



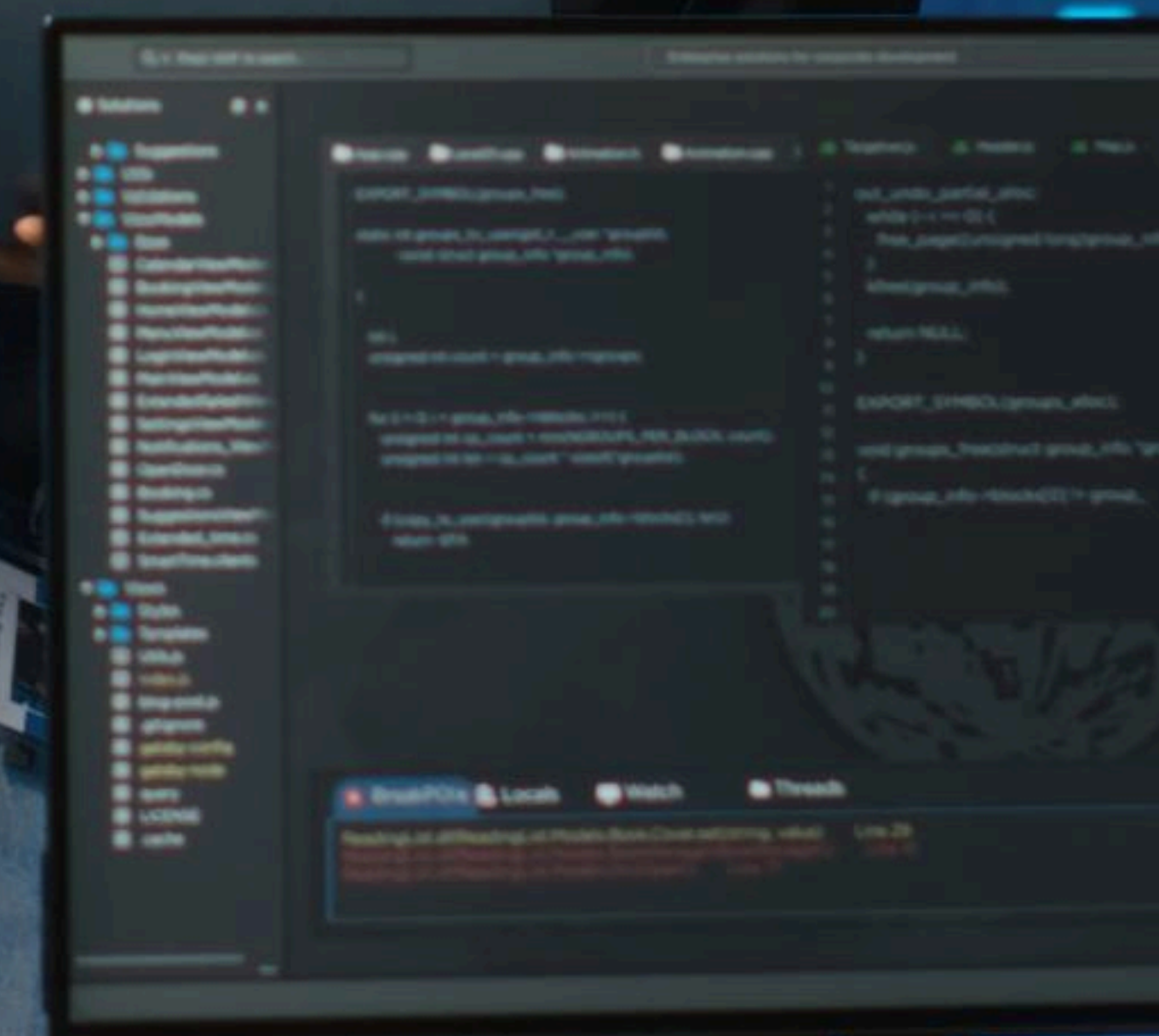
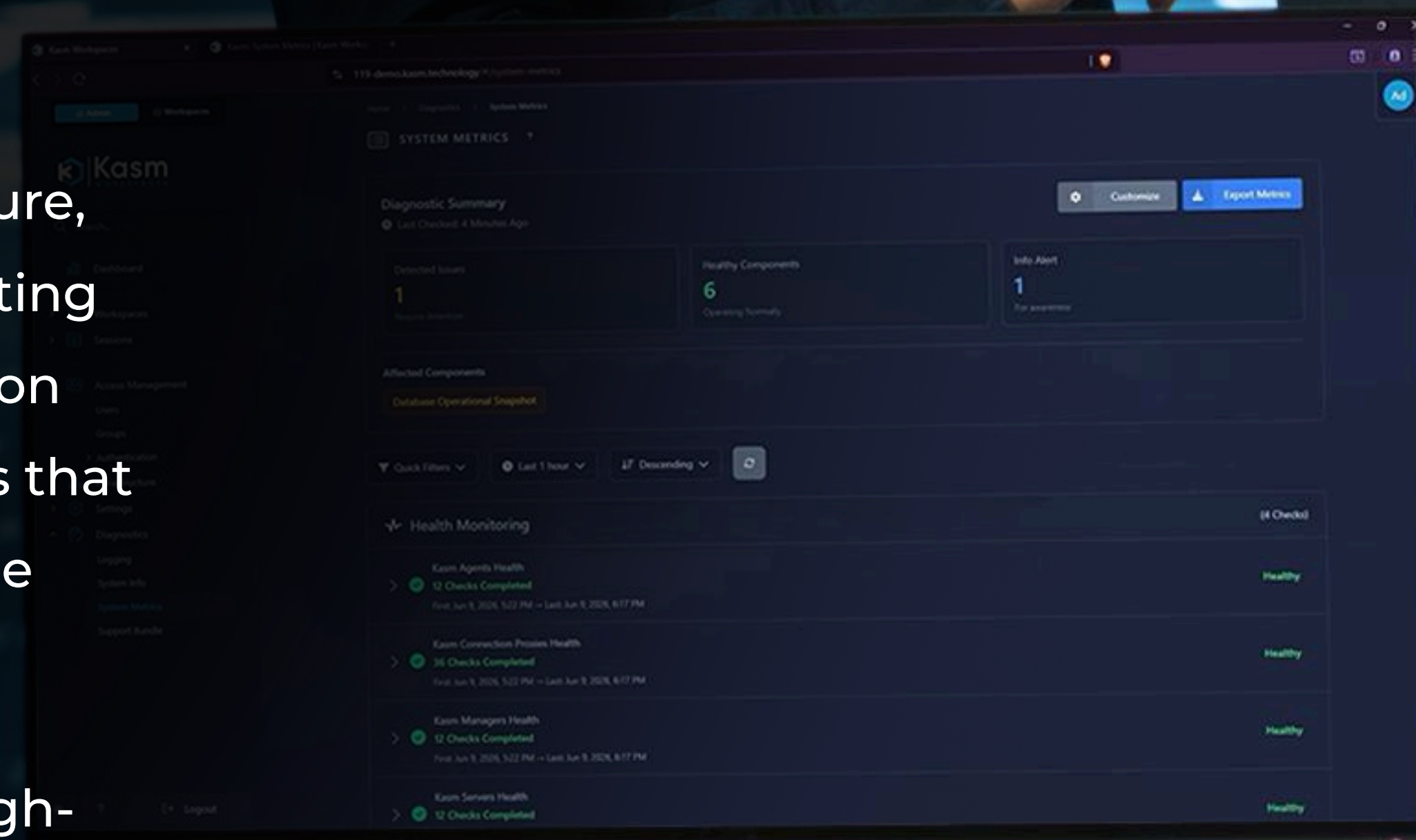
Web Isolation

Isolate Risk. Enable Secure Access.

Modern organizations rely on the web for research, collaboration, SaaS applications, and day-to-day operations. Yet every browsing session introduces risk—from malware and ransomware to credential theft and data exfiltration.

Kasm Web Isolation delivers every browser session inside a secure, isolated workspace that is streamed to users through their existing browser. Rather than allowing web content to execute directly on corporate endpoints, Kasm creates disposable browser sessions that are destroyed when work is complete, dramatically reducing the attack surface while giving users the experience they expect.

Whether protecting employees, contractors, third parties, or high-risk research teams, organizations can safely enable web access without sacrificing security, performance, or productivity.



Business Challenges

Organizations face growing challenges when securing web access:

- ✓ Malware and ransomware delivered through malicious websites
- ✓ Phishing attacks targeting user credentials
- ✓ Browser-based exploits and zero-day vulnerabilities
- ✓ Users accessing untrusted websites during investigations or research
- ✓ Balancing security with user productivity
- ✓ Protecting sensitive environments without restricting access

Traditional browser security solutions often rely on endpoint agents, complicated infrastructure, or restrictive policies that frustrate users.

Why Kasm

Traditional browser security solutions often rely on endpoint agents, complicated infrastructure, or restrictive policies that frustrate users.

Key Benefits

- ✓ Browser sessions run in isolated containers
- ✓ Zero Persistence™ ensures sessions are destroyed after use
- ✓ No software required on user endpoints
- ✓ Supports cloud, on-premises, hybrid, and air-gapped deployments
- ✓ Fine-grained policy controls for downloads, uploads, clipboard, printing, and more
- ✓ Centralized management with enterprise scalability



Enterprise-Ready Web Isolation

Key Capabilities



Disposable browser sessions



Policy-driven browser security



Integration with existing identity providers



Role-based access controls



Download, upload, clipboard, and printing controls



Session recording and auditing



Secure access from managed and unmanaged devices



Support for isolated, disconnected, and highly regulated environments



Built for Modern Enterprises

Ideal for:

- ✓ Government agencies
- ✓ Defense and Intelligence organizations
- ✓ Financial services
- ✓ Healthcare
- ✓ Critical infrastructure
- ✓ Enterprise security teams
- ✓ Managed security providers

Related Use Cases

Secure Web Research (OSINT)

Allow analysts, investigators, and cyber teams to safely research suspicious websites, threat intelligence, and external sources without exposing corporate infrastructure.

Learn more about the **Web Research (OSINT)** use case.

Browser Isolation

Provide every employee with secure web browsing by isolating browser sessions from endpoint devices while enforcing organizational security policies.

Learn more about the **Browser Isolation** use case.

Why Organizations Choose Kasm

Unlike traditional browser isolation products, Kasm is part of a broader platform powering secure work.

Organizations choose Kasm because it enables them to:

- ✓ Protect users without changing how they work
- ✓ Deploy anywhere—cloud, on-premises, hybrid, or air-gapped
- ✓ Integrate with existing identity and security infrastructure
- ✓ Support Zero Trust initiatives
- ✓ Scale on modern infrastructure, including Kubernetes
- ✓ Extend the same platform to remote desktops, applications, secure remote access, and AI environments



Protect users without compromising productivity.

Request a Demo



Talk to Sales

