirusScan Enterprise combines antivirus, antispyware, firewall, and intrusion prevention technologies to stop and remove malicious software targeting application servers. McAfee VirusScan Enterprise includes support for both Windows and Linux distributions. It detects malware using heuristics and signatures, plus real-time file reputations from McAfee Global Threat Intelligence™ (GTI) to evaluate suspicious files. Access protection rules prevent unwanted changes to your servers by restricting access to specified ports, files, shares, registry keys, and registry values and preventing unauthorized changes to VirusScan Enterprise. Buffer overflow protection protects against memory-based exploits that can affect critical servers. McAfee GTI guards against malware before signatures become available.

McAfee Security for Microsoft SharePoint
McAfee Security for Microsoft SharePoint (MSMS) extends specific protection for SharePoint components and services. When data is accessed, copied, or written to SharePoint servers, MSMS will proactively scan that content for malware, viruses, and Trojans to prevent compromise of the server's integrity.

With MSMS, you can ensure real-time protection when content is accessed and schedule deep scans of all data using the latest malware and content filtering signatures. You can minimize processing overhead by choosing to scan only new files or opt to limit full repository scans to scheduled maintenance windows or specific scan targets, including web applications, websites, folders, and specific file types.

McAfee VirusScan Enterprise for SAP NetWeaver
As your users upload, modify, and delete content in the SAP environment, they can introduce malicious content. To protect your organization’s critical SAP data, McAfee offers VirusScan Enterprise for SAP NetWeaver, which is designed specifically to scan for malware, viruses, and Trojans within the SAP NetWeaver environment. This allows organizations to mitigate risks that can affect data integrity on the SAP NetWeaver platform.

Like other McAfee server products, McAfee VirusScan Enterprise for SAP NetWeaver can be managed and deployed centrally via McAfee ePolicy Orchestrator.

McAfee Application Control
McAfee Application Control gives IT administrators the ability to prevent the unauthorized installation of software on application servers. Application Control uses a dynamic trust model, in which administrators have the ability to define which processes and applications are allowed to run, and which trusted sources can make changes. Application Control gives administrators the ability to tightly protect the applications hosted on the application server by only authorizing those specified application functions within the server. In addition, it extends coverage to Java, ActiveX controls, scripts, batch files, and specialty code for greater control over application components. It will also prevent buffer overflow attacks exploiting memory and vulnerabilities. Application Control supports Linux, AIX, Solaris, and Windows application servers.
McAfee Change Control
McAfee Change Control delivers continuous detection of system-level changes being made across the server and prevents unauthorized changes to critical system files, directories, and configurations. Change Control tracks and validates every modification to the application server and can track those authorized changes to change management tickets.

McAfee Policy Auditor
McAfee Policy Auditor allows administrators and auditors to map their internal policies and controls to predefined or customized policy content. Therefore, when you need to audit an application server you can easily define a benchmark, set an audit scan, and quickly retrieve a report stating if the server is in compliance with internal and regulatory policies. In addition, McAfee Policy Auditor can automatically schedule reoccurring audits to ensure application servers stay compliant. Waivers and blackout windows help prevent audits during critical periods.

To build policies, you can start with out of the box policy templates provided for major industry regulations such as PCI DSS, GLBA, HIPAA, and FISMA, as well as best practice frameworks such as ISO 27001 and COBIT. You can also import and build on regulatory benchmarks that support the Security Content Automation Protocol (SCAP). When benchmarks and policies change, download updates from authoritative sites such as NIST and view detailed security guidance to benchmarks.

McAfee ePolicy Orchestrator (McAfee ePO)
McAfee ePO enables centralized, automatic software distribution and policy management of McAfee VirusScan Enterprise, McAfee VirusScan Enterprise for SAP NetWeaver, McAfee Application Control, and McAfee Change Control, as well as reporting of McAfee Network Security Platform. McAfee Policy Auditor is integrated within the McAfee ePO console to make it easier to deploy policies and manage audit processes.

- The McAfee ePO extension provides the interface for configuration, scheduling, and security reporting for McAfee endpoint and server products
- The McAfee ePO agent on the application server manages policies and updates on the server and communicates with the McAfee ePO console and database
- McAfee ePO itself provides a “single pane of glass” for managing security for the enterprise, enabling monitoring and reporting across physical and virtual systems and protection tiers

Impact of the Solution
McAfee recommends bringing your application server security up to modern standards with protections that are resilient to threats and help you maintain security while minimizing disruption. These strong controls can reduce the alarms, alerts, phone calls, and management reviews that have forced your organization into a reactive security stance in the past.

By reducing the attack surface of your application servers, you minimize the opportunity for malware or hackers to take down your application server infrastructure. Perimeter protection from the McAfee IPS will fend off both known and breaking threats using advanced heuristics and McAfee Global Threat Intelligence. Server-based protection for your application servers, SAP NetWeaver systems, and SharePoint servers will layer additional malware protections around each server itself.

To prevent unauthorized or untested changes—software installations, patches, and malicious executables—to your approved configurations, McAfee offers dynamic application whitelisting and change policy enforcement systems.

By providing a single policy management environment across your server protections, integrated with the McAfee IPS for unified reporting, McAfee also targets the complex management and compliance rituals that hamstring productivity. Since auditing is integrated within the graphical console used for monitoring, compliance processes become less manual and more accurate. It’s possible to achieve and demonstrate continuous compliance with both internal and external controls.
Q&A

Can I create my own custom benchmarks with McAfee Policy Auditor?
Yes, Policy Auditor has full functionality to customize and create your own benchmarks for audits. You can also create rules from any scripting language supported by the system being audited to extend the check capabilities of policy agents further. Sample languages include VBScript, batch files, Perl, and Python.

What types of executable files can be whitelisted with McAfee Application Control?
With McAfee Application Control, you can whitelist a variety of executables such as .exe, .dlls, and scripts such as .js, .vbs, and .bat for Windows.

Can McAfee Application Control and McAfee Change Control be tampered with?
McAfee has built controls into both products that prevent users from disabling either McAfee Application Control or McAfee Change Control. This includes users with administrator rights to a server.

What if certain IT administrators need access to make changes to an application server while it is locked down with McAfee Application Control?
In the Application Control policy, you can define trusted users based on Active Directory domains. These users are allowed to make changes to an application server. Used in combination with McAfee Change Control, the activity conducted by that administrator can still be monitored to ensure that the administrator is not making any system level changes that can have an adverse effect on the application server.

How does GTI work in McAfee VirusScan Enterprise?
GTI will perform a DNS Query of a file hash of the suspicious file. If that file hash matches the GTI checks in the cloud, the appropriate action will take place to either allow the file or block the file depending on policy configurations.

Does McAfee Network Security Platform need to be deployed in-line on a network?
McAfee NSP can be deployed in several ways. If your organization simply wants to monitor but not block any events discovered by NSP, you can simply deploy it in SPAN or TAP configuration. However, if your organization wants to enforce the full blocking and mitigation functionality, then the device would need to be deployed in-line. All NSP appliances include full Fail-Open Kit support and High Availability configurations.
Additional Resources
www.mcafee.com/virusscan-enterprise
www.mcafee.com/virusscan-enterprise-for-sap
www.mcafee.com/nsp
www.mcafee.com/appcontrol
www.mcafee.com/changecontrol
www.mcafee.com/policyauditor

Risk and Compliance Overview Demo
www.mcafee.com/us/resources/demos/grc-demo.html

For more information about the Security Connected Reference Architecture, visit:
www.mcafee.com/securityconnected

About the Author
Joseph Fiorella is a senior security engineer at McAfee and based in New York City. Joseph has been involved in the information security field for the past 8 years. Since Joseph joined McAfee in 2009, he has been implementing and supporting security technologies for some of the largest Public Sector organizations in the North East. Joseph holds a Bachelor’s Degree from Pace University, as well as numerous certifications, such as Certified Information Systems Security Professional (CISSP), Security+, and Certified Information Security Manager (CISM). Joseph is an active member of (ISC)² and the New York Chapter of ISACA. Joseph is currently in the process of completing his Master’s Degree at New York University.