Unique Black Boxes Offers Big Business Protection on a Small Business Budget.

Unique Black Boxes creates a Patent Pending solution designed for small business owners to benefit from Enterprise Network Power at small business pricing.

HAMILTON, ONTARIO, CANADA, November 14, 2022 /EINPresswire.com/ -- If it were measured as a country, cybercrime would be the world's third-largest economy after the U.S. and China. Cybercrime cost businesses in excess of $6 trillion USD globally in 2021, and is projected to cost $10.5 trillion annually By 2025.

> Depending on how the customer wants it configured, it can act as a server, firewall, NAS unit, or a combination of these. It can also operate in a Linux or Microsoft environment."
>
> *Keith Green, President, UBB*

Small businesses are particularly vulnerable to cybercrime. Why small businesses? Many smaller companies don't have a strategy in place to protect themselves and their essential data. And criminals know this. Large companies may be the ones we read about in the news, but they are often harder targets because they invest in IT and data protection.

So, how do companies protect themselves, and their data, against cybercrime, ransomware and data theft?

A Canadian firm believes they have created a solution. Unique Black Boxes has developed an effective and affordable option for small and medium sized businesses. Critical data is safer when kept backed up in a secure on-site environment. Data kept online and "in the cloud" is great. Until it isn't. Hackers can access your online data through websites, servers, and even cloud backup solutions. Anything that's connected to the internet. Unique Black Boxes can provide a protected computer environment that resides in the business office or an off-site location. According to co-founder Keith Green, "Depending on how the customer wants it configured, it can act as a server, firewall, NAS unit, or a combination of these. It can also operate in a Linux or Microsoft environment. We call it 'The Swiss Army Knife of computers'."

Think of UBB as a safety deposit box for your data. If cybercriminals access your data and attempt to hold it for ransom, UBB owners have peace of mind knowing that they don't need to negotiate. UBB ensures that everything is backed up and protected. It depends on the

application and configuration as requested by the client. A NAS won't protect, but it will retain a clean copy of everything. A firewall can protect but if a server application with correct permissions is configured, that is the best defence in conjunction with an Acronis AV option.)

One Solution. Multiple Benefits.

File Recovery
The surest way to survive a ransomware attack is to maintain a secure and up-to-date backup of all essential files. Beyond just backing up the files, incorporating dedicated software on the UBB can actively work to detect and help prevent ransomware attacks.

What Is Ransomware, and How Do You Get It?
The idea behind ransomware is simple. A potential attacker finds a way to take something of yours and demands payment for its return. The most common type, known as encrypting ransomware, takes away access to your important documents by replacing them with encrypted copies (gobbledygook). Pay the ransom and you get the key to decrypt those documents (you hope). There is another type of ransomware that denies all use of your computer or mobile device. The most harmful and sneaky example is malware that

UBB (Unique Black Boxes), creator of the BCS4000

Unique Black Boxes BCS4000 – Enterprise Network power at small business pricing

encrypts your entire hard drive, rendering the computer unusable. Fortunately, this last type is currently uncommon. Not to scare people even more, but there is a new ransomware attack out now called wipeware. If you don't pay, it wipes your drives and overheats your electronics, effectively destroying it.

Several years ago, you could choose from a dozen or so standalone ransomware protection tools from consumer security companies, and many of those tools were free. Most of those have since vanished, for one reason or another.

So what's at stake? What have you really got to lose? Cybercrime costs include damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm. Any one of these occurrences can cause losses in the thousands.

The BCS4000 starts at $2200 CDN and increases in price depending on configuration and storage requirements of the customer. At any level, the BCS4000 is priced to make enterprise level protection accessible to small business owners.

How does the Unique Black Boxes Solution Work?
The BCS4000 is a versatile solution, and depends on the application it was purchased for and functionality requested by the client. In the event of a system or hardware failure, the BCS4000 starts up and runs in a virtual environment, saving you thousands in downtime.

About the BCS4000
The units are designed and built in Canada by UBB (Unique Black Boxes). The design is Patent Pending. The product provides real-time data protection and creates a backup of your entire system. For IT professionals, the BCS4000 can better protect your customers and add tremendous value to your service. Contact UBB for a complimentary demo. IT pros can also become a UBB Certified Reseller.

Keith Green
UBB
+1 866-928-3265
keith@ubbinc.ca

This press release can be viewed online at: https://www.einpresswire.com/article/598159489