

Bit9 Parity 5.0 shines brightest among competitors with strong protection and useful risk metrics

By Roger A. Grimes | InfoWorld

NOVEMBER 04, 2009

As many product vendors can readily tell you, this reviewer is the ultimate computer security cynic and a tough writer to please. I'm unsparingly critical of overhyped products. Although I've evaluated a number of excellent products over the years, I've never given a perfect 10 in any scorecard category -- until now. Bit9 Parity is one of the few computer security products that, if deployed in your Windows environment, will radically and immediately reduce your enterprise's level of security risk. It's not perfect, and it did not score a perfect 10 in every field -- but it earned the highest score this reviewer has ever given.

Started in 2002 from a NIST grant, Bit9 Parity is the most mature whitelisting product in this review. It provides broad coverage of Windows clients and file types, and its functionality and features assist users with making the right trust decisions needed to secure their environment.

Bit9 Parity's server console, called Parity Center, runs on Windows Server 2003, with IIS enabled and a Microsoft SQL Server database. The Parity client supports Windows 2000 and later, including embedded versions. Bit9 Parity comes linked, like SignaCert, to a cloud service with more than 7.5 billion legitimate and malicious files predefined and hashed.

Machines can be scanned to create baseline rule sets, and individual files and folders can be whitelisted or blacklisted. Where Bit9 takes application control to a new level is in rating identified files as to their trust and risk, based upon hash, digital signature (if included), software category (if known), and location. All reported client hashes are compared against known malware and legitimate vendor files.

For example, if a managed, trusted user downloads Apple iTunes, it may violate corporate policy, but not necessarily be a real security risk to the enterprise. However, a known malware program or unidentified file would be marked as higher risk. Bit9 Parity's risk and trust ratings allow you to discriminate between the merely noncompliant, such as iTunes and Picasa, and a security threat, such as the Fiasco virus. It's important to note that Bit9 doesn't automatically decide what is the appropriate treatment for a particular risk level; it just reports the result and lets the administrator define the policy.

Bit9 Parity has three main policies and an emergency mode. In Monitor mode, users are allowed to execute anything, but all executions are monitored. In Block & Ask mode, users are asked to approve executions of unknown programs. And in Lockdown mode, execution of all unknown and unapproved programs is blocked. Emergency Lockdown mode returns to a previously more secure state, blocking all execution of originally unapproved programs across all managed machines, regardless of whether trusted users later whitelisted them.

Test Center Scorecard						InfoWorld
	Accuracy/ Effectiveness	Coverage	Administration	Reporting	Value	Overall Score
	30%	15%	25%	10%	20%	
Bit9 Parity Suite 5.01	10	8	9	9	10	9.4 EXCELLENT

Each policy can be tied to a computer, user, group, organizational unit, or other Active Directory component. Parity can be integrated into McAfee's ePolicy Orchestrator administrative console, and it works with multiple patching products.

Software can be pre-approved in the same four ways shared by most competitors: Trusted Directories/Paths, Trusted Users, Trusted Publishers, and Trusted Updaters. Files marked for approval by Trusted Users or policy can have their whitelisted status subsequently revoked, either globally, on a per-user basis, or anywhere in between. Protected files can be protected against unauthorized writes, renames, or moves. Like some of the other products, Parity can pinpoint all the places where a particular file resides. If Parity can identify the file, it can also tell you the category (for example, Hacking Tool) when it was installed, and by which user.

But here's where Bit9's software gets really interesting. Parity can report overall risk, based upon individual file risks, for each managed computer. SignaCert achieves something similar with its Authenticity score rating, but that has more to do with the legitimacy of a particular file than its potential risk to a system. This feature of Bit9 Parity not only raises it above the other products in this review, but above most computer security products in general. Administrators can run reports to see which computers are at highest risk in their environment and then work to resolve those outliers first.

Another statistic, called Drift, indicates how many program executions have been approved by a trusted user for files not previously whitelisted on the baseline image. If a computer drifts too far away from the baseline or incurs too much risk, the previously trusted user can be confined to Lockdown mode. This sort of real-time assistance alone deserves a top rating. But Bit9 also gives IT the means to improve risk and drift numbers over time, and to report real, consequential, or diminishing security risk to upper management.

I haven't mentioned many of the other features that raise Bit9 above the competition. First, Parity allows bulk imports of previously defined blacklists to block file executions even before the first instance of a file has reared its ugly head. Second, if a trusted user installs or executes a new program offline, away from the managed network, even if the user uninstalls it before reconnecting, the event is reported to the central console upon the next network connection. If possible, newly identified software is categorized: Browsers, Entertainment, Hacking Tools, IM, Media Players, P2P Apps, Photos, Security, and so on. All the hashes in a client's environment are rechecked every week because software classified one week as something legitimate could become less trusted the next. Did I mention that control over mobile devices and licensing is included for free? A few competitors offer similar functionality, but for additional cost.

While Parity's client-side alerts for blocked execution are only slightly above average, the program rises above the pack with excellent alerting, thresholds, and reporting on the administrative side. Alert templates -- including file activity, system activity, malware, licensing, and elevated privileges -- can be used to define alerts and triggered alarms on nearly any monitored behavior at any desired threshold. One of my favorites is the Block Propagation Alert (a Spread Check in Lumension), which alerts administrators to an unexpected wave of users installing a particular file. It could be a legitimate upgrade or a crafty Trojan horse program.

Parity's central console also has dozens of reporting reviews, including charts and drill-down data, as well as the unique risk and trust ratings I've already applauded. Naturally, ratings can be customized.

Bit9 Parity doesn't corner the market on every unique whitelisting feature, and it's missing a few of the cool features found in some competitors, such as the inline blocking of buffer overruns found in CoreTrace Bouncer and McAfee Application Control. Nonetheless, its trust and risk ratings mark it as the whitelisting program to have.