

Mosaic: Bromium's Complete Endpoint Security Elevates Risk Posture

Company Snapshot

INDUSTRY

World's leading producer of concentrated crop nutrients

ENVIRONMENT

9,000 employees worldwide
6,000 Microsoft Windows endpoints

SOLUTIONS

Bromium® Advanced Endpoint Security

CHALLENGE

Reduce endpoint risk and improve overall security posture with a solution that is significantly more effective than current traditional security technologies

BENEFITS

- Virtualization at the CPU level ensures security of the system and prevents the spread of malware to the enterprise network
- Simplicity of implementation and configuration eliminates the possibility of security gaps
- Defeats ransomware and renders it a non-issue

The Mosaic Company is the world's leading producer and marketer of concentrated phosphate and potash with approximately 9,000 people in six countries. The company mines phosphate rock from nearly 200,000 acres of Mosaic-owned land in Central Florida and mines potash from four mines in North America, primarily in Saskatchewan. Mosaic's products are processed into crop nutrients, and then shipped to customers in the major agricultural centers of the world.

The challenge: traditional security is ineffective against modern zero-day and targeted attacks

Paul Hershberger, director of security, risk and compliance at Mosaic, is on a mission: to improve the company's overall risk posture by modernizing the computing environment and optimizing endpoint security. On a regular basis, his department tackles the advanced threats any company in the same sector would face—threats executed by four types of malicious actors: state-sponsored bad actors, hactivists, external cybercriminals and internal bad actors.

Hershberger embarked on a thorough risk assessment of Mosaic's existing security infrastructure, beginning with endpoint security. At the time, Mosaic had a multi-vendor environment consisting of traditional

threat-mitigation technology layers: intrusion detection systems (IDS), intrusion prevention systems (IPS), Web and email filters, desktop firewalls, antivirus, anti-malware and anti-spam. After the assessment, Hershberger started looking for more effective endpoint security and was introduced to Bromium's unique approach by a channel partner.

Hershberger's team began their assessment by identifying "residual risk" (the threat that remains after security controls designed to identify and eliminate risk have been implemented) on secured laptops, desktops and mobile devices, taking into account all the solutions they currently had in place to manage those risks. "We came to the conclusion that we were putting a lot of time, effort and money into endpoint solutions that were making

Case Study

“Bromium has a simple, yet complete, approach and provides us with a broader level of protection with fewer opportunities to create gaps or a false sense of security. Whereas other solutions all too often ‘fail silently,’ we found that this was not the case with Bromium.”

PAUL HERSHBERGER,
DIRECTOR OF SECURITY,
RISK AND COMPLIANCE, MOSAIC

only small, marginal effects on the risk. After we evaluated all our solutions and controls, we discovered that our residual risk was only one point away from our inherent risk,” explains Hershberger. “Everything we were doing was fundamentally not working. We started looking for ways to truly shift the risk dynamic, and that’s why we looked at Bromium.”

Bromium’s CPU-enforced security eliminates breaches

Before selecting Bromium, Hershberger and his team evaluated a wide variety of endpoint solutions, but ultimately it was the simplicity and completeness of the Bromium solution that won them over.

When they looked at the way other endpoint-security solutions operate, they found that there were too many ways that things could go wrong. “Most of these solutions offer many configuration options, and the way they are configured can mean the difference between effectiveness and a false sense of security,” says Hershberger. “When we looked at where gaps could arise in the different tool sets, we found that Bromium has a simple, yet complete, approach and provides us with a broader level of protection with fewer opportunities to create gaps or a false sense of security. Whereas other solutions all too often ‘fail silently,’ we found that this was not the case with Bromium.”

Hershberger and his team attribute the effectiveness of Bromium to the way it isolates user tasks in a secure micro-virtual machine that is enforced by the CPU on the device. As he suggests, some security products incorporate virtualization to some extent—such as spinning up virtual machines (VMs) to do analytics on the fly, detonating malware in a sandbox, and then sending it through analysis—but Bromium takes the technology much further. “Bromium’s technology is really sound. I like the fact that this is the only solution that leverages virtualization through the technology stack at the CPU and hardware layer,” affirms Hershberger.

A successful initial deployment

Initiated in early 2015, the first Bromium deployment wave included 2,000 endpoints. Hershberger describes the technical deployment as “simple and straightforward—and the collaboration with Bromium consultants was nothing short of stupendous.”

Mosaic users with Bromium installed on their systems like the extra protection, which does not interfere with their productivity. They appreciate the “freedom to click on anything without restriction and without worry,” says Hershberger.

Beyond just using Bromium Advanced Endpoint Security as a tool for protection, the Mosaic security team

Case Study

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

almost immediately started using it as an investigation and analysis tool, along with the Bromium Threat Analysis module. "We have a lot of potentially suspicious code and files coming into our environment, and we don't always know what they are. In the past, we've had to very carefully move them to an isolated lab environment. With Bromium, we can start interacting with them right away from the desktop," says Hershberger. "It's a liberating feeling when one of my people can safely and confidently look at a piece of suspicious code right on the desktop and make a decision as to how to handle it from there."

Bromium defeats ransomware

Hershberger noticed that ransomware, which locks down a computer and its files until the victim pays a ransom to regain access, was a growing threat at Mosaic. Over the course of several months, his team detected several instances of ransomware, which is known for being highly evasive and destructive, avoiding detection by antivirus solutions and other defenses. Hershberger determined that the sources of ransomware were typically commonly accessed, popular websites.

After Bromium had been running in the Mosaic environment for a while, Hershberger and his team could see how well Bromium was defending systems against ransomware compared with the company's traditional defenses. They highlighted the differences in experience to the user and the IT support staff between unprotected hosts and protected hosts in terms of lost productivity, lost files and host re-imaging. The conclusion? "Bromium is effective" says Hershberger.

Expanding the Bromium footprint

Fully convinced of Bromium's efficacy in the face of advanced, stealthy threats and its acceptance among users, Hershberger plans to deploy Bromium on all PCs on a worldwide basis this year. Adopting Bromium has motivated Mosaic to take steps to replace legacy systems and build an up-to-date, securable, hybrid endpoint environment with both virtual desktops and physical systems, where required. "Bromium has the potential to truly change the security dynamic," says Hershberger.



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

Copyright ©2016 Bromium, Inc. All rights reserved.
CS.Mosaic.US-EN.1603