# Using Zero Trust Solutions to Support Hybrid Work

## Shifting from a secure-perimeter mindset, to a secure-behavior mindset.

The commute to work once drew a sharp line between work and private life. Then the necessity of working from home caused a mad scramble to adapt IT policy to meet the changing security environment. Now as we settle into a new way of work, it is staff habits and culture that expose us to risk.

## False sense of security

We live with people we can trust, but from a company point of view, their staff homes are zero-trust environments. Private discussions can now be heard, intellectual property can be seen on screens and monitors in living rooms everywhere in the world.
—Bianca Soare, Communications and PR Officer at Heimdal Security

Workplaces do a lot to manage security that the staff don't see. What staff experience working from home appears the same as when in the office, so some may fail to recognize they don't have the same levels of protection. They may be missing:

- Email and network security
- Firewalls and port management
- File checking and backups
- Physical security
- Keeping safes and rooms locked

## Security controls that supported a zero-trust posture in the workplace need to be reconsidered:

- Device login breaks trust when the device is shared by the family
- Passwords fail to establish trust when written passwords are visible in the home office
- Home VPNs make IP address verification difficult
- Personal email and applications on PC increase opportunities for phishing and ransomware attacks
- Insecure home networks greatly increase attack surface

Zero Trust implemented at home requires higher barriers and more frequent verification, which is a paradigm shift from traditional security architectures. Supplying staff with appropriate hardware and software tools increases trust without reducing employee experience. These include:

Printers

- Code validation and reboot recovery
- Network evaluation for malware prevention
- Run-time monitoring and protection
- Fleet-wide security policy and management

Physical shutters on webcams

IR camera facial recognition

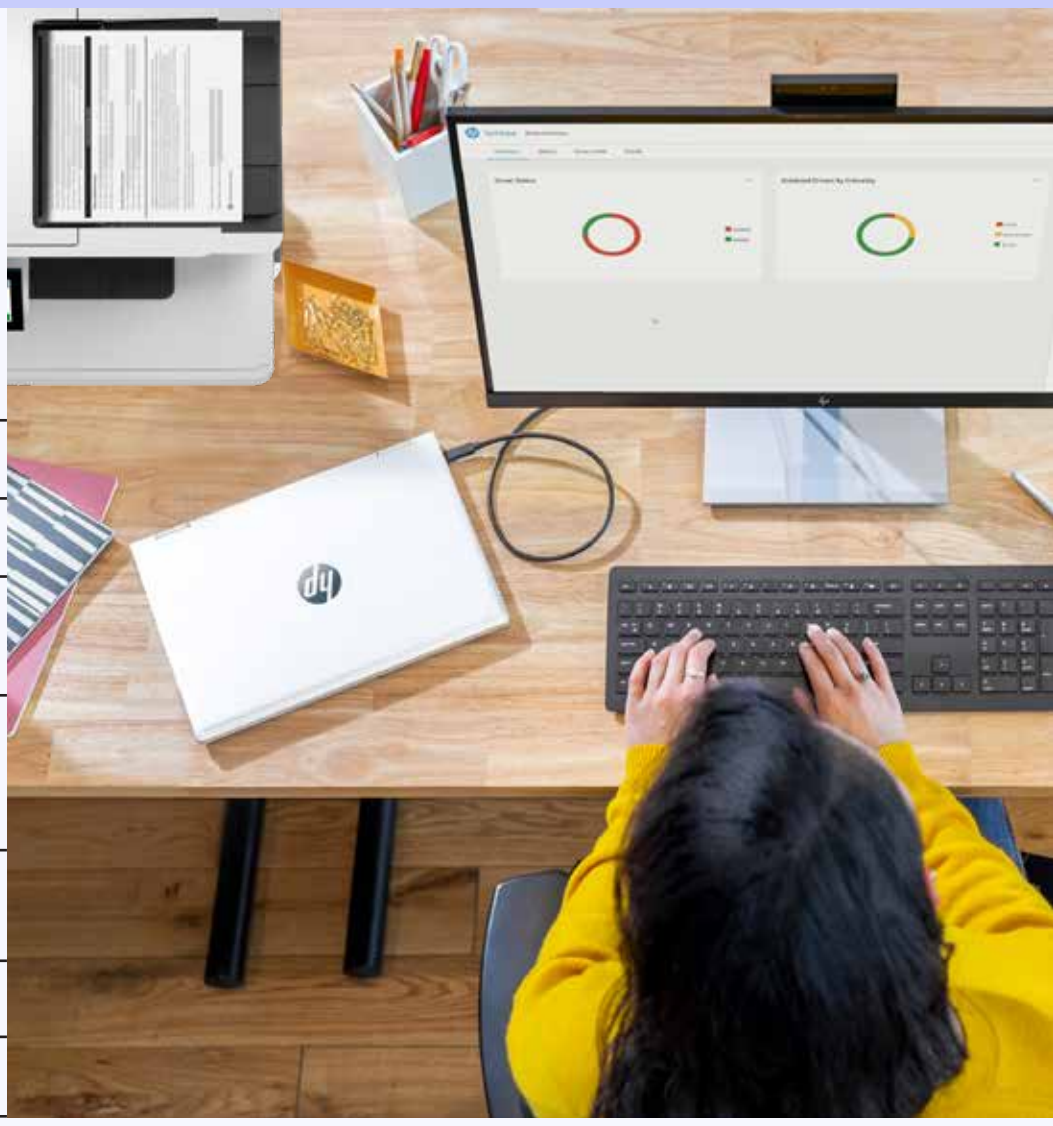
Endpoint isolation for threat prevention for each user task

PC Platform security for "full-stack" integrity (peripherals, BIOS, and recovery OS)

Increase the trust in home network security

Over-the-shoulder protection

Fingerprint scanners



By using hardware and software solutions to establish trust across endpoints and within networks, security will be easier to maintain and audit. This will improve end-user experience and drive greater availability and lower support costs. In summary, there is no better place for Zero Trust than the home office.

4AA8-1439ENW, April 2022