What did we have in place before and Why?	Cisco Security Agent. We had used it for many years on Windows XP to stop the frequent malware infestations.
What products did we look at? (Both what philosophies and what products) and why?	We discussed the ideas around privilege elevation and application whitelisting and decided that since we had success with whitelisting we'd stick with it. We looked at Microsoft AppLocker and Bit9 Defender.
Product Name	Bit9 Defender
What influenced your decision?	Completeness of product, customer references, demonstration and proof of concept.
Once a decision was made, what did we think we were getting?	We had done a proof of concept so we felt comfortable that we were getting a very good solution. We knew we wanted a solution at least as powerful as CSA but easier to manage on a day to day basis and with better reporting.
What did we REALLY get?	We got what we had hoped. Bit9 is working as advertised, the only times we've had issues with Malware were related to poorly conceived rules. The ongoing management is minimal and the reporting is excellent.
What did it take to get there?	It took a lot of work, configuring the product, inventorying the machines, preparing allowed and not allowed lists, testing, evaluating results, retesting, etc.
What did we learn along the way?	Whitelisting was not new to us, but there was still plenty to learn. We learned that even with CSA there was a lot of unapproved software running because the helpdesk was at times willing to suspend the CSA engine for users without much prodding. We've since tightened the process for adding new entries to the whitelist.
Has it met our expectations?	It really has. Our users are much happier because we can more easily manage exceptions and because Bit9, unlike CSA, allows for regular updates like iTunes, flash, etc. to run without interference.
What do we do going forward	We are actively looking at the CarbonBlack add-on to Bit9 which provides the ability to do detailed reporting for incident response. CB keeps an eye on each end point and records the interactions between all components and can "replay" attacks.