HP WOLF ENTERPRISE SECURITY

POWERED BY Bromium®

HP WOLF SECURITY

DATAPORT PROTECTS ITS USERS AGAINST CYBERATTACKS WITH HP SURE CLICK

Dataport, an information and communication provider for public administration, is gradually safeguarding 32,000 select clients against cyberattacks with the Bromium Secure Browser. The encapsulated internet access ensures optimum security while performance and usability noticeably improve at the same time.

As an information and communication service provider, Dataport supports the municipalities of Hamburg, Bremen, Schleswig-Holstein, and Saxony-Anhalt, as well as the tax municipalities of Mecklenburg-Western Pomerania and Lower Saxony and many municipalities in Schleswig-Holstein. With more than 100,000 total clients, the optimal goal is to protect a giant, attack-prone area.

Until now, secured internet access occurred via a terminal-server environment in the Dataport computer center. This model simultaneously limited usable points of access and convenience during uploads, downloads, and data transfers, as well as leading to insufficient performance when accessing web pages. Dataport wanted to change to a solution that would allow secure, high-performance internet usage.

ENCAPSULATED INTERNET ACCESS WITH HP SURE CLICK

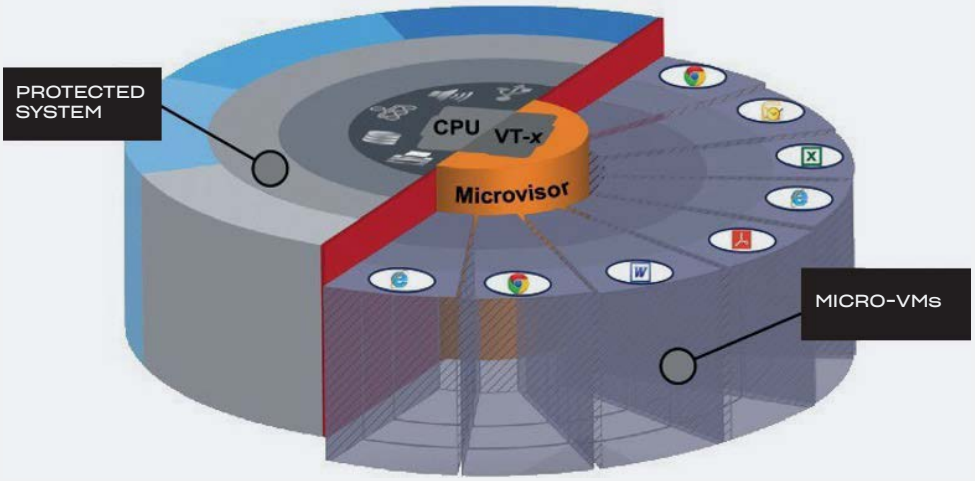
After researching options, Dataport decided on the application-isolation solution Bromium Secure Browser, which provides an encapsulated internet browser directly to approximately 32,000 of its more than 100,000 clients. Dataport turned to consulting company Computacenter for help conducting a pilot project on 50 clients. To set up the trial environment, the corresponding policies were configured via the central Bromium Enterprise Controller and tailored to the requirements of the computing center. After a successful trial, Dataport plans to handle the remaining software rollout itself, supported by consulting services and administrator training sessions by Computacenter.

Bromium performs risky user activities—such as opening an email attachment, downloading documents, or accessing unofficial websites—in what is known as a micro-VM. These dynamically generated virtual environments run the applications in isolation, so that no malware code can escape and attack the device's operating system—preventing the end device and company network from being compromised and allowing users to continue working as usual.

The Bromium solution implements the encapsulation through hardware-insulated micro-virtualization. The core elements are a Xen-based hypervisor that is especially developed in terms of security and the integrated virtual features of all current CPU generations.

MORE SECURITY, MORE CONVENIENCE

Dataport has now installed the Bromium solution on more than 32,000 clients, with more to follow gradually. The low-performance internet access of the clients via a terminal-server environment is now a thing of the past, while users, PCs, and networks are protected against new, unknown malicious code for file downloads.



“With the Bromium solution, we are perfectly safeguarded against attacks via our internet browser. While drive-by and watering-hole attacks went nowhere with our customers since the introduction of the terminal-server-based browser, we then also added optimum protection against file-based malware that could end up on our clients when downloading files. Moreover, the improved performance and usability is very notable compared to the previously used terminal-server landscape,” explains Jan-Eric Hein, Bromium Product Manager at Dataport.

ABOUT DATAPORT

As an information and communication service provider, Dataport supports the municipalities of Hamburg, Bremen, Schleswig-Holstein, and Saxony-Anhalt, as well as the tax municipalities of Mecklenburg-Western Pomerania and Lower Saxony and many municipalities in Schleswig-Holstein. The public law institution was founded based on a state contract on January 1, 2004 and has its headquarters in Altenholz near Kiel with branches in Hamburg, Rostock, Bremen, Lüneburg, Magdeburg, and Halle.

Learn more at www.dataport.de

ABOUT HP SURE CLICK ENTERPRISE

Powered by the former Bromium Inc.'s industry-leading containment technology, HP Sure Click Enterprise[1] provides a virtual safety net for PC users, even when unknown threats slip past other defenses. Hardware-enforced virtualization isolates high-risk content to protect user PCs, data, and credentials, rendering malware harmless—while IT gets actionable threat intelligence to help strengthen organizational security posture. HP Inc. entered a formal OEM relationship with Bromium Inc. in 2016 and began shipping Bromium containment technology, branded as HP Sure Click,[2] on millions of enterprise-class devices the following year. After formally acquiring Bromium Inc. in late 2019, HP updated the name of the Bromium Secure Platform to HP Sure Click Enterprise, which is now the flagship offering in the HP Wolf Enterprise Security portfolio.[3]

Learn more at www8.hp.com/us/en/security/enterprise-pc-security.html

[1] HP Sure Click Enterprise requires Windows 10 and Microsoft Internet Explorer, Edge, Google Chrome, Chromium, or Firefox are supported. Supported attachments include Microsoft Office (Word, Excel, PowerPoint) and PDF files, when Microsoft Office or Adobe Acrobat are installed.

[2] HP Sure Click requires Windows 10. See https://bit.ly/2PrLT6A_SureClick for complete details.

[3] HP Wolf Enterprise Security requires Windows 10. HP Sure Click Enterprise supports Microsoft Internet Explorer, Edge, Google Chrome, Chromium, and Firefox browsers and isolates attachments from Microsoft Office (Word, Excel, PowerPoint) and PDF files, when Microsoft Office or Adobe Acrobat are installed. HP Protected App currently supports RDP sessions, Citrix® ICA sessions, and a Chromium-based browser.

4AA7-7798ENW, Rev 1, June 2021