

McAfee Security Management Platform

Empower your team to secure the enterprise by Stuart McClure

Defending your enterprise against cyberattacks is like playing defense on your side of the field for the entire game. The opposition is relentless. Your team is highly skilled and hyper-vigilant. But you wonder if the tools they have are good enough to hold up against an increasingly intense and sophisticated onslaught. And, of course, securing the enterprise is no game. The stakes couldn't be higher.

Today, most enterprises manage multiple security products and layers of security independently. One threat after another is addressed by one tactical solution after another. So, for example, a spate of attacks on web servers triggers IT to purchase a web gateway product. Which is fine, but it's a short-term fix. The fact is, threats are proliferating by orders of magnitude faster than new products can be deployed and managed.

That's why McAfee now offers the McAfee® Security Management Platform. This strategic solution brings all of the various enterprise security components together in a holistic view of security, risk and compliance. The McAfee Security Management Platform coordinates security defenses, so that IT teams can focus on offense—that is, delivering the applications and infrastructure that organizations need to compete and win.

Putting It All Together

The McAfee Security Management Platform combines and refines key aspects of security so IT staff can manage the expanding scale of enterprise security more easily than ever before. The solution combines situational awareness and analysis, shared security intelligence, global heterogeneous protection, and an open platform approach that enables you to integrate security into core business operations. Briefly, let's look at these four areas one at a time.

Gaining Situational Awareness

Consider the role of a soccer goalie. This player is the personification of situational awareness—constantly assessing the risks of the moment and focusing on potentially serious threats far and near while ignoring likely diversions or nuisances. For great goalies, that ability is intuitive. For even the best IT professionals, it comes down to experience and their choice of software.

The situational awareness components of the McAfee Security Management Platform enable IT staff to monitor, prioritize, and report on security risks in real time. New capabilities include automatic asset discovery and synchronization that eliminate manual processes and security risks due to out-of-sync policies. Also new are situational policy assignments—logical groupings of policies that you can apply based on business need. Similarly, new selective threat and asset analysis capabilities give organizations the ability to reduce threat detection and response times. This is made possible largely by McAfee Risk Advisor, which proactively combines threat, vulnerability, and countermeasure information to pinpoint assets that are truly at risk.

Sharing Intelligence

The McAfee Security Management Platform includes new capabilities in global threat intelligence. Like the previous incarnations of this service, it tracks threats in cyberspace using real-time, reputation-based behavioral analysis. McAfee has been gathering this kind of intelligence for more than 15 years. But what's new with McAfee Global Threat Intelligence™ is that this reputation-based intelligence is now being shared across security solutions (endpoints, networks, email, web, and data, etc.) in order to provide coordinated defenses that minimize or eliminate security attacks.

Game-changing enhancements include the evolution of our reputation services and use of our cloud to hunt for threats proactively and prevent attacks long before they can exploit a company's network. McAfee is also making global threat intelligence available on the Apple iPhone and Apple iPad, enabling IT security professionals to have real-time access to threat information wherever and whenever they need it.

Information sharing is vital to your team's response. McAfee Security Management Platform customers can access the new McAfee Threat Center anytime. The "threat portal" enables users to search and drill down into threat information across eight dimensions: files, messages, IPs, URLs, web domains, DNS servers, applications, and vulnerabilities. There's nothing else like it in the world today.

Global Heterogeneous Protection

Physical and virtual. On-premises and the cloud. Servers and desktops. Laptops and smartphones. You should be able to pick your network, system, or device and go about your business unscathed. That's the idea behind global heterogeneous protection.

In virtualized environments, the key technology from McAfee in this category is Management for Optimized Virtualized Environments, or MOVE for short. An integral part of the McAfee Security Management Platform, MOVE enables deployment of McAfee VirusScan software at the hypervisor level for VMware virtual machines (VMs) and Citrix virtual desktop interfaces (VDI). So, running an instance of anti-virus software on every VM—and dragging down performance—is a task whose time has passed.

In addition, MOVE provides virtual server context awareness, allowing security management policies to follow the virtual machine they are protecting regardless of where the VM is provisioned or how often it is moved.

Last, but far from least, are the new guided configuration capabilities in McAfee ePolicy Orchestrator® (McAfee ePO™) software. These let IT staff install, configure, and generally get up and running more rapidly than ever before.

A Platform That's Open for Business

Wide open and ready for expansion. That's the McAfee Security Management Platform. New interfaces and software development kits (SDKs) provide an open platform for companies, developers, and partners to integrate centralized security management into existing business processes. Expanding on the integrated solutions already available from McAfee and partners involved in the McAfee Security Innovation Alliance (SIA), the McAfee Security Management Platform offers new integration capabilities.

Of particular note is the new web API for McAfee ePO technology that enables integration with systems management frameworks, such as Tivoli, Remedy, and HP Service Manager. In essence, the web API makes the McAfee Security Management Platform an extension of these frameworks by letting you create policies that trigger automatic threat protection responses on their consoles. McAfee Risk Advisor now includes an SDK that enables rapid integration of new security countermeasures—broadening the view of a company's risk profile and reducing operational costs. Strategic partners are also integrating McAfee Risk Advisor's IT risk profile information into their governance, risk, and compliance portals, enabling a comprehensive governance solution from business to IT.

It's a Whole New Ball Game

Pervasive, coordinated, and persistent. Those are the adjectives that best describe today's threats. But those words must also be applicable to enterprise security if it is to be effective. And that's why the integrated, enterprise-wide capabilities of the McAfee Security Management Platform are so vitally important.



Stuart McClure is Senior Vice President and General Manager, Risk and Compliance for McAfee, where he is responsible for sales, engineering, product management, product marketing, strategy, quality assurance, and customer support for the entire risk and compliance product line. Widely recognized for his extensive and in-depth knowledge of security, McClure is today one of the industry's leading authorities in information security. He is lead author of *Hacking Exposed: Network Security Secrets & Solutions*, which has been translated into more than 30 languages and is considered one of the definitive computer security books.

