Case Study

Bromium Protects Sensitive Data and Provides a Transparent Experience at Taft Stettinius & Hollister LLP

Taft Stettinius & Hollister LLP (Taft), in business since 1885, is headquartered in Cincinnati, Ohio and employs 400 attorneys who service clients across a wide range of industries—from finance to real estate to environmental organizations—in virtually every area of law.

Company Snapshot

INDUSTRY

Full-service law firm

ENVIRONMENT

- 800+ employees
- 850 Microsoft Windows 7 PCs and laptops

SOLUTIONS

- Bromium® vSentry®
- Bromium LAVA™

CHALLENGES

Implement a transparent endpoint security solution that protects end users, intellectual property and client data against malicious downloads, spear phishing and ransomware

BENEFITS

- Dramatically reduces the need to re-image PCs
- Completely non-disruptive to users
- Protects against phishing attempts, Web-borne malware and morphing threats

The challenge: enabling employees to work without risk

At Taft, employees and the clients they serve come first. “In the legal sector, most end users are also owners of the company and have a lot of influence on how we safeguard the computing environment. It’s important for us to implement security products that run smoothly and don’t get in the way of their productivity. They like solutions that are transparent, so that they can focus on what’s important to them,” says security manager Phil Miller.

At Taft, attorneys and legal assistants spend much of their time online, researching legal forms and documents, perusing content from websites like Forbes and exchanging confidential documents with clients and partners. In the past, all this activity continually exposed the company’s Microsoft Windows 7 PCs and laptops to infected downloads and other threats. Miller and his team found themselves re-imaging 15 or more PCs on a weekly basis, in spite of their diligent efforts to secure the infrastructure. Taft needed a better way to protect its endpoints without disrupting users and enabling them to confidently search and download from the Web.

Antivirus and IPS inadequate defenses against modern threats

Taft has approximately 850 Microsoft Windows 7 PCs and laptops at its headquarters and its branch offices across the Midwest. Many of the attorneys are required to travel or choose to work remotely on occasion, so they frequently connect corporate laptops to unsecured Wi-Fi networks at airports, hotels or cafés.

Prior to 2011, Taft focused its security efforts primarily on the perimeter, deploying Web-filtering technology, which would crash frequently and disrupt operations. This was replaced with a robust intrusion prevention system (IPS) but, as Miller pointed out, “It doesn’t find everything.” For example, in one recent instance, Taft

"We were blown away by the solution of isolating malware."

"Bromium is completely transparent to the users. It just works, and that's basically what we want out of a security tool."

PHIL MILLER, SECURITY MANAGER,
TAFT STETTINIUS & HOLLISTER LLP

had 40 infections in one day from malicious banner ads on a legitimate site frequently accessed by its attorneys.

Over a period of time, Taft also deployed various antivirus solutions to protect endpoints. Additionally, Taft implemented whole-disk encryption and removable-disk encryption to safeguard its sensitive data, which is housed in a content management system on a separate network. The company uses a spam filter to block phishing attempts and unwanted ads.

Another concern is targeted phishing attempts. When Taft was migrating from Windows XP to Windows 7, users received phishing emails about the migration process. Miller noted that while the company has never suffered any negative consequences from phishing attempts, he is always concerned about bad actors potentially accessing the company's intellectual property through social engineering tactics.

Bromium to the defense

In order to better protect the environment, Miller decided to investigate better options for securing endpoints. When he attended a Bromium demo presentation in his area, he was "blown away" by the solution's ability to leverage virtualization technology, isolating malware in a micro-virtualized machine (micro-VM). After getting the nod from the CISO, Miller embarked on a 30-day proof-of-concept (PoC) for 25 to 30 machines across the enterprise. He engaged legal assistants for testing purposes, as they spend the bulk of their time online doing research every day. The biggest concern was whether Bromium would interfere with legitimate downloading of documents from county and court websites. The PoC was a great success. Taft discovered that Bromium was completely transparent to users and did not interfere with document downloads. Another big plus was Bromium's frequent policy updates—every two minutes instead of 15 minutes, as is the case with other endpoint security applications.

Completely transparent and easy to support

Early this year, Taft signed off on Bromium for the entire company. The initial setup, which was assisted by Bromium consultants, took only half a day. Full deployment across every laptop and desktop took approximately three months. User training was minimal—Miller distributed a one-page support document, and users were up and running in no time.

"Most users don't even realize Bromium is there," he said. "Transparency is a huge requirement for us, and Bromium meets that need perfectly. Every once in a while, Bromium prompts users

To learn more about Bromium's game-changing security architecture, please visit www.bromium.com.

when a suspicious file shows up. We all appreciate that extra layer of visibility. Most of all we appreciate that Bromium is isolating all Web browsing so that users can go anywhere online, and no Internet Explorer, Flash or Java exploit, even when wrapped with a kernel zero-day, can escape a micro-VM and infect the PC."

Support issues have been minimal for Taft. "Bromium has always been extremely responsive whenever we've had issues and usually resolves them in less than an hour. I never feel that I've been handed a substandard product and have to work out the bugs. In fact, we are up for renewal, and everyone, including the CISO, is on board." Miller also feels that since Bromium is a Microsoft partner, "they're obviously doing something good."

Bromium saves time

As a result of deploying Bromium, Miller's team spends about 75% less time on re-imaging systems. "We're extra careful here, so we re-image PCs anytime there's an inkling of a suspicious file—from coupon adware to CryptoLocker variants. We always completely wipe the system clean. With Bromium, we now only have to re-image one or two per week instead of our usual 15 and those are because of user errors," said Miller. "Bromium helps me sleep better at night because I don't have to worry about someone downloading a potentially malicious file."

Miller and his team also take advantage of the Bromium Live Attack Visualization and Analysis™ (LAVA) engine to collect granular information on threats that are isolated in the micro-VM. "We use it to troubleshoot issues and for post-mortem analysis. It provides great visibility to the security posture of our endpoints," he said.

Ready for anything

So far, Taft has not experienced any major incidents resulting from targeted phishing campaigns or advanced, evasive threats, and Miller fully expects to continue on that trajectory. "Having the right tool in place makes us feel more confident. We're very happy with the product. In our environment, Bromium doesn't interfere with our users, and it's not complicated. It just works, and that's basically what we want out of a security tool."

Br Bromium®

Bromium, Inc.
20813 Stevens Creek Blvd
Cupertino, CA 95014
info@bromium.com
+1.408.213.5668

Bromium UK Ltd.
Lockton House
2nd Floor, Clarendon Road
Cambridge CB2 8FH
+44.1223.314914

For more information go to www.bromium.com
or contact sales@bromium.com