REMOTE WORK WITH

Plurilock

Welcome to the Remote Work Era

Remote work is no longer just a lifestyle choice. As we're seeing, it's also a way to protect staff and maintain operations when facts on the ground make onsite work impossible. Security can be forgotten when this happens, as companies work rapidly to get users connected. Unfortunately, attackers know this—and are ready to seize the moment.

Why You're Not Ready

Remote work makes cybersecurity—and authentication in particular—more complex:

- In an office environment, face-to-face authentication happens constantly; workers recognize nearby co-workers and apparent strangers are questioned.
- In minimally-staffed offices, the few that are present may not recognize others with whom they don't normally work, making it harder to spot strangers.
- Phones, hardware authenticators, and other traditional 2FA devices can be used by anyone holding them; they don't guarantee actual identity.
- After login, open sessions can be seized by anyone with access to a workstation or network; further checks are rare.
- Unauthorized access to systems and data can be a serious risk or liability even without malicious intent. If not prevented from doing so, in informal environments friends, family members, or others may inadvertently access sensitive systems and data—with catastrophic results.

Why Plurilock Can Help

- Plurilock prevents credential-based attacks—credential theft, sharing, stuffing, and re-use—at login.
- Plurilock prevents unauthorized users from using remote systems, even after login or in already open sessions.

Our Solutions

- **Plurilock ADAPT** enables biometric strong, privacy-friendly MFA—without the delays or costs involved in deploying YubiKeys or RSA tokens, and without any reliance on users' personal mobile devices.
- **Plurilock DEFEND** checks for the presence of authorized users all day long, as they work, in the background—ensuring that attackers, strangers, and household members aren't able to step in and compute.

Our solutions recognize authorized users by observing patterns in typing, pointer movement, and other moment-by-moment details that are as unique as fingerprints. When a stranger is detected, they are kept from logging in—or logged out just seconds after they appear.

Unlike other behavioral authentication tools, Plurilock doesn't monitor activity—only the numeric measurements that result from regular bodily movement.

No transmission or storage of browser visits, files accessed, words typed, fingerprints or faces scanned, or other identifying data is required. Plurilock is remarkably secure—yet ready for high-privacy environments.

Plurilock safely answers the key question of the remote work era: "Is this really them?"

Is this really them?

In remote work situations, recognized credentials and traditional 2FA simply don't guarantee that the user on the other side of the screen is the intended user.

Plurilock protects remote workers and their employers. Contact us www.plurilock.com

Plurilock

Secure Your Remote Users and Ecosystem

If your company is among the many that have rapidly arrived in the work-from-home era this year, it's important that you not remain complacent about security. Practices and solutions that work well in office environments can add new risks when a workforce is remote. Survey this list and take action where necessary to ensure that your systems and data remain secure.

	Action Item	Notes
Basic Security and Hygiene	**Force password resets across all devices and systems**	**Reason** Eliminate any hidden bad password hygiene, shared passwords, or widely-known passwords, slow or stop account sharing. **Advice** Where possible, impose new passphrase-oriented rules: • Minimum 12 characters • Combinations of unrelated words • Easily memorable to prevent password write-downs
	Authenticate during work sessions, not just at login	**Reason** In remote work situations, employees may work in and around parties unrelated to the company, and in environments where they may step away from their machines without remembering to log out of secure applications or services. **Advice** For general work, deploy a behavioral-biometric solution providing true continuous authentication, like Plurilock DEFEND. To protect particular high-security workflow steps, deploy a behavioral-biometric workflow solution like Plurilock ADAPT. Avoid solutions that will buy increased in-session authentication at the expense of productivity (repeated OTP code entry) or security (increased need to carry and handle easily-stolen and easily-lost hardware OTP fobs.
	Ensure that work is being carried out by human users	**Reason** Bots can be harder to detect in remote settings where it's not obvious that an employee at a desk is the one performing tasks; employees themselves can also be tempted to take risks by automating tasks without authorization in remote work settings. **Advice** Deploy a behavioral-biometric solution able to detect the difference between human work and bot work, like Plurilock DEFEND.

Plurilock

	Action Item	Notes
Authentication	**Deploy multi-factor authentication as widely as possible**	**Reason** Passwords alone are not secure, particularly in remote environments where keyboards may be observed/observable by strangers. **Advice** Deploy a centrally-administered, low-training behavioral-biometric solution like Plurilock ADAPT. Be wary of methods that are insecure, particularly in remote settings: • Hardware OTP fobs are easily snatched • SMS is fundamentally insecure • BYOD mobiles are fundamentally insecure Be wary of methods that will require training or generate support cases, both of which are difficult to address in remote situations.
	Deploy single sign-on where possible	**Reason** Eliminates the need to remember multiple passwords, prevents oversimple passwords and password write-downs.
	Encrypt and isolate company work and assets from the external world	**Reason** Remote work may occur on untrusted networks in untrusted environments where eavesdropping and interception are far more easy to accomplish. **Advice** Stand up an internal VPN and limit company applications and data resource access to users connected to the VPN. Alternatively, rely on a VDI infrastructure to ensure that applications and data are not stored locally, but instead on secured company resources.
	Set BYOD device policies and secure BYOD devices	**Reason** In remote work conditions, it is both tempting and easy for employees to rely on their own devices for some work, particularly if company devices are more carefully secured or capability-limited. **Advice** Set clear BYOD policies and back them with technical implementations and deployments that prevent off-policy BYOD use; require that BYOD devices be secured with centralized policy and management tools, then secure productivity endpoints like Windows or Mac OS machines with continuous behavioral biometric authenticators like Plurilock DEFEND.

Policy, Contingency, and Compliance	Action Item	Notes
	Ensure the existence of an audit trail	**Reason** In the absence of premises entry and exit data, security cameras, and direct observation, attributing actions definitively to individuals is more difficult; relying on login credentials in use is not sufficient, as usernames, passwords, and OTP codes can be stolen and used by strangers. **Advice** Deploy a full-time behavioral-biometric logging solution like Plurilock DEFEND to maintain records authoritatively attributing responsibility to particular individuals, not just accounts.
	Review regulations and compliance requirements and address them	**Reason** Companies in regulated industries may face regulatory requirements about the kinds or locations of systems on which sensitive data is accessed, the locations where sensitive data resides, how these are protected, and so on. **Advice** Conduct an explicit review of compliance requirements in relation to work-from-home circumstances and needs, then list areas in which these are not aligned and address the list. Rely on VPNs and/or VDI infrastructure as a baseline to address system and data access, location, and isolation requirements, then deploy authentication and other systems as necessary to comply with authentication and other security requirements.
	Ensure the existence of alternate chains of critical responsibility	**Reason** In remote work settings, connectivity can be unexpectedly slow or unexpectedly interrupted, and individuals can be unexpectedly out of contact or unavailable, leading to potential breakdowns in emergency or crisis situations. **Advice** Establish alternate chains of action, responsibility, and sign-off for key systems and contingencies including outages, attacks and breaches, and other similar rapid-response events.
	Establish review and oversight of security and readiness status	**Reason** In remote work conditions, communication about identified risks and issues can be more easily delayed or forgotten. **Advice** Hold periodic but regular status and review meetings with key stakeholders to survey the points outlined above along with any other relevant points. Deploy a ticket system or similar avenue for centralized feedback and problem reporting from front-line users in the field that doesn't rely on simple email or phone calls to a support desk; tabulate, summarize, and review issues at periodic meetings.