APP NOTE

SCHNELL DIE KONTROLLE BEWAHREN IM FALLE EINES CYBERANGRIFFS MIT DEM IGEL UD POCKET

Laut einer IDC-Studie zum Thema Ransomware aus dem Jahr 2021, gaben 37 % der Unternehmen weltweit an, im selben Jahr Opfer einer Ransomware-Attacke geworden zu sein. In den letzten Jahren haben die Schlagzeilen über Ransomware-Angriffe auf kritische Infrastrukturen, Regierungen und Unternehmen leider stark zugenommen, wobei Gesundheitsdienstleister ein Hauptziel sind. Die Frequenz und die Raffinesse von Angriffen wie Malware, oder Phishing und die Höhe der Lösegeldsummen sind beispiellos und es gibt keine Anzeichen für ein Abklingen. Cyberangriffe können wichtige Dienste und Prozesse zum Stillstand bringen, was zu finanziellen Verlusten, Lösegeldern in Millionenhöhe und dem potenziellen Verlust wichtiger oder sensibler Daten führen kann. Ein umfassender Disaster-Recovery-Plan ist entscheidend für die Gewährleistung der Geschäftskontinuität, nachdem Ihr Unternehmen beeinträchtigt wurde.

Das Ausmaß der Angriffe zeigt uns, dass selbst Unternehmen mit einer umfassenden, mehrschichtigen Sicherheitsstrategie betroffen sein können, was die beunruhigende Erkenntnis mit sich bringt, dass jedes Unternehmen einem Risiko ausgesetzt ist. Diejenigen Unternehmen, die Windows-"Fat Clients" auf ihren Endpoint-Geräten einsetzen, sind besonders gefährdet, da sie häufige und zeitaufwändige Patches und Updates benötigen, die ihr Risiko nur noch erhöhen. Dies und die globale Beschleunigung des hybriden Arbeitens haben die perfekte Basis für opportunistische Cyber-Kriminelle geschaffen, um eine Flut von Malware-Angriffen zu entfesseln.
Sehen Sie sich das IGEL OS-Sicherheitsvideo an

IM AUGE EINES CYBER-WIRBELSTURMS IST EINE SCHNELLE REAKTION ENTSCHEIDEND

IGEL OS ist das Managed Operating System für den sicheren Zugriff auf jeden digitalen Arbeitsbereich

IGE hilft IT-Administratoren, die Kontrolle über die betroffenen Geräte zurückzugewinnen. Sie ermöglichen ihren Mitarbeitern einen sicheren und verwalteten Zugriff auf Unternehmensanwendungen, -daten und -desktops von jedem Gerät und von jedem Ort aus. So wird die Produktivität inmitten eines Sicherheitsvorfalls wiederhergestellt, selbst von Endpoint-Geräten, die direkt von einem Cyberangriff betroffen sind.

Mithilfe des UD Pockets kann IGEL OS selbst von Malware infizierten Geräten gebootet werden. Da IGEL OS schreibgeschützt und manipulationssicher ist, sind die Firmware-Dateien verschlüsselt und befinden sich in einer separaten Partition, so dass sie für vorhandene Malware unzugänglich sind. IGEL OS verfügt über eine "Chain of Trust"-Sequenz kryptografischer Signaturüberprüfungen, die mit dem UEFI Secure Boot beginnt und sich bis zum VDI-Host oder der Cloud erstreckt. Dies wird bei jedem Startvorgang überprüft, um sicherzustellen, dass die IGEL-Firmware und -Software in der Startsequenz nicht manipuliert wurde.

ERHALTEN SIE DIE KONTROLLE MIT DEM IGEL UD POCKET

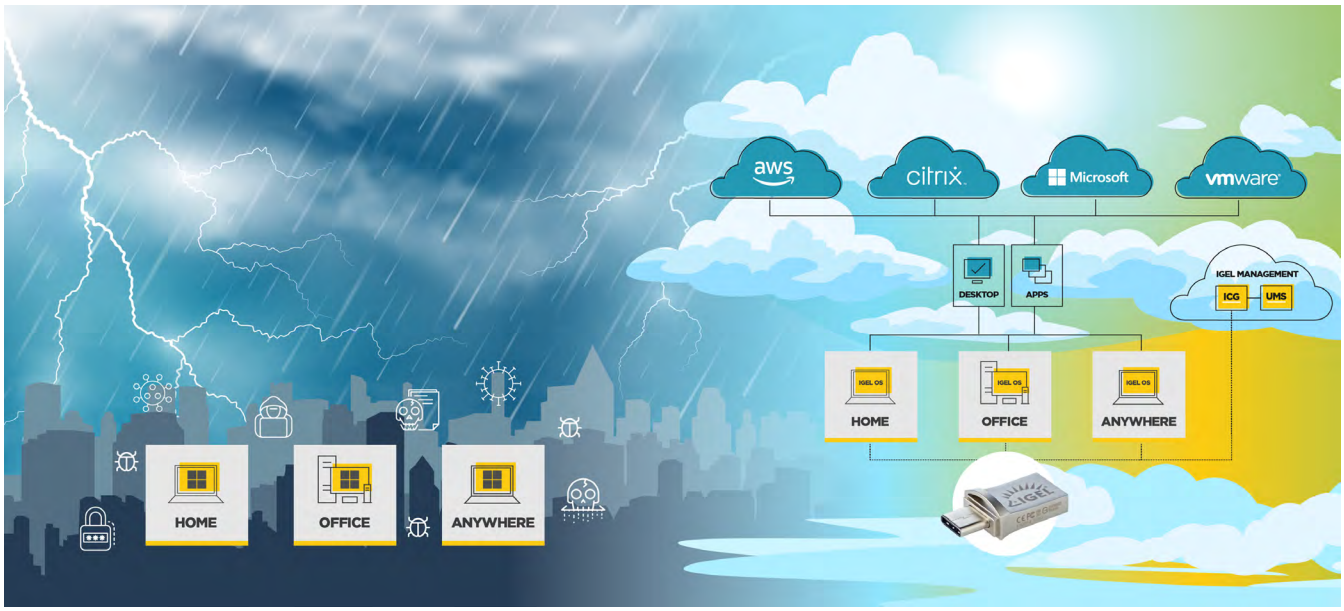
Verwandeln Sie jedes Gerät in einen sicheren Arbeitsbereich

Der IGEL UD Pocket, ein kleiner USB-Stick, ermöglicht es Mitarbeitern, das Gerät ihrer Wahl vorübergehend in einen sicheren, verwalteten Arbeitsbereich zu verwandeln. Stecken Sie den IGEL UD Pocket einfach in einen USB-A- oder USB-C-Port und booten Sie von USB zu IGEL OS, um auf die Citrix-, VMware-, Microsoft AVD- oder Cloud-Umgebung Ihres Unternehmens zuzugreifen. Der UD Pocket kann IGEL OS auf jedem x86-64-Gerät eines beliebigen Herstellers booten.
Zu den beliebtesten IGEL-Kunden gehören HP, LG, Lenovo und Dell.

Erfahren Sie, wie der IGEL UD Pocket einem Gesundheitsdienstleister half, nach einem Malware-Angriff die Kontrolle zurückzugewinnen.

Erhalten Sie die Kontrolle über Remote-Geräte und digitale Arbeitsbereiche, selbst über infizierte Endpoint Geräte

In der heutigen Welt des hybriden Arbeitens erfordern Disaster-Recovery-Pläne eine leistungsfähige Verwaltung von Remote-Endpunkten. Mit der IGEL Universal Management Suite (UMS) kann der IT-Administrator die IGEL OS-Geräte über eine einzige Konsole bereitstellen und steuern. Das IGEL Cloud Gateway (ICG) erweitert die Reichweite der Verwaltungskonsole, indem es eine sichere, verschlüsselte Verbindung zu jedem Remote-Benutzergerät herstellt, ohne VPNs.



Die Ruhe nach dem Sturm

IGEL OS ist ein sicheres, schreibgeschütztes Betriebssystem, das den Mitarbeitern eine Alternative zu dem infizierten Betriebssystem bietet, das sie bisher verwendet haben. Der UD Pocket führt das IGEL OS-Betriebssystem direkt vom USB-Gerät aus, so dass auf das lokale, verseuchte Betriebssystem, die Festplatte und deren Inhalte nicht zugegriffen wird. Diese vollständige Trennung von lokalem Betriebssystem und IGEL OS macht den UD Pocket zu einem leistungsstarken Tool zur Wiederherstellung der Produktivität inmitten eines Sicherheitsvorfalls. Sobald die Störung behoben ist, kann der UD Pocket ausgesteckt werden, und das Gerät kehrt zum ursprünglichen Betriebssystem zurück.

IHR SICHERER HAFEN IN TURBULENTEN ZEITEN

Fachkundige Unterstutzung zur Beschleunigung der Implementierung Ihrer IGEL Disaster Recovery-Lösung

Premier Technical Relationship Manager (TRM)
Ein IT-Experte, der Ihr Unternehmen versteht und Sie proaktiv dabei unterstützt, IGEL UD Pocket, UMS und ICG in Ihrer Umgebung zu nutzen, um schnell die Kontrolle über Ihre Endpoints wiederzuerlangen.

Die IGEL Academy bietet zielgerichtete eLearning-Programme zum Selbststudium, um IT-Administratoren das Know-how zu vermitteln, das sie benötigen, um alle Funktionen des IGEL-Betriebssystems und der Managementkonsole zu nutzen.

KONTAKTIEREN SIE IGEL DISASTER RECOVERY FÜR WEITERE INFORMATIONEN

DEMO ANFORDERN
IGEL.DE/DISASTER-RECOVERY