

Securing the Bank from the Inside to the Outside

In medieval times, a castle and its treasures were protected by building a moat. It is not surprising that this traditional way of thinking about security remains the focus for many organizations today. There are a range of outside service organizations that bring advanced perimeter capabilities to even small community banks which lead it to feeling safe.

But the perimeter cannot stop the malicious insider or worse, an insider whose computer unbeknownst to them is bypassing perimeter defenses to launch or propagate malware across an organization. Once inside a bank, the custom targeted malware is often free to roam and connect to the outside because it is deemed to be safe or trusted.

What's disturbing of late is the growing sophistication of attacks which are increasingly able to fool perimeter defenses. The insider threat has become equally as significant as the threat of the outsider.

There is a range of well established security practices required to provide end-to-end protection for community banks. These technologies are relatively basic (reset passwords periodically), well known and often required to be compliant. We won't enumerate those here since we assume that your auditors and you are painfully aware of them. Unfortunately the bad guys are just as well aware of these technologies as well.

A new technology for making security ubiquitous throughout the organization is application whitelisting. It operates within your bank, your castle, protecting your employees from becoming compromised or pawns of the bad guys. It allows permitted applications to run, but denies unknown executables (exes, dlls, etc.), including custom malware that bypasses perimeter or antivirus security, from running.

With Savant Protection's Application Whitelisting software, community banks are now able to protect endpoint computers from malicious attacks such as keyloggers, bots and other advanced persistent threats. Since Savant only allows permitted executables to run, a bank can protect its users from drive by downloads and malicious payloads buried inside of seemingly legitimate attachments, PDFs and other files. In addition, Savant's unique approach to protecting and updating endpoints also prevents a compromised computer from spreading its malware and doing further damage to the bank.

Savant Protection is not based on heuristics but reality since only authorized programs are allowed. The result, the people in the bank can do their jobs, accept documents, and visit web sites, without fear of compromise. Plus, IT benefits because it does not have to spend time fighting fires by rebuilding compromised and slow machines peppered with unauthorized executables and spyware. Savant Protection is a layer of defense that complements your perimeter security in a way that was not possible in the past.



Paul Paget
CEO

Paul Paget joined Savant Protection as the CEO to drive the company's strategy and plan for establishing a leadership position in the market. A veteran of the information security industry, Paul enters Savant Protection with 30 years of high tech experience with companies ranging from startups to the Fortune 50. He brings a strong leadership background and a successful track record in growing and guiding security software companies, and has extensive experience managing sales and service organizations. Previously, Paul served as President and CEO of Core Security Technologies where he launched the Core IMPACT product and successfully built Core into the market leader in automated penetration testing with over 600 customers in more than 40 countries. Prior to Core, he was SVP of Operations for Baltimore Technologies Americas where he grew the company to a \$30+ million dollar business. Paul joined Baltimore via the acquisition of GTE CyberTrust, where he was Worldwide Vice President of Sales and Marketing. Paget holds a Bachelor's degree in History from Bowdoin College and has completed management, technology and executive education with IBM, GTE and the University of Michigan.

