SESSION GUARDIAN™

Transforming VDI Security

Continuous Identity Assurance and Data Protection

January 2024

ABSTRACT

Many organizations use virtualization technologies such as Virtual Desktop Infrastructure (VDI) or Desktop as a Service (DaaS) solutions as a way to provide remote workers and third parties access to business-critical systems, applications and data. These technologies provide standardized desktop environments, enhanced security, and centralized management and control. Even with the added security there continue to be risks associated unauthorized access to sensitive data and data leakage.

To address these concerns, many organizations layer other security tools such as Multi-Factor Assurance (MFA). However, relying solely on MFA may fall short in scenarios where an end user shares the code with an unauthorized party to gain remote access and work on the system.

While VDI and DaaS solutions can prevent exfiltration of data from an organization's network they cannot protect sensitive data from screen capture or photos once the data is displayed on the end-user's device.

The only solutions that can close these gaps are ones that provide continuous identity assurance with biometric authentication and continuous data protection by preventing the capture, share and unauthorized viewing of data once the data is displayed on the end-users screen.

SessionGuardian VDI enables organizations to further secure their sensitive data and business critical applications from access unauthorized users as well preventing screen capture, screen print and attempts to photograph data on the screen.

THE NEED FOR CONTINUOUS IDENTITY ASSURANCE

In response to the COVID-19 pandemic, and even earlier for many technology-focused or dispersed industries, remote work has become more commonplace in average organizations than ever before. The swift shift to remote work, driven by the pandemic, caught many organizations off guard, as they were unprepared for the security demands that remote infrastructures necessitated. According to the OECD (2020), "most organizations' digital ecosystems [were] placed under high stress."

The readiness for a dispersed workforce was not typically a concern for smaller organizations before, often only considered within the context of a business continuity plan for environmental disaster recovery of critical business operations. However, the COVID-19 pandemic accelerated the need for remote work, compelling widespread industries into immediate adoption. This sudden shift tested information security infrastructures and policies globally, as remote work quickly became the new standard. With this accelerated schedule for remote work growing, it is important to note that in a 2020 study, “Gartner projected that 47 percent of employers plan to let workers work remotely full time moving forward. In addition, 82 percent of business leaders … plan to allow employees to work remotely at least some of the time as they reopen closed workplaces” (Zielinski, 2020).

The zeitgeist of work environments has been permanently changed to be largely inclusive of fully remote or hybrid work environments and is a movement current literature and organizations are confident is not changing moving forward.

Remote work, in its current state, is viewed by information security experts with concern, with “77% of SMEs See[ing] Remote Work as a Security Risk” (Cawley, 2022). Largely, Cawley’s study identified that primary risk concerns were due to an inability to confirm that resources were being securely used and were not left unmonitored. Specifically, the underlying concern boils down to a direct security concern related to verifying that authorized users were the ones accessing sensitive material and were restoring its security through locking the system or logging off safely once the need to access the systems concluded.

The abundance and push towards remote work has been further fueled socially through many employees requesting remote opportunities over in-office employment and coupled with the COVID-19 pandemic push towards this work format, has become a permanent stay in the global economy. Coupled with the seen security hesitation, it has become clear that remote work will continue, and requires robust solutions such as continuous identity assurance to protect organizations in their dispersed security postures.

With regards to SessionGuardian’s continuous assurance approach, the ability to continually authorize an end user predetermined by the organization to have access to a virtual machine or web-based work such as specific applications and websites fills this security need. By performing continuous assurance and authorization checks paired with liveness detection, the application is able to ensure the three primary goals identified, by:

1. Mathematically verifying the end user through biometric calculations for verification,
2. Empower remote workforces to meet the new workforce push for ‘work anywhere’ opportunities through offering security capabilities, and
3. Allowing organizations to ensure that their sensitive systems and information are unable to be left unattended or viewed by unintentional parties, as verification checks will lock down information when an authorized user is not found and can prevent the viewing of information when a second party is identified.

PROTECTION AGAINST INTERNAL DATA LEAKS

A data leak, by definition, can occur either intentionally or accidentally, originating from either an internal or external source. While the common perception revolves around safeguarding against deliberate external attacks, a surprising 2017 study revealed that internal accidental leaks accounted for "43% of corporate data leakage incidents, and half of these leaks are accidental" (Cheng et al., 2017).

Amidst the COVID-19 pandemic and the surge in remote work, accidental employee data leaks have become a heightened concern for information security departments. A study by Stealthlabs in 2020 found that 97% of these departments are specifically worried about internal data leaks in the context of remote work. As remote work continues to witness exponential growth, fueled significantly by the ongoing pandemic, the apprehension surrounding internal data leaks has become a critical facet of risk management efforts that demands immediate attention.

The primary risks associated with unintentional internal data leaks often stem from seemingly innocuous actions that may not appear overtly dangerous at the time. However, these actions can lead to financial, reputational, regulatory, or competitive damages. While it's evident that organizations can suffer losses such as trade secrets or expenses to rectify errors, regulated industries face additional risks, such as compliance incidents that unintentionally violate regulations like HIPAA.

These compliance incidents may involve actions like accidentally emailing sensitive information, leaving unlocked applications accessible to unauthorized users, or accessing sensitive data in the presence of unauthorized individuals who can 'shoulder surf' to view information without authorization. Historically, remote work has struggled to prevent these accidental data leaks. However, continuous identity assurance technology, particularly in biometric security like the SessionGuardian application for remote or on-premises work, has emerged as a solution.

This technology enhances endpoint security, helping end users avoid inadvertently causing organizational harm. In instances of biometric security, SessionGuardian restricts workspaces and sensitive information, safeguarding against shoulder-surfing by identifying more than just the authorized user. Secure sessions also offer protected email capabilities, preventing the accidental transmission of sensitive information to unauthorized users. Through continual identity assurance, these sessions lock down all sensitive information if the authorized user is not positively identified.

By leveraging these capabilities within secure continuous identity assurance applications as part of an organization's security infrastructure, the risk of accidental data leaks can be significantly mitigated.

PRIVACY AND PROTECTION

The importance of Continuous Identity Assurance in a security infrastructure is shown through the need of protecting sensitive information remotely during the push towards remote work. Additionally, with the usage of any security solution that interfaces directly with end users, questions related to end user privacy and data protection arise. Socially conscious workplace efforts have been demanded more consistently by employees and end users of platforms, especially in remote work environments. Through a 2021 study, it was identified that the end user's trust in coworkers, employer and/or contractor directly influences their work productivity and quality when working remotely (van Zoonen et al., 2021). A large component of employer and contractor focused trust during the COVID-19 pandemic remote environment and persistent remote work opportunities is a concern over employer spyware in which employers and contractors monitor the behavior and actions of employees whether disclosed or secretly. In a recent study of remote work during the COVID-19 pandemic (Zielinski, 2020) it was identified that "73% of employees feel that introducing technologies to monitor the workplace would damage trust between them and their employers." With review of the study by van Zoonen et al. (2021), it is noted that employee trust directly relates to their work quality, by which these monitoring tools pose a significant risk. Additionally, "43% [of employees] are concerned that the introduction of workplace monitoring technology could make it easier for their privacy to be violated" (Zielinski, 2020) which strengthens the data privacy and trust concerns employees are presenting for remote work opportunities. Due to these concerns, it is vital that organizations select an access control and authorization solution that does not infringe upon end user trust or data privacy.

CONCLUSION

Continuous Identity Assurance software is a term that can bring hesitation to the discussion when spoken or written, however may be largely misunderstood in the software solutions they are implemented alongside. Certain employee monitoring applications exist and are regularly implemented with “26% of HR leaders report having used some form of software or technology” (Zielinski, 2020) to monitor their employees.

These software and others that claim Continuous Identity Assurance may be able to record or stream video of the end user accessing sensitive information or a restricted workspace as the “continual” portion of identity assurance, however these solutions largely fall short and damage employee trust and subsequently performance. Instead, Continuous Identity Assurance methodologies implemented such as in the case of the SessionGuardian application perform biometric identity verification checks on the local machine where the application is installed. Therefore, under no circumstances is there a video or photographic stream recorded or sent of the end user, as the software works under the same framework as facial verification for mobile device “passwords,” or facial scans completed to instantly analyze an authorized user in a restricted facility.

These biometric points are, when viewed, immediately compared against data points associated with the user locally, and therefore have no recording potential. Continuous Assurance proves to be a consistently developing field of access control study, and the impacts of choosing the incorrect solution are dire with a loss of employee trust and decrease in work performance. Therefore, while a critical technology to review for business application, it is important to consider applications such as SessionGuardian that fill gaps in an organization’s security posture without negative impact to the end user.

REFERENCES

A migud, A., & Lancaster, T. (2019). 246 reasons to cheat: An analysis of students' reasons for seeking to outsource academic work. In Computers & Education (Vol. 134, pp. 98–107). Elsevier BV. https://doi.org/10.1016/j.compedu.2019.01.017

Cawley, C. (2022, February 17). Study: Remote work leads to increased cybersecurity risk. Retrieved March 2, 2022, from https://tech.co/news/remote-Work- increased-cybersecurity-risk

Chappell, B. (2013, January 16). Outsourced: Employee sends own job to China; Surfs Web, from https://www.npr.org/sections/thetwo-way/2013/01/16/169528579/ outsourced-employee-sen ds-own-job-to-china-surfs-web

Cheng, L., Liu, F. and Yao, D. (2017), Enterprise data breach: causes, challenges, prevention, and future directions. WIREs Data Mining Knowl Discov, 7: e1211. https://doi.org/10.1002/widm.1211

OECD (2020) Seven lessons learned about digital security during the COVID-19 crisis. OECD Policy Responses to Coronavirus (COVID-19). doi:10.1787/e55a6b9a-en

Stealthlabs (2020, December 22). 2020 insider data breach survey: 97% it leaders consider insider threats as a major concern. Retrieved March 3, 2022, from https://www.stealthlabs.com/blog/2020-insider-data-breach-survey-97-it- leaders-consider-insider-threats-as-a-major-concern/

van Zoonen, W., Sivunen, A., Blomqvist, K., Olsson, T., Ropponen, A., Henttonen, K., & Vartiainen, M. (2021). Factors Influencing Adjustment to Remote Work: Employees' Initial Responses to the COVID-19 Pandemic. International Journal of Environmental Research and Public Health, 18(13), 6966. https://doi. org/10.3390/ijerph18136966

Walkowski, D. (2019, July 09). What is the CIA triad? Retrieved March 2, 2022, from https://www.f5.com/labs/articles/education/what-is-the-cia-triad

Zielinski, D. (2020, August 08). Monitoring Remote Workers. Retrieved March 2, 2022, from https://www.shrm.org/hr-today/news/all-things-work/pages/monitoring- remote-workers.aspx