

**“Real Time” Compromise Assessment FAQ**

*Last Updated: 12/21/2015*

*This FAQ applies to the “CrowdStrike” software for “real time” compromise assessment*

**What problem does CrowdStrike solve?**

CrowdStrike helps Harvard respond quickly to advanced attacks, both those that use “malware” (malicious programs specifically designed to steal information) and those that do not use malware but instead use stolen credentials to move around a network and steal data. See “How does CrowdStrike actually work?” for more detailed information.

By deploying CrowdStrike’s software, we will better protect research and student data that faculty may have as well as administrative data across the University. Quickly detecting these attacks also helps to protect individuals’ personal data and credentials (like online banking usernames and passwords). We believe that this technology would have helped us to detect the three intrusions over the summer even more quickly than we did.

**What are we proposing to do with CrowdStrike?**

CrowdStrike’s software is deployed as an “agent” on servers and end user computers. We propose to install this “agent” on all computers that are managed by HUIT. We would also encourage its installation on any other computers used at Harvard.

**What information does the software have access to?**

CrowdStrike’s software records details about programs that are run and the names of files that are read or written. For example, if you open a Microsoft Word document called “example.doc”, the software will record that Word was run and gather some details about the Word program itself and will record only the name “example.doc” but not access or provide any information about the contents of that file. It also records information about the computer itself, including the machine name and logged in user name.

The software does not access the contents of documents, email messages, IM communications, etc. The information that the software records is transmitted and stored in a “cloud” server operated and protected by CrowdStrike that has been properly vetted by Harvard. Harvard’s contract is clear that the information collected and transmitted belongs to Harvard.

**What information does Harvard have access to?**

A small number of trained and authorized individuals in Harvard Information Security have access to the information recorded by CrowdStrike’s software. They only access this information when they receive an alert about a security issue, as part of an authorized investigation into a security issue or to perform updates to alerts.

**How long is the information kept?**

CrowdStrike archives data for 31 days for investigative purposes. After that, the data is securely deleted per NIST “Guidelines for Media Sanitization” (SP800-88). This is true of both the production and disaster recovery environments.

**How is the information protected?**

CrowdStrike uses industry standard security measures, including strong encryption, and has been vetted against Harvard’s Level 4 data protection requirements. Harvard’s contract with CrowdStrike was reviewed by OGC and includes appropriate legal protections on how the data is handled and protected.

**Will the software cause performance issues if I’m either working with very large files or very large numbers of files?**

Generally not. CrowdStrike’s software records a file “hash” (signature) for executable program files but not for data files. Therefore, working with large data files does not incur a performance penalty. The software records data file names in memory only, so there is a very minimal additional CPU use if a program were to rapidly open and close large numbers of files. We will be sure to test these cases ourselves before general deployment.

**How much network bandwidth does it consume in talking to the cloud?**

On a standard user machine it consumes about 1MB over the course of 24 hours on a fairly continuous basis. By comparison, downloading the Harvard homepage is about 5.4MB that is consumed in a second or two.

On a more active machine like a server, if consumes about 5MB (about the size of the Harvard homepage) over the course of 24 hours on a fairly continuous basis.

**Will it have problems with specialized software that often have negative interactions with programs like anti-virus?**

We do not expect it to. Because it does not do point-in-time scans and does not request “hashes” of large data files, there should be no impact or interaction. We will carefully test it in sensitive environments and are happy to work closely with anyone with concerns about this to ensure that there are no issues.

**How does CrowdStrike actually work?**

CrowdStrike monitors process executions, file read/writes, network activity and child/parent process relationships to create a situational model of what is occurring on a computer. Using this model, it leverages hash matching (“indicators of compromise”), pattern matching (“indicators of attack”), proprietary intelligence drawn from other incidents, machine learning and their CrowdStrike Security Operations Center to find malicious activity.