



Omgeo Relies on Bit9 for Malware Protection



Blocking Malicious Software in Financial Services

As the leading provider of post-trade, pre-settlement trade management solutions, Omgeo LLC, a global joint venture of Depository Trust & Clearing Corporation (DTCC) and Thomson Financial, is dedicated to providing its customers with products and services that are fast, efficient, scalable, and flexible. This commitment is built upon a network of resources and depth of expertise that enables Omgeo to keep its clients at the forefront of a fast-evolving industry.

Omgeo currently processes more than 120,000 transactions each day on behalf of 6,000 clients in 42 countries—with a total trading volume of more than \$4 billion. With that much business at stake, Omgeo can't let spyware, viruses, or other malicious software cause system disruptions that impact its responsibility to its customers.

Key Benefits to Omgeo

- Solved zero-day threat problem
- Reduced threat response times from days to 10 minutes
- Blocked malware attacks and prevented propagation
- Reduced and simplified clean-up activities

“Omgeo takes customer data confidentiality very seriously. Bit9 Parity will help us maintain the integrity of our information systems on a consistent basis.”

—Dennis Arndt, CISO, Omgeo LLC



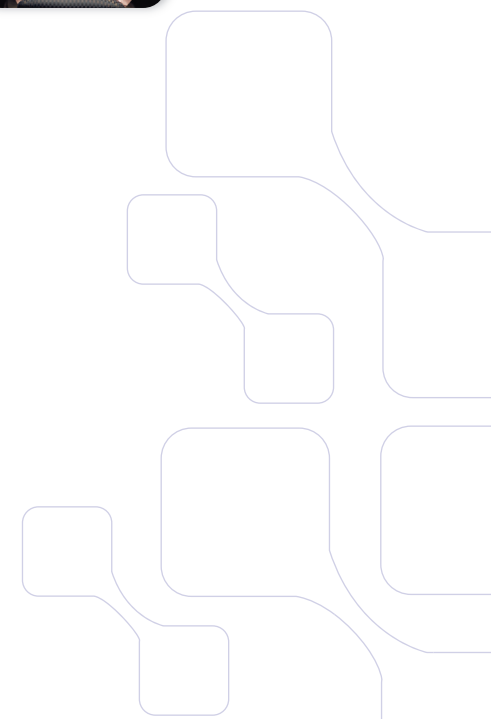
When Anti-virus Isn't Effective

“When’s the next Melissa coming?” asks Anthony Zannella, Omgeo’s Manager of Corporate Services and Support, referring to the next virus outbreak. Responsible for Omgeo’s Windows® 2000 Active Directory infrastructure and all Windows workstations and servers, Zannella feels the pain caused by every virus or Trojan horse.

- **Signatures not available for days:** Omgeo’s existing anti-virus tools rely on specific signatures to recognize any new viruses they detect. It was not uncommon for this process to take up to a couple of days when a new virus appeared, during which time IT was virtually powerless to stop an outbreak. This situation, known as a “zero-day vulnerability,” was becoming more frequent.
- **Spyware and malicious software disrupting business operations:** There is a class of “invisible” malware, never detected by Omgeo’s existing tools, that is known only through its symptoms. Users complaining to the help desk about poor performance may get their machines re-imaged. This brute force tactic removes spyware, but at the cost of significant end-user disruption.

- **Unreliable virus cleaning:** Finally, anti-virus tools were frequently unable to clean infected machines properly. In these cases, no other option remained—IT was left to solve the problem on its own. A virus that propagated in such a way would typically require two or three people to manually track it down and eliminate it over several days.

With limited resources and a small team supporting multiple facilities, Omgeo needed a solution that could alleviate the pressure caused by increasingly sophisticated malware. Frustrated that a state-of-the-art security model including firewalls, anti-virus, and anti-spyware was still unable to prevent malicious software from getting onto Omgeo’s desktops, Zannella went looking for a new approach.



Omgeo Case Study

“The whole concept of ‘just don’t let it run’ is so basic. I can’t believe that such a simple concept is something that is just starting to catch on now.”

—Anthony Zannella, Manager of Corporate Services and Support, Omgeo LLC



■ The Bit9 Solution

Omgeo chose Bit9 because it provided IT with the straightforward ability to block spyware or other malicious or unknown software from running—a capability not present in any of its other security products. “The whole concept of ‘just don’t let it run’ is so basic,” says Zannella. “I can’t believe that such a simple concept is something that is just starting to catch on now.”

With a deployment of nearly 1,000 endpoints in Boston and New York City, Omgeo has configured Bit9’s endpoint security software, Parity™, to allow every employee to install and run whatever software they want on their desktops. Through Bit9, IT monitors the environment for any software that is new—and therefore unknown to IT. Parity’s Automatic Graylist™ technology prioritizes and highlights the most risky of this unknown software. When something is found to be malicious, Omgeo relies on Bit9 Parity’s reports to find all the machines where it exists. Finally, an enterprise-wide ban is created that prevents that file from running, anywhere, ever again.

■ Preventing malware propagation:

Now, when a new zero-day threat is detected, the IT group can create an instant ban in Parity that blocks the file from running throughout its entire organization. Since it may take days for a signature to arrive, Bit9 provides Omgeo with a catch-all malware protection layer.

■ Simplifying clean-up:

After banning a file, Omgeo uses Bit9 to discover where any malicious code was copied. By targeting its cleanup efforts, IT no longer has to deal with complicated network sniffing or quarantine efforts. Furthermore, Bit9 makes sure the threat can not reappear and execute again.

■ Maximize end-user flexibility:

It was important to Omgeo that it do everything it can to protect the flow of the business. Bit9 was able to give IT the ability to lock out unwanted software without implementing full-scale lockdowns of user desktops. This way IT provides the right level of service to meet the needs of the business environment.

Prevent Malicious Software

> Try Bit9’s FREE service for identifying unknown software

▶ <http://fileadvisor.bit9.com>

> Learn about Bit9’s solutions

▶ <http://www.bit9.com/solutions.html>

> Talk with a Bit9 Sales Representative

▶ http://www.bit9.com/sendinfo_contact.html
▶ 617.393.7400

■ Hitting the “Big Red Button”

In a recent example of Omgeo’s new-found effectiveness against the growing malware threat, Bit9 Parity reduced what had been a multi-day process into a 10-minute exercise.

A virus had hit, spreading through instant messenger buddy lists. Omgeo’s existing anti-virus tools identified it as a Trojan, but did not provide a signature right away. So even though IT was getting “clobbered” with messages alerting them to the presence of the virus, there was nothing the anti-virus software could do about it.

At that point, an IT administrator accessed the Bit9 Parity console and banned the file in question in real time. By blocking the malicious executable directly, it could no

longer run anywhere—propagation was instantly stopped. Then, using Bit9’s Find File™ utility, every system in the environment that had been infected was located and targeted for a clean-up. The problem was immediately solved, with a nice side benefit of no more useless anti-virus alerts.

Conclusion

According to Zannella, Bit9 Parity is instrumental in Omgeo’s ability to “shut down executables from running in a very short time, and preventing the next outbreak.” With more and more malicious software getting through the gates of traditional network and desktop security systems, Omgeo relies on Bit9 Parity for catch-all malware protection.

■ Solve the problem of unwanted software and regain control over what runs on your infrastructure—call Bit9 today: 617.393.7400 or visit us at www.bit9.com.

© 2008, Bit9, Inc. All Rights Reserved. Bit9, Inc., FileAdvisor, Find File, Parity, and ParityCenter are trademarks or registered trademarks of Bit9, Inc. All other names and trademarks are the property of their respective owners. Bit9 reserves the right to change product specifications or other product information without notice.



Bit9, Inc.

266 Second Ave.
Waltham, MA 02451

p: 617.393.7400

f: 617.393.7499

www.bit9.com