Microsoft's FCS Only Partially Delivers the Goods

May 21 2007

Review: eWEEK Labs found that Microsoft's new Forefront Client Security package meets only the baseline requirements for an enterprise security solution.

Forefront Client Security marks Microsoft's initial foray into enterprise desktop security, and the product holds out the promise of anti-virus and anti-spyware detection and cleaning services that both integrate tightly in companies' existing network infrastructure and provide superior visibility into and reporting around these ongoing processes.

However, eWEEK Labs tests indicate that at this time, FCS only delivers on some of these promises.

In particular, eWEEK Labs found that while Microsoft's new offering meets the baseline requirements for an enterprise security solution, the case for FCS will sound most sweet when preached to an end-to-end Microsoft infrastructure choir.

FCS is designed to fully capitalize on Microsoft's burgeoning portfolio of management and reporting solutions, at least theoretically easing management through the use of existing systems. FCS relies on Active Directory for policy deployment, WSUS (Windows Server Update services) 2.0 or later for signature and software deployment, and MOM (Microsoft Operations Manager) 2005 for client monitoring and alerting.

Also, FCS requires a full blown version of SQL Server (rather than

MSDE or SQL Server Express) to provide robust reporting and data collection services.

Companies with a heavy investment in Active Directory Group Policy and in WSUS should find FCS a cozy match for their environments. However, companies that have deployed third-party management or patching alternatives might be better off giving FCS a pass, as the product totes with it a plethora of potentially redundant systems.

What's more, we found in our tests that FCS' detection capabilities still have a ways to go before they match the performance of more entrenched anti-virus players. For instance, we were not impressed with FCS' detection rates and we discovered some isolated incompatibilities that could hamper the FCS testing process. Even from a management perspective, we were taken aback by how many different application consoles we needed to consult while operating and maintaining a FCS deployment.

Another drawback to FCS is that its client support is more limited then we'd like. Foresight can be installed on Windows XP with SP2, Windows Vista or Windows 2003, but does not work with Windows 2000 (or earlier operating systems).

However, from a visibility standpoint, Microsoft's FCS scored well with us. We appreciated the way that FCS' modular design helped set apart the product's excellent reporting capabilities from its data collection and policy deployment functions, thereby keeping information flowing even while our test network was under attack.

According to customers we consulted during our review, Microsoft's support services for FCS also shine, exceeding customer expectations in helping decipher, detect and clean previously unknown infections and outbreaks.

But solid reporting and helpful customer service aside, FCS has significant hurdles to clear to diffuse negative public perceptions that began to take root before the product was even released, due to the fact that FCS is based on the same underlying technology as Microsoft's much maligned, consumer-grade Windows OneCare Live.

Earlier this year, OneCare Live suffered a series of public blunders, performing poorly on several independent malware detection tests and, worse, incorrectly quarantining entire mail stores rather than individual messages or attachments. Competitors like Symantec have not been shy about calling Microsoft to the mat for these failings.

Microsoft is working diligently to remedy this image problem by gaining certifications from respected anti-virus research groups. Forefront Client Security has already garnered West Coast Labs' Checkmark certifications for wild list virus detection, wild list cleaning and Trojan defenses on Windows XP, 2003, 2000 and Vista-based systems. FCS is also undergoing the certification from ICSA Labs, which has already given clearance to OneCare Live.

Pricing for Forefront Client Security, which started shipping this month (May), is based on a subscription model, with recurring charges for both the client and central management components, but no upfront cash outlay.

Client agent prices start at $1.06 per user (or per device) per month, while the Security Management Console component costs $205.66 per month. Volume discounts are also available. Considering that Management Console licensing fee includes the costs for the SQL Server 2005 and MOM 2005, we found the pricing to be more than competitive. The licenses for these components are restricted solely for use with FCS, however.

Management

We were somewhat disappointed with FCS' disjointed management facilities, which for us fell short of the integrated, cohesive and simplified management experience for which Microsoft is aiming.

Rather, as we moved back and forth between the management consoles for WSUS, Active Directory, MOM and FCS itself, we felt that we were straddling too many disparate applications for comfort. We hope to see Forefront's management story becomes better aligned as Microsoft moves to an MMC-based management approach for WSUS 3.0.

However, the Microsoft Forefront customer who we interviewed during our review disagreed with this perspective. Kevin Hayden, Desktop Engineering Manager for Analog Devices, of Norwood, Mass, indicated that his team does not spend much time in the MOM console, for instance, except when trying to isolate an alert.

According to Hayden, after initial setup and trials, Forefront management was a pretty simple, single console affair. What's more, Hayden told us that the inclusion of MOM gives his staff a leg up on a client operations management project they have in the works.

Disparate management perspectives aside, one thing we can say for sure is that with all software components that FCS requires, administrators of the product will have to throw some significant hardware at their Forefront deployments.

For a single server configuration that hosts all elements of the Forefront Client Security platform, Microsoft recommends at least a dual 2.85 GHz CPU server with 4GB of RAM. Forefront's component prerequisites may be split among up to six different servers, separating out the reporting, collections, management, distribution server

components as well as the reporting and collection databases.

Like Hayden, however, we opted for a two-server setup, using an existing WSUS 2.0 server while hosting all other elements on a single machine.

Microsoft's decision to utilize WSUS and Windows' Automatic Update client to deliver both the client software packages as well as malware signatures seems to us an odd match to fit the needs of a signature-based security solution.

A WSUS server is only designed to synchronize with Microsoft Update servers on a daily basis, and Automatic Updates is only designed to install software once a day. During tests, we found Microsoft released new signature files between three to six times a day, so WSUS and Automatic Updates—at least in their default configurations—fall short.

Fortunately, Microsoft has addressed these shortcomings by providing a component for installation on the WSUS server that bumps synchronization frequency to once per hour. Along similar lines, Foresight's client software component triggered more frequent update checks.

Companies that have chosen a third-party patch delivery system will likely be loathe to install and maintain WSUS on top of their existing systems, not to mention re-enable Automatic Updates on their clients. Microsoft does offer signature file downloads from their Web site, and these files can be installed manually or with a script—this, however, is hardly an ideal solution given the frequency of signature updates.

Moving forward, we expect to see third-party patching vendors offer scripts or other mechanisms to automate this process for their own customers, which would make life easier for companies out to mix

Forefront with non-Microsoft patching products.

During our tests, we configured FCS updates by visiting the WSUS console, enabling WSUS synchronization and approving the signature files and FCS client installation package to push out to our Windows endpoints. We also configured WSUS to automatically accept, download and deploy future updated signature files.

Before we could begin deploying Forefront's components to our clients, we had to visit a separate interface, the FCS Management Console, to create a security policy to govern the process. Forefront's security policies allowed us to centrally control whether to engage anti-virus or anti-spyware defenses, enable heuristic detections, schedule scan times, or create exemptions (either file folders or file types).

We could also schedule periodic security state assessments, providing a Baseline Analyzer-type scan to look for missing patches, unnecessary services, compromiseable passwords .

After we'd created our policies, we were ready to deploy them via Active Directory. From the FCS console we assigned one of the policies we'd drafted to a Security Group or an Organizational Unit, which triggered the creation of a new Group Policy Object consisting of a number of specific registry changes, which Foresight then automatically linked to our targeted AD object.

We could also assign the FCS policy directly to an existing GPO or we could copy it to a file for manual distribution using FCS's command-line policy distribution tool.

Reporting

The FCS console presents a dashboard with executive-level view of the

deployment, presenting at-a-glance insight into the ratio of clients reporting issues versus those without problems and those who have not reported in recently.

The dashboard also presents quick links to create a variety of summary reports that provide a top-level view of infection status with total systems affected, aggregate malware reports and enterprise-wide security state assessments.

We particularly like the Deployment Summary report, which breaks down the status of policy deployment, spyware and anti-virus signature distribution, and client engine deployment onto a single page, and even singles out some of the information on a per-security policy basis.

From these high-level reports, we could quickly drill down to more specific details and instances as needed by administrators tasked with resolving the problems, for instance identifying exactly what patches are missing and unnecessary services are present from a specific machine on the network.

The reports are initially presented as a Web page, but we could easily export reports to XML, CSV, Excel or PDF formats. Using the included MOM reporting Engine, we could access the same reports as above plus a few others, or design our own reports with the SQL Report Builder. We found we could use the MOM report engine to schedule periodic snapshot reports to provide regular insight into ongoing system behavior.

Detection

In our malware detection tests, we quickly noticed that FCS real-time file system did not initially work in our tests using virtualized client instances. For instance, with all protections enabled, we were able to download our malware bundles to the virtualized client's hard drive

either from the Web, a file share or a thumb drive.

Fortunately, the real time protections worked as expected on a Windows XP-based laptop client, and we suspect that FCS does not interact in an expected fashion with VMware's virtualized disk drives. Although this circumstance is certainly not a deal breaker, it may hinder the FCS testing process in some organizations. During a disk sweep, FCS did detect 10 different malware strains infecting 14 of our sample files. The Windows Filter Manager, meanwhile, helped block the installation of these infected bundles before they could take root on our system.

However, our malware test suite consisted of 29 different executables known to contain malware (a mix of viruses, adware, trojans, and other malware)—which added up to a lackluster sub-50 percent detection rate. We verified this by individually submitting the samples to www.virustotal.com, which ran each of our samples through 31 different scanners and assessment solutions.

But even this marginal success was tempered by some buggy behavior. When we found the malware with our manual scan, we noticed the icon in the system tray changed from its usual state (green check mark) to a warning (a red x).

When we closed the client interface without choosing a course of action to clean the found infections, we discovered that the next time we opened the interface, the system tray icon had reverted to a green check mark, and the history contained no mention of the previous scan's findings. Findings were correctly reported to the central console, however.

Hayden acknowledged that FCS has not yet coped with some minor threats (like toolbars) around his network as well, but he was quite happy with the software's performance nonetheless. FCS had already detected

many malware instances around his network that Analog's previous solution had missed.

But more importantly, Hayden said Microsoft's Premier Support Services were ready to assist when an outbreak hit the network. Microsoft's team even went so far as to accept a full disk image to help isolate an unknown infection, something his previous AV vendor was unwilling to do.

By Senior Technical Analyst Andrew Garcia
Copyright 2007 by Ziff Davis Media, Distributed by United Press International