



HP WOLF ENTERPRISE SECURITY



HP WOLF SECURITY

THE MUNICIPALITY OF BADEN-WÜRTTEMBERG IS ARMING ITSELF AGAINST CYBERATTACKS



From left to right: BITBW President Christian Leinert; Jochen Koehler, Regional Director DACH of Bromium; the Minister of the Interior, Digitalization and Migration Thomas Strobl; and the CIO/CDO of the state government Stefan Krebs following the contract signing. (Source: Bromium by HP)

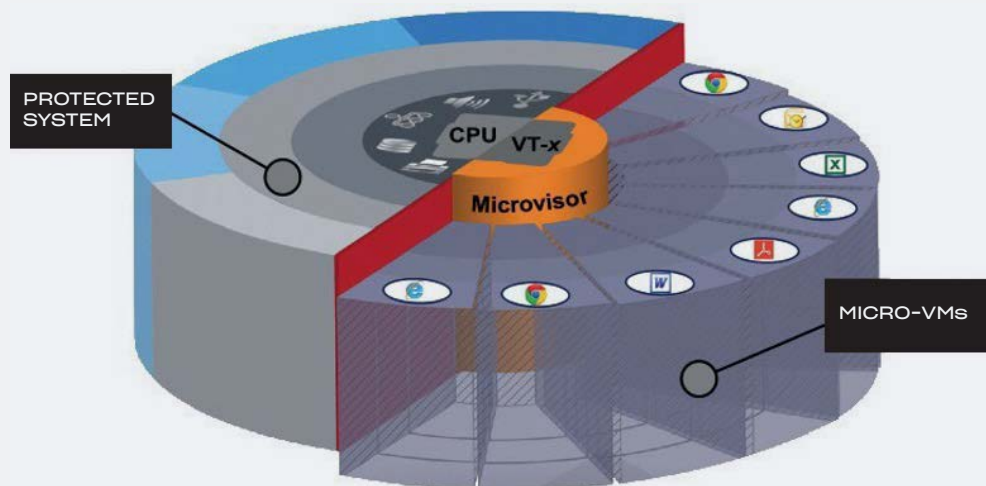
The municipality of Baden-Württemberg safeguards 60,000 clients with the secure platform of Bromium. Using micro-virtualization, the state's IT system can best be protected from novel cyberattacks.

With more than 60,000 employees in the municipality of Baden-Württemberg requiring regular internet and email communication to manage their daily operations, the optimal goal is to protect a huge, attack-prone area. More than six million emails arrive every week in electronic mailboxes, and more than 85 percent are from undesired advertising content that can contain malware codes, viruses, Trojans, or ransomware.

To prevent the widest range of attacks on IT security, the municipality of Baden-Württemberg has traditionally used solutions such as firewalls, web and email filters, protected browser areas, and antivirus programs. With these conventional actions, authorities struggle with reliable detection from zero-day attacks, advanced persistent threats, or always-refined ransomware Trojans. The reason: These solutions rely on the detection of known malware software, but traditionally, the suppliers of security tools are always lagging one step behind the attackers.

PREPARED FOR ALL HAZARDS IN THE FUTURE

As the central IT service provider of the municipality, the supreme state authority IT Baden-Württemberg (BITBW) decided on the application-isolation solution Secure Platform by Bromium, the pioneer of micro-virtualization on endpoint devices. “In Baden-Württemberg, we are continuously working on data security. With the new technology of micro-virtualization, the IT system of the state can be even better protected in the future against non-detectable malware software,” explained State Minister Director Stefan Krebs.

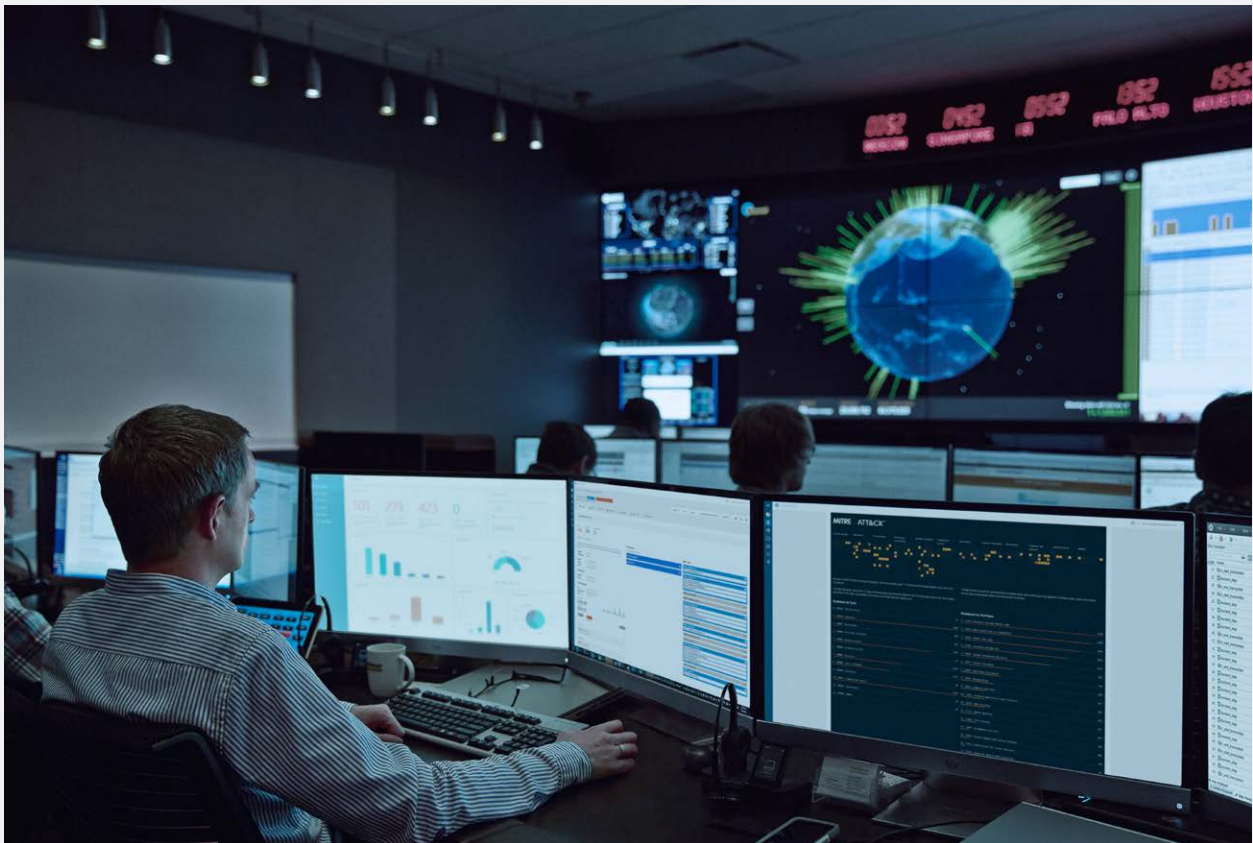


IT service provider Computacenter supported BITBW in the implementation. Computacenter set up a test environment according to BITBW’s specifications and checked the Bromium software under real-world conditions. After the successful proof of concept, the software has been used comprehensively on all clients of the ministries and other service areas of the state since 2020.

THE MOTTO: ISOLATION INSTEAD OF DETECTION

A core part of 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 Secure Platform 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.

“The optimization of actual security is an ongoing topic in which all aspects are to be taken into account in the sense of a 360-degree analysis,” said Christian Leinert, President of the BITBW. “The Bromium solution offers a very high level of security. We expect even more effective protection of the client and rely on the fact that, in reaction to the improvement in usability, we can forego other security mechanisms.”



ABOUT HP SURE CLICK ENTERPRISE

Powered by the former Bromium Inc.'s industry-leading containment technology, HP Sure Click Enterprise¹ 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

ABOUT BITBW

The superior state authority IT Baden-Württemberg (BITBW) is the central IT provider of the municipality. The BITBW was founded on July 1, 2015 as the core of the new IT ordinance. The product portfolio includes the operation, maintenance, and further processing of the state IT system. All setups and service centers directly from the municipality acquire IT services as customers from the BITBW. Currently, the BITBW has almost 500 employees.

Learn more about BITBW at www.bitbw.de

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.

© Copyright 2021 HP Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

4AA7-7795, Rev 1, June 2021