Georgia Institute of Technology Drives Nowell Software 05/08/2009

I view the Nowell software as having several potential uses which have a natural overlap. Nowell monitors and learns how a user is using various applications and the times at which they are used.

Two routes can follow can follow from this data collection, one is reporting exclusive of security considerations, how a machine is used or how a user operates a machine.

This data can be used to learn which applications are most used and at what times of the day the machine and its applications are used. This data can be reported per machine, per user or per group of machines to yield statistical information for planning and purchasing. The same data can also be used forensically to determine if a machine, group of machines or a single user is making proper use of the machines applications or if the applications are being used excessively or at inappropriate times of the work day.

Should a particular machine and it users be determined to require significant security concerns, the machine and user can be trained and monitored by Shalom to enforce a high level of defense against intrusion and simultaneously providing a audit trail of application use by those with qualified access to the machine.

Use Cases and Enhancement Areas

A few detailed possible uses and enhancements are listed below:

1. Track and report which application is being used and by whom
2. Track and report how many apps are being used
3. Report how much time the users are spending in different applications and information resources
4. We should be able to graphically quantify how a user is using a machine
5. Quantify how an enterprise network is using the information resources and detect anomalies on an enterprise level
6. Screen Blanker time out with Shalom interrogation for reactivation for high security machines that require restricted viewing of the screen or access to records, ie. HIPAA
7. Develop a VM "Virtual Machine" based version of the the server side component. This would allow administrators to run the server portion on a non-dedicated linux or windows system. It allows a reduction in deployment costs and since it is a pre-built image it can potentially reduce the skill level required to install and maintain the system. Hybrid VM packages can also be deployed with snapbox and rpath.
8. Think of ways to help companies comply with Sarbanes Oxley requirements regarding security and integrity of financial data another potential reporting/security area might be (I haven't researched it lately):
   (Sarbanes Oxley -> CFO's and/or CEO's have to certify not only are the finance numbers

correct but also that they haven't been manipulated or tamper with)

The Final Conclusion

Shalom Security Platform with a sliding scale using the combination of reporting and security features can combine to produce a very high level of confidence that machines and users are making appropriate and secure use of IT resources.

Kimsey Pollard is a Computer Systems Manager at Georgia Institute of Technology, MIRC Lab.