SOLUTION BRIEF

Security for Remote Work Environments

Remote employees present a unique challenge for IT and security teams. They sit outside the corporate network and lack the strong, reliable protections of enterprise IT. That's why the advanced endpoint protection of the Morphisec Unified Threat Prevention Platform is designed to secure endpoints regardless of where your employees work—inside or outside the corporate network.

The Higher Risks of Remote Employees

UNRELIABLE AND UNSECURE HOME NETWORKS

Home networks are inherently less secure than corporate networks. They lack the network security solutions that corporate IT teams deploy on enterprise systems for an additional layer of protection. As a result of the lack of advanced security tools, the reality of home networks is that they are far less secure than corporate ones.

INCREASED RISK OF SOCIAL ENGINEERING, BROWSER-BASED ATTACKS, AND REMOTE WORK APPLICATION EXPLOITS

Remote employees rely on web applications and secure browser access to perform critical functions. Unfortunately, this places them at higher risk of attack through exploits in these remote applications as well as the social engineering of phishing emails.

INABILITY TO REMEDIATE INCIDENTS ON REMOTE MACHINES

Remediating security incidents on a remote employee's machine is much harder, especially when IT is physically unable to have the workstation in front of them. This complicates ensuring that security incidents can be resolved.

HIGHER RELIANCE ON ENDPOINT PROTECTION SOFTWARE

On the home network, aside from basic firewalls, the endpoint is the first and last line of defense against cyberattack. This results in additional strain on signature-based, client-grade antivirus software

INABILITY TO ENSURE PROPER IT HYGIENE ON HOME COMPUTERS

Remote employees might be working with dangerous unhardened systems with an increased attack surface. Further, they might be working with vulnerable applications that leverage high privileges without the IT team's knowledge.

PROTECT REMOTE EMPLOYEES WITH MOVING TARGET DEFENSE

Morphisec provides a dedicated memory defense layer to secure remote employees with:

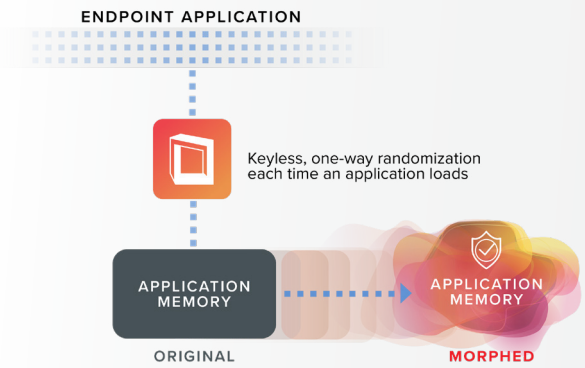
- Secure advanced endpoint protection with low-touch maintenance.
- Tight Windows 10 Defender AV integration for advanced protection and full visibility across all threats.
- Protection without updating a signature database; perfect for offline protection or unreliable home internet connections.
- Business continuity that allows remote employees to keep working in a secure environment if they can't go into the office.
- Secures virtual desktop infrastructure (VDI) and integrated with Citrix XenApp and XenDesktop, VMware Horizon and Windows Virtual Desktop.
- Protection against unknown exploit vulnerabilities, known CVEs, and unpatched software.
- Security against remote work application exploits, browser-based attacks, and social engineering.

MORPHISEC
Moving Target Defense

How Morphisec Solves the Problem

Morphisec works by morphing the application memory. This changes the memory structure of your applications and turns it from a known entity into an unknown landscape.

By doing this, Morphisec protects your applications from zero days, fileless attacks, in-memory exploits, and evasive malware. We make your application memory secure, and allow you to get back to business.



With moving target defense from Morphisec, paired with built-in Windows Defender AV, your employees have the tight security they need to work without relying on network tools that are meant to ensure those attacks never reach the endpoint in the first place.

The Morphisec platform's performance also doesn't rely on or degrade internet connectivity. Because Morphisec doesn't require access to the internet to update a signature database, unreliable networks aren't a barrier to ensuring that your employee's endpoints are protected.

This includes protection against:

- Web application exploit kits
- Browser-based attacks
- Attacks that bypass traditional AV

Morphisec's deterministic prevention technology automatically locks down the most dangerous cyberattacks, leaving nothing for remote IT teams to remediate.

The Morphisec platform also instantly hardens any workstation it's installed on, and acts as a virtual patch against vulnerabilities—ensuring that remote employee workstations are secure before a patch is released.

With more than five million endpoints currently under Morphisec protection, the Unified Threat Prevention Platform is the only solution with a truly set-and-forget deployment model that blocks more than 10,000 evasive attacks every day.

ABOUT MORPHISEC

Morphisec delivers an entirely new level of innovation to customers with its patented Moving Target Defense technology - placing defenders in a prevent-first posture against the most advanced threats to the enterprise, including APTs, zero-days, ransomware, evasive fileless attacks and web-borne exploits. Morphisec provides a crucial, small-footprint memory-defense layer that easily deploys into a company's existing security infrastructure to form a simple, highly effective, cost-efficient prevention stack that is truly disruptive to today's existing cybersecurity model.

MORPHISEC
Moving Target Defense

www.morphisec.com
+1 617-209-2552