

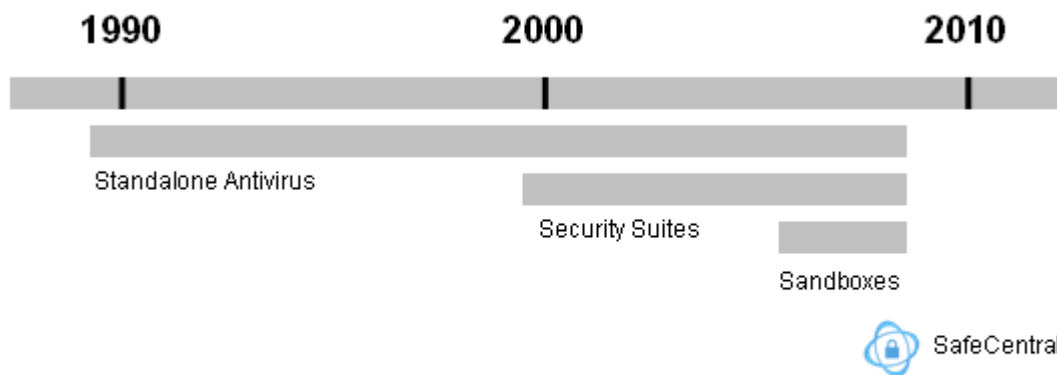
Introduction

Authentium has developed a unique approach to protecting Internet users as they conduct online banking and shopping. Authentium's SafeCentral service delivers secure web browsing even on computers that are compromised with data-stealing malware. This innovative approach is called *Reverse Sandboxing*.

Background

Authentium understands the myriad threats of today's Internet and has created SafeCentral to keep users one step ahead of the bad guys. It should come as no surprise that online criminals are enjoying nearly unfettered access to millions of computers across the Internet, infecting them with data-stealing malware and operating them by remote control from far away places that traditional law enforcement authorities cannot reach. There are many software vendors that are fighting the good fight, trying to keep the PCs of consumers and businesses clean of malware. Sadly, the current state of this war on Internet crime has the bad guys advancing and the good guys struggling to keep up. Now, however, SafeCentral changes the rules and delivers safe online transactions even to users who have had their computer infected by malware.

The history of the anti-malware arms race looks something like this:



History of Internet Security on the Endpoint

Antivirus

In the beginning there were viruses. These early digital miscreants were passed around on floppy disks and via word processing documents. Antivirus programs were developed to block viruses from infecting computers.

Security Suites

Viruses became more sophisticated and starting using many more entry points to infect the PC. These vectors included email, executable files, and even direct access to computers over the network. Spyware, Adware and other forms of malicious software proliferated and made Internet users' lives miserable. Security Suites were developed to combat the many forms of malware and protect their many avenues of entry onto PCs.

Sandboxes

As Internet usage exploded and more users started browsing the web in increasing numbers, the Web emerged as a primary source of infection. Sandboxes were created to place the web browser inside a virtual fortress on the PC in order to protect it from infection by web-borne malware.

What Next?

The user is caught in an arms race between online criminals and the security software industry. Antivirus definition files are growing to tens of megabytes in size (in some cases, 100 megabytes!) and still can't catch all the malware.

SafeCentral

Authentium is an anti-malware company that has developed Antivirus programs and Security Suites. These are important components in the overall protection of a PC. But SafeCentral targets another point of protection: online transactions like banking, shopping, and any web session that involves sensitive data. Starting with the assumption that a computer has been infected with data-stealing malware, or DNS-changing trojans that lead users to forged copies of authentic websites, SafeCentral protects the user and their data from online theft and fraud. We call this the *Reverse Sandbox*.

Reverse Sandbox

- Sandboxes try to filter out bad stuff from the Internet so it cannot infect a PC.
- Reverse Sandboxing keeps the bad stuff on a PC out of a web session, so users can browse and transact safely.

Why a Reverse Sandbox?

Online use of sensitive data in banking, shopping and running a business is increasing, but traditional anti-malware methods cannot scale to meet the online threats. Authentium has collected and analyzed over a million malware samples. We receive gigabytes of virus samples every day. These startling numbers point to two things: (1) the high number of unique or variant malware samples we see and (2) the sheer volume of malware being passed around on the Internet. Traditional antivirus and sandboxing technology essentially boils down to distinguishing between good and bad data. Good data are the web pages and programs you want to see and use on your computer. Bad data are executable

programs that want to steal your good data, especially the valuable data like your bank account number or password. But think about it, if a million criminals who look just like good people descended on the downtown area of your favorite city, how could the police protect you? When the police round up thousands of criminals and cart them away, thousands more take their place.

Solution	Traditional Security Software <i>Antivirus, Security Suite, Sandbox</i>	SafeCentral
Security Promise	Keep computer clean of malware infection	Assume computer is infected and provide safe browsing anyway
Approach	Reactive	Proactive
How it works	<ul style="list-style-type: none"> • Obtain and analyze malware, creating rules and signatures to identify it. • Distribute definitions on daily or hourly basis. • Scan applications and other data to identify malware and block it. 	<ul style="list-style-type: none"> • Allow only SafeCentral browser to access keyboard and screen during online transactions • Provide Secure DNS lookups for web sites. • Protect SafeCentral browser against tampering

Antivirus, Security Suites and Sandboxes all take the same approach: they try to distinguish between the good programs and the bad programs, and block the bad programs. Sandboxes go a step further: they allow the bad programs into a confined place on your computer and then try to keep them there. This has not been shown to work in a way that sufficiently protects users and their computers.

Authentium’s Reverse Sandbox technology simply ensures that your web browser, your DNS, your keyboard and your screen are only accessible to you. The www.safecentral.com website has videos that show this unique solution in action, allowing Internet users to shop and bank safely even though one of the millions of pieces of malware may have gotten onto their computer.