Bromium®

OVERVIEW

# BROMIUM PROTECTED APP

## Isolate and secure Windows applications that directly access your IP

### Protecting Your Intellectual Property

Intellectual property (IP) theft is at an all-time high, despite dramatic technological advancements in the last 30 years. Data breaches and the resulting theft of IP may cost the US $600 billion in losses annually[1]. To protect IP, organizations need to defend their high-value data, controlling which users and applications have access.

Traditionally, organizations use network segmentation or virtual desktop infrastructure (VDI) to control access. Both approaches provide some level of security, but like other defense in depth security solutions, can be easily bypassed by abusing application vulnerabilities.

> *"The perimeter has died. It is safe to consider the impenetrable network perimeter officially dead, as our data, applications, and devices cannot predictably be found in the networks that reside behind perimeters."*
>
> IDC[2]

### Separation and Access Control Does Not Solve the Problem

Using VDI to separate end-user host machines from high-value services is a viable option. But if the end-user PC is compromised, the VDI services in the datacenter or cloud infrastructure are at significant risk:

- Data leakage via clipboard/upload/download
- Stolen credentials being used to log in by automated scripts
- Exploits to the VDI host by the Remote Desktop Protocol (RDP) viewer

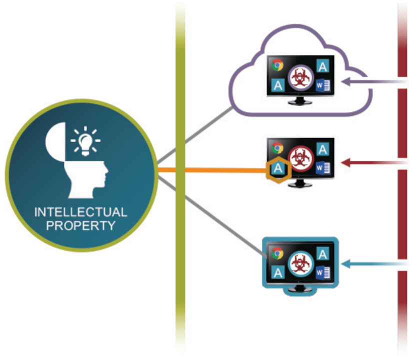
Despite application access controls for business partners, agents, suppliers, or contractors, authentication alone does not ensure application security. The business may require that third parties have access to some of your core applications, and they may have compromised hosts that you cannot control.

> *"Organizations that isolate and remove digital business services from direct public internet access will experience 70% fewer successful attacks than organizations that didn't adopt isolation."*
>
> Gartner[3]

## Protect Your IP with Hardware Isolation

Bromium is the leader and a pioneer of application isolation, and is revolutionizing security using virtualization to protect malware from infecting Windows hosts. With Bromium, organizations prevent the host from malicious activity by hardware-isolating common threat vectors inside micro-virtual machines (VMs).

The virtualization approach also works in reverse — isolating the Windows applications that have direct access to your IP. This helps safeguard your applications against malware and protect your data by keeping applications completely separated from the host PC.



### Hardware isolate applications accessing your IP with Bromium Protected App

## Bromium Protected Remote Access

Bromium Protected Remote Access provides a secure virtual extension of enterprise network access via the RDP/ICA client in a hardware-enforced VM. The protected RDP/ICA client is not visible to the host, and, if the host were compromised, the Bromium Protected Remote Access Client remains isolated and untouched.

### Security Features:

- The protected VM is isolated by Bromium's microvisor technology
- Uses the latest Intel and AMD CPU technologies to prevent host software from tampering with memory (VT-x, VT-d, UEFI secure boot, and TPM)
- Keylogging and screen-capture obfuscation techniques
- User and application authentication for secure network segmentation
- Application audit logging
- Application control

Citations

1. The Theft of American Intellectual Property: Reassessments of the Challenge and the United States Policy, February 2017

2. "Validating the Known: A Different Approach to Cybersecurity," IDC Perspective, October 2017

3. "It's Time to Isolate Your Services From the Internet Cesspool," Gartner, November 2017

### About Bromium

Bromium is the leader in application isolation. We pioneered virtualization security to protect your brand, data, and people using our patented hardware-enforced containerization with application control, and a distributed Sensor Network to protect across all major threat vectors and attack types. Unlike detection-based techniques, Bromium automatically isolates threats and adapts to new attacks using behavioral analysis, and instantly shares threat intelligence to eliminate the impact. Our technological innovations have earned the company numerous industry awards. Bromium counts a rapidly growing set of Fortune 500 companies and government agencies as customers.

Bromium

**Bromium, Inc.**
20883 Stevens Creek Blvd.
Suite 100
Cupertino, CA 95014
+1.408.213.5668

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

**For more information**
visit Bromium.com or write to
info@bromium.com.