APP NOTE

MITIGATING THE IMPACT OF RANSOMWARE WITH THE IGEL UD POCKET

The tiny device that keeps business running, even while dealing with potentially dire and costly disruptions

Ransomware. The mere mention of that word is enough to send chills up the spine of any C-level executive. WannaCry, NotPetya, BadRabbit, and crippling ransomware attacks on the Colorado Department of Transportation (CDOT) and the City of Atlanta are just a few of the many now infamous attacks that have occurred worldwide. Today, businesses of all kinds face a greater possibility of having to deal with a cyber attacker demanding money, in some cases millions of dollars, just to simply continue to operate. Most organizations find themselves underprepared, ill equipped, or both, when someone or some group suddenly infects a part of the IT infrastructure and holds it "hostage" in exchange for money – oftentimes in staggering amounts.

Every organization takes their IT security seriously, but even those with the most robust, comprehensive multi-point security strategy and best practices can be infected. No organization is immune, since clever hackers with ill intent continue to find new ways to render key proprietary data compromised. Even with redundant data centers that include high availability, automatic backups, and powerful data protection safeguards including the use of cloud service providers, there still remains the possibility that a key C-level exec can "get the call" that some critical data or process is compromised and the only way to get it back is to pay an exorbitant amount of money. If this happens, entire businesses and their ongoing operations, services, sales, and logistics can come to a grinding halt while negotiations and possible "temporary workaround" tactics are considered.

But business does not have to come to a stop if malware attacks. People not directly impacted should continue to keep the business moving, despite an ongoing threat. This is where IGEL can help by offering a simple, secure, tiny little USB pluggable device called the UD Pocket. No larger than a thumbnail, the UD Pocket can turn any compatible x86-64 endpoint device into a secure company workspace. It gives people the ability to quickly start to work remotely from home or anywhere else, while the company retains full corporate management and control of those endpoint devices.

So if a malware attack occurs, people can retreat to their homes or work remotely away from the physical office environment on any variety of hardware vendor devices running a variety of operating systems (Windows 7, Windows 10, Mac OS, differing Linux distributions, or other proprietary OSs).

Basically "IGEL OS on a USB stick", when plugged into any compatible x86-64 endpoint device (company or personally owned), upon boot-up from USB the UD Pocket presents a secure virtual desktop environment, defined by the organization, that is virtually identical to what that person has been using when "at work" – Citrix, VMware, or Microsoft for example. The UD Pocket runs the IGEL OS operating system in its own separate, secure environment on that machine, with all company data stored in the data center or cloud, and not on the local endpoint. If the company data center is under siege due to an ongoing malware dilemma, the UD Pocket can store all data on a public cloud of the organization's choosing. When the user terminates his or her session and unplugs the UD Pocket, that user's device reverts back to its native operating system. This complete separation and protection of the user's personal/home environment and the company's work environment for that user, along with the ability to safely store data in an alternate cloud environment, is what makes the tiny UD Pocket such a powerful business continuity tool.

UD Pockets can be configured within minutes and managed by the organization's IGEL UMS management console. Upon activation, the UMS can "see" every UD Pocket user's IGEL OS instance and operation. In fact, the UMS can even remotely manage and shadow "off network" UD Pocket IGEL OS-powered user devices via the IGEL Cloud Gateway (ICG) feature. So for any company faced with the need to give hundreds or many thousands of users rapid access to the freedom of work-from-home or remote work, that can be done within a single day. And the company never loses the management and control that is so critical throughout the organization.

So when a malware attack occurs, the UD Pocket can enable any organization to continue to operate at full strength, without interruption, from end-to-end. Essentially, the UD Pocket does for end-user devices accessing virtual apps, desktops, and cloud workspaces what data center redundancy and cloud service providers do to offer those services without interruption, regardless of what may happen. If your goal is to build out a complete end-to-end business continuity strategy that can weather any severe disruption, even a ransomware attack, the UD Pocket should be viewed as a key, "must have" element.

Want to learn more about how the UD Pocket is a key enabler for malware mitigation and business continuity? READ THE CASE STUDY

IGEL
next-gen EDGE OS
for cloud workspaces