HP WOLF SECURITY

HP WOLF ENTERPRISE SECURITY

POWERED BY Bromium®

THE CITY OF BONN BUILDS A PROTECTIVE SHIELD AGAINST UNKNOWN MALWARE

The protection of confidential data is of the highest importance in the municipality—and it's taking an innovative direction. By choosing the HP Sure Click solution, the city is safeguarding the end devices of its employees—and thereby the confidential data of citizens—from previously unknown malware code.

The 72-meter-high city hall is the headquarters of the municipality of the federal state of Bonn. (Source: Federal City of Bonn)

Traditional security tools have now become standard in communal IT today. New zero-day attacks, advanced persistent threats, and ransomware Trojans cannot be reliably detected with them. This is reason enough for the municipality of Bonn to take on the task of increasing client security. Two aspects were of particular importance: security when surfing and communicating via email. While companies can strictly regulate the reception of email enclosures or access to websites, this is not possible in municipalities due to legitimate citizen concerns. PDFs and ZIP archives must be permitted; employees must be able to visit relevant-but-questionable forums or sites while protecting youth. An additional challenge lies in the fact that, due to the extensive range of municipal tasks, hundreds of applications, tools, and specialized processes must be provided and kept operational.

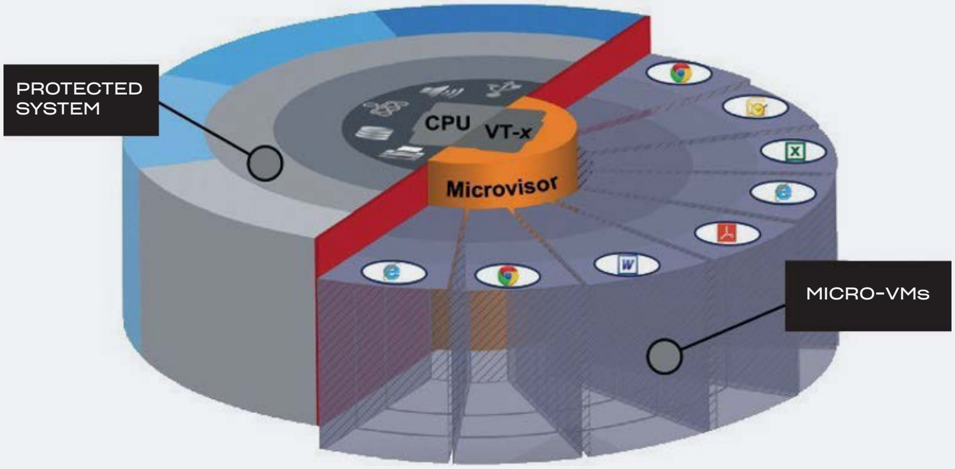
EMAIL AND BROWSER PROTECTION FROM ONE SOURCE

When selecting a client security solution, the municipality of Bonn initially considered several applications that address the vulnerability of internet browsers and allow safe surfing. However, these applications didn't address the extremely important topic of email. It quickly became clear that the secure platform of Bromium, with its technical concept of "isolation instead of detection of malware code using micro-visualization," was the best choice.

As part of a brief evaluation phase, extensive functional and performance tests were conducted. A central result was that around one quarter of the approximately 4,000 computers did not have the required setup for a seamless use of the Bromium solution. Consequently, the municipality decided on a successive rollout of the secure platform in combination with replacement of older hardware and the introduction of Windows 10.

BROMIUM SOLUTION RELIES ON ISOLATION INSTEAD OF DETECTION

The central characteristic of the Bromium solution is that the detection of malware code is not the priority, but rather the effective avoidance of its effects. This is implemented through the isolation of all risky user activities through micro-virtualization. The core elements are a Xen-based hypervisor that's especially well-developed in terms of security and the integrated virtual features of all current CPU generations.



The Bromium solution then always processes tasks in virtual instances if it can be dangerous, such as when accessing a website, when opening an email attachment, or accessing the data of a USB device. Here each individual task runs in its own micro-VM and is strictly separated from the actual operating system and the connected network, preventing the compromise of the end device and the municipal IT network.

Bromium 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.

“Bromium offered both the technically best solution as well as clearly the most cost-effective solution with the licensing and service model,” said Dirk Schumacher, manager of the specialized department IT Security and IT Strategy in the HR and Organizational Office of the Federal City of Bonn.

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.

4AA7-7797ENW, Rev 1, June 2021