



eBook

# **WFH Cybersecurity: 5 Critical Questions You Should Ask**



# Do you really know who's looking at your most confidential data? Documents travel the globe to employees, contractors, business partners and collaborators.

That's a lot of opportunity for leaks. WFH creates new cybersecurity hazards.

It's impossible to lock down all those computers manually and ensure they stay that way. Answer these five questions to find out if your security posture is all it can be.



# 1. Do you really know who's looking at your data?

You've locked down everything. You think you have great endpoint protection -- but the edge of your network is now in someone's living room. Do you really know who can see the screen?

Use artificial intelligence and facial verification to create a safe zone around the edge of your network, wherever it is. AI-powered biometric verification allows only authorized users. If the authorized user looks away or invites someone to look over their shoulder, the screen blurs. If someone tries to take a screenshot or point a smartphone camera at the screen, they're blocked.

endpoint protection





# user restrictions

## **2. Do you prevent users from taking screenshots of confidential information?**

There are so many ways to game the system. If someone wants access to source code, contracts or other proprietary data, they've got a hacker's encyclopedia of workarounds.

Can you confidently prevent your WFH employees or contractors from printing or saving documents to their home PCs? Can you really enforce a "clean desk" policy? What about blocking screen sharing, or copy/paste a key passage into a chat thread? Even trusted, well-meaning employees can accidentally send or share docs if they have them locally. Can you provide these players a safe environment? And when the bad actor tries to get past digital security in place, they must be shut down, not simply identified after the fact.



### **3. Do you have project-specific encrypted email capability?**

In many organizations people use company email to send and receive documents. Sure, there is confidentiality or ownership language at the bottom of the message, but that's never stopped anyone from downloading and sharing. Most of the time, it's innocent. But it takes only one slip to create a data breach that could cost your company millions of dollars, and your reputation.

Instead, consider a secure project-specific platform that includes an entire isolated, dedicated email system. Correspondence, metadata and document attachments are never vulnerable. It's all firewalled and protected. Email only goes to and from pre-authorized users. Important messages and documents stay inside the project bubble.

# it only takes one slip





## 4. How many factors of authentication do you use to protect your data?

You think you know who's at the edge of your corporate network. But maybe you don't. Perhaps a spouse, roommate, or other household member shares a computer with your employee or contractor.

### **Authentication factors can include:**

- Facial Verification
- Authorized Computer Verification
- Authorized IP Address
- Additional Multi Factor Authentication
- User Credentials

Each factor of authentication increases the security of the system and reduces the chances for unauthorized access. In a COVID-19 WFH world, strong authentication mechanisms are key to maintaining operational security.

## 5. Are you well protected against hackers and malware?

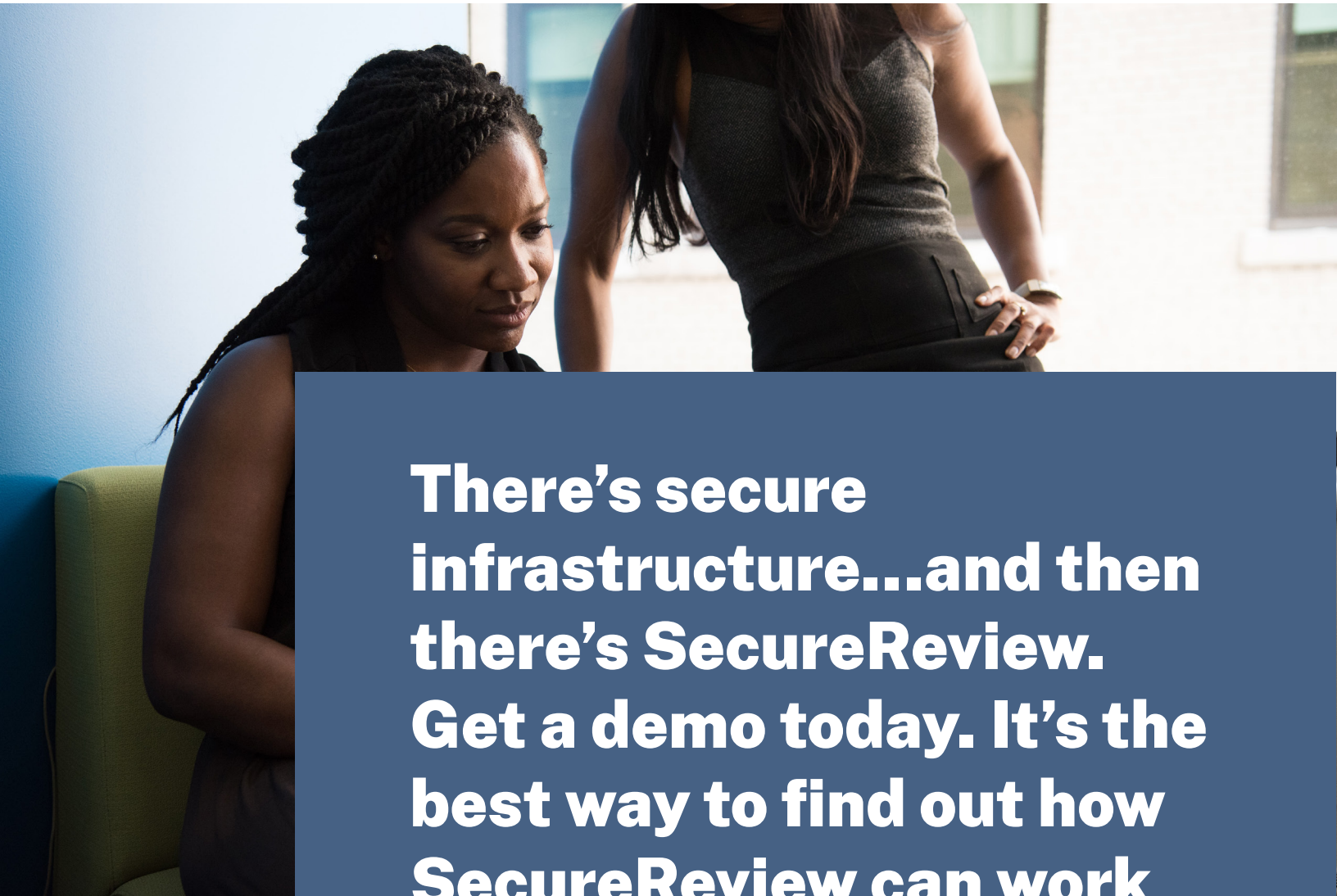
COVID-19 means that people are working from home, creating a potential hacking bonanza. It is critical to not only separate users from data with virtual machines, but also to ensure that defenses are in place to thwart a hack attack, especially when people use their own computers.

The right solution employs security mechanisms that track project, workspace and user lifecycles, as well as any administrative activity by IT personnel. Make sure you have a rotating network activity log tracking all user connections within the network, as well as between workspaces and designated cloud endpoints. Internet access should be on a whitelist-only basis so that malware and ransomware that may be present in the environment can't "call home," and are blocked from doing damage.

data  
details

SecureReview with SessionGuardian solves the challenges of remote work cybersecurity. With state of the art technology, you keep confidential documents in front of only the right people, at only the right time, in only the right place.

The Security as a Service platform works with Citrix, Azure Virtual, AWS workspaces and many more. Implement the full SecureReview platform, or sign up for SessionGuardian Enterprise to integrate with existing hosted virtual machine infrastructure.



**There's secure  
infrastructure...and then  
there's SecureReview.  
Get a demo today. It's the  
best way to find out how  
SecureReview can work  
for you.**





# The future of workforce cybersecurity

Get started at **[securereview.com](https://securereview.com)**

 **844-303-5324**

 **secure\_review**

 **/securereview**

© 2020 SecureReview All Rights Reserved