Case Study

East Coast Financial Investment Advisory Firm

Bromium Alleviates Productivity and Downtime Concerns

This prominent East Coast financial investment advisory firm, which has been in business since 1999, currently has more than $5 billion in assets under management.

Company Snapshot

INDUSTRY

Financial services: investment fund management

ENVIRONMENT

100+ employees

150 Microsoft Windows 7 PCs

SOLUTIONS

Bromium® vSentry®

Bromium LAVA™

CHALLENGE

Excessive employee downtime and need to reimage PCs due to malware infiltrations from email and the Web

BENEFITS

- No need to reimage PCs
- Reduced disruptions to the daily workflow
- Eased concerns about potential breaches
- Improved alignment with SEC security guidelines
- Excellent ROI

The challenge: excessive employee downtime due to compromised endpoints

Everyone at the firm was frustrated—from financial analysts to IT. The more than 100 employees—especially the research analysts and finance personal—endured almost daily interruptions in their workflow due to malware infections and inadequate endpoint protection, which included spam filtering, email encryption, and antivirus. The IT staff reimaged an average of two PCs every week, which resulted in downtime for employees whose systems were attacked by viruses, malware, spyware, and malicious attachments. When the situation reached a tipping point, the CTO was determined to find a better, smarter solution—an endpoint solution that would fit in with their security backend and provide users with a seamless and secure endpoint experience.

Antivirus and other solutions weren't doing the job

The firm has approximately 150 Microsoft Windows 7 PCs at headquarters, including spares, desktops at the main office, and laptops that employees would often take home. In addition, there are six employees who work remotely at branch or home offices in other parts of the country.

For several years, the firm incorporated a sophisticated array of layered security, including the most advanced endpoint solutions. But these solutions weren't doing the job. Updates to some of the security solutions were two or three steps behind hackers, spam and other unwanted content was still getting through the email channel, and antivirus protection was completely ineffective.

Frustrated users

Busy users were not always aware of online risks. "Our research analysts and back-office financial operations staff spend a great deal of time on the Internet or responding to emails, and they often don't pay attention to where they are clicking," said the CTO. "In the past, they didn't even know they had a problem until they realized that their PCs were sluggish or malfunctioning." To fix these problems, IT had to take

Bromium®

users' systems offline and completely reimage the PCs, which meant as much as a full day of lost productivity. And when employees got their machines back, some of them would have to go through the time-consuming process of recertifying themselves in order to access key financial applications.

Enter Bromium

In 2013, the CTO learned about Bromium's unique endpoint solution from peers who also worked for companies in the financial sector. He was particularly interested in Bromium's ability to isolate all content for each task, including threats, through microvirtualization technology that leverages CPU hardware technology. He liked the idea that Bromium could encapsulate Web browsing activities and downloads, preventing malicious third parties from harming endpoint systems and the network via Internet Explorer.

The firm adopted Bromium vSentry early last year and now has it deployed on nearly every endpoint. Over a two-week period, Bromium engineers worked side by side with the firm's security professionals to make sure that everything ran smoothly and any issues were resolved swiftly. In the process of installing and deploying Bromium, IT cleared temp directories of unwanted files, revoked administrative rights on users' systems, and eliminated USB access to prevent employees from downloading sensitive data.

Though some of the employees were somewhat resistant to the change at first, just about all of them acknowledged that browsing the Internet was a risky, albeit necessary, activity. The CTO asked IT to take the time and hand-hold users through a brief training session, and soon everyone was on board. "Once people got used to it, they liked it," said the CTO. "Upper management also saw the value of the Bromium solution, especially when they saw how hard their competitors were being hit by viruses."

Bromium makes everyone more productive

The CTO and his colleagues have seen the difference now that Bromium has replaced their traditional endpoint security solutions. "The best thing about Bromium is that it keeps our PCs clean and our employees productive," said the CTO.

In April of 2014, Microsoft released a security advisory about a serious zero-day vulnerability in Internet Explorer that could corrupt memory and enable an attacker to execute arbitrary and potentially malicious code within a user's browser session. "In the past, this could have had a huge impact on our business," said the CTO. "With Bromium in place, we were completely unaffected by this event and continued to function at full capacity."

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

Another big plus is operational cost savings. "Systems used to go down regularly due to malicious Internet-borne threats. My desktop team spent a good deal of its time on reactive fixes, scanning and reimaging PCs while deploying spare systems to mitigate downtime. With Bromium, we've achieved greater uptime for the business and diverted desktop resources to more value-added projects," said the CTO. He equated this to significant annual savings and increased productivity. The CTO believes that the solution will pay for itself in no time: "The ROI is compelling and will help any CTO justify deploying Bromium into his/her environment."

The CTO was impressed with the responsiveness of the Bromium team. "Bromium support has been fantastic," he added.

Improved cybersecurity preparedness

Another key benefit derived from Bromium deployment is better alignment with industry compliance standards. Thanks to Bromium, the CTO feels confident that his firm can meet many of the critical requirements of the US Security and Exchange Commission (SEC) National Exam Program. The SEC Office of Compliance Inspections and Examinations (OCIE) will be conducting examinations of more than 50 registered broker-dealers and registered investment advisors, focusing on areas related to cybersecurity—and this firm is prepared.

Looking at the future

The CTO is also using Bromium's Live Attack Visualization and Analysis engine to collect granular information on threats that are isolated on Bromium's micro-virtualized machine. "We are currently using LAVA to analyze attacks and hope Bromium will help harden the overall landscape to malware and virus attacks," he said.

Bromium®

Bromium US
20813 Stevens Creek Blvd
Cupertino, CA 95014
info@bromium.com
+1.408.598.3623

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

For more information refer to www.bromium.com,
contact sales@bromium.com or call at 1-800-518-0845