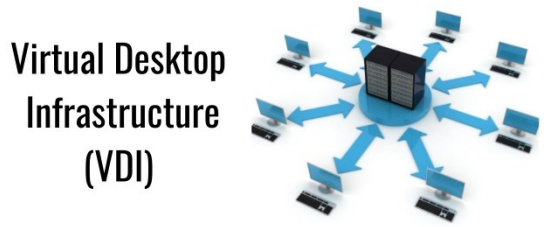
CISO Executive Forum
Using Containerized Workstations to Achieve Zero Trust

This CISO Forum took a detour from the normal vendor-agnostic focus as a result of Tim and Sandy Dunn's extensive research around ways to Enable GenAI Securely.

We ran across a solution called Kasm which is a modern-day VDI tool that leverages Docker to create containerized workspaces.

DISCLAIMER: My apologies up front for this being more single-vendor-focused. Please note there are other VDI and Secure Browser tools such as Citrix, VMWare, Island, Talon, X-Layer to also consider. Our research found that all of those solutions required an end-user agent that either requires much more complexity and cost to implement, or they did not provide the isolation to enable full DLP and protection on the BYOD device.



POLL STATS from Attendees:

- 77% of employees are working remotely at least 50% of the time.
- At least 69% of the workload is spent accessing apps through a browser.
- 69% were not using secure browsers.
- Concerns included: Patch management, Cost and complexity to manage endpoints, DLP/Insider threats, Minimizing attack vectors, Ransomware, Securing BYOD, Data Privacy/Exfiltration, Limiting lateral movement, and Speed to deploy new technologies.

The Kasm containerized workspace solution solves many of these technical challenges by leaving zero footprint on a user's device. Therefore, we invited in John Papazian, a solutions consultant with Agile Directive who has implemented the solution to present Kasm's use cases.

Here is a summary of some of the use cases discussed:

1. **Prevent Sensitive Information Disclosure -** Built for military Intelligence on FedRamp approved technology. Containerized workspaces can monitor, isolate, and lock down all data, as required, preventing data loss or inappropriate use.

2. **Ransomware Protection -** Safely open any authorized websites or click on any email link without worry. These workspaces prevent threats from going anywhere destructive.

3. **Ready For Work -** Prebuilt Secure Workspaces that can be turned on instantly for Remote Workers to quickly scale on a lower-cost OPEX consumption model.

4. **Enabling BYOD For Everyone –** Instantly give Employees and Contractors access to the necessary apps they need without sending out desktops, laptops, or other assets.

5. **Reduce IT Costs –** Simplify end-user management and costs by eliminating the need for end-user virus protection, individual VPNs, DLP, system and application patching, desktop support, or hardware upgrades.

6. **Work Your Way -** Enable the use of Windows, Linux, and Mac - AT THE SAME TIME - on any device, plus use any Cloud (AWS, GCP, Azure, etc), On-Prem, or any combination of them to make users more productive.

7. **Isolated Workspaces -** Create an impenetrable boundary between personal apps, web apps, and business apps to prevent cross-contamination and data loss.

8. **Enable GenAI Securely** – Enable users to leverage GenAI and Chatbots, as appropriate, without the worry of data loss or propagating threats created by AI.

9. **Privacy/GDPR Protection** – Protect users from outsider threats by locking down sites, sharable IP, location, content, and personal data. Since no local agent is required on the device, authorized users across the globe can use BYOD devices to access data in other countries without GDPR or legal concerns.

10. **Easy Implementation** – Most implementations take less than a day to set up across the entire institution.

John explained the product is completely isolated in the servers/cloud, so there is no footprint trace on the local device. The containerized workspace enables four types of applications: secure browsing, cloud applications, on-prem applications, and the full desktop itself.

Tim Howard emphasized the effectiveness of delivering video through the platform with minimal degradation so video conferencing works well and it lightens the load on the endpoint.

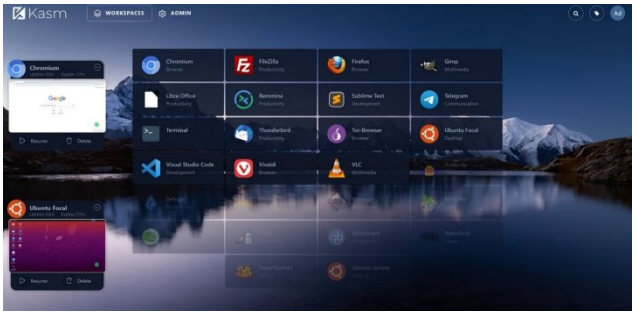
Test drive a Kasm Workspace Desktop:

https://agile-directive.kasm.cloud/#/cast/desktop

Test out a Kasm-Enabled Safe Brower at the same time: https://agile-directive.kasm.cloud/#/cast/kiosk

NOTE: Expand the Arrow on the left side for controls

Kasm Presentation Download Link



To learn more about Kasm call Tim or schedule a meeting here.

FAQ's by CISOs

1. **What about the challenge of customer persistence and customization?**

   User persistence is a feature within Kasm. The user can control when to pause, delete, or reset back to base. The session configuration can also be imaged as to create a new base. The user's profile details can reside in a separate location from the session allowing for the profile to reconnect to a new session in the event the data center goes down.

2. **How does a containerized workspace address the need for high availability and failover?**
   Kasm manages the high availability and failover itself. The feature allows for failover to occur not only across multiple data center regions but also across multiple cloud providers. To the user, the experience is invisible, and the switch happens in real-time.

3. **What value does containerized workspace bring to zero trust?**

   As discussed, Zero Trust is a framework. A key tenant of the framework is for systems to speak directly with the upstream or downstream system. Intermediaries, for example, 3rd party authentication though valuable may be seen as lowering the trust.

   a. The container locks down the workspace, hardens it, and reduces the intermediaries between the user and the resource.
   b. It provides strong identity for each container and isolates the endpoint
   c. It enables secure data delivery and control.

4. **Can virus protection be used at the endpoint if it is required to comply with PCI DSS?**

   First, yes absolutely virus protection can be installed. Applications such as Citrix, VMWare and Island.IO place agents on the local device. In PCI DSS terms, the endpoint is considered the local device. Kasm is isolated from the local device. There is no code or processing that occurs on the local device. The activity, happening in the Kasm workspace is 'rendered' to the local device. Like watching TV, therefore, no local protection should be needed.

5. **Is Kasm FedRamp approved?**
   FedRamp has approved all the components found in Kasm. However, more importantly, Kasm meets STIG security requirements meaning that it can run in an isolated or air gapped mode. This deployment model can run in the government agency's data center or private cloud without any needs from the internet and can be hardened per STIG guidance. Government agencies can deploy Kasm.

6. **Does it have multi-language Support?**
   Auto-translation is provided in real-time for many languages.

Join us for next month's CISO FORUM discussing:

How to use AI in your Security Program to Become more Efficient and Effective.
Registration Link: Zoom Registration Here – Thursday, November 16th, 1:00 pm CST