NITAAC (U.S. Gov.) Interview with Ed Brinskele, CEO of Vir2us – July 2015

NITAAC is the designated federal Executive Agent authorized by the Office of Management and Budget (OMB) to administer three Government-Wide Acquisition Contracts (GWACs) for information technology (IT).

Why do you think so many organizations are having such difficulty achieving genuine cyber security?

Information technology professionals are compelled to rely on vendors who provide what many so-called experts consider to be best-practices for cyber security. The difficulty is that there has been a significant failure on the part of solutions providers to recognize that a *keeping-the- bad-guys-out* approach reveals a failure to correctly identify the problem. Once the checkpoints in these solutions are bypassed, they provide virtually no security. This is known as an outside-in and top-down approach and is a fundamentally flawed strategy. As a result, these solutions only address the symptoms of a much more fundamental design problem.

What is that fundamental design problem?

The fact is, we have pushed to the limits a more than thirty-year-old computing architecture designed by engineers who never envisioned the Internet or the security challenges that such a globally connected computing architecture would produce. The unpredictable and exploding demand for greater computing capability and applications quickly overran these architectures and simplistic security solutions such as antivirus and other checkpoint and list-based products.

If nearly all solutions are attempting to deal with only symptoms and not the real problem, then what is the approach that can get us to genuine secure computing?

Experts, including the National Institute of Standards and Technology (NIST), NSA, DHS, DARPA and DOD agree that security must be built into computers and applications and not just layered on top of the OS. For this reason, NIST has adopted the specifications for Vir2us' VMunity platform as part of their recommendations for cybersecurity in critical infrastructure projects like Smart Grid.

What makes this approach different from antivirus, firewalls and other so-called advanced threat cyber security solutions?

Antivirus and firewalls are list-based solutions and can only deal with known threats. In today's world of morphing viruses and malware, these solutions are less than 27% effective. Symantec recently said that their average time to identify threats and update lists is more than nine months. In a challenge that is moving at the speed of light this approach is problematic.

Vir2us engineers were solving incredibly complex computing problems for some of the most tech savvy companies in Silicon Valley and the San Francisco Bay Area for more than a decade. They recognized that the problems their customers were encountering on a daily basis were the result of basic computing processes that were simply not secure. Over more than a decade, they developed and patented new computing processes and concepts that would make computers inherently secure and make cyber threats irrelevant.

So many other solutions are in the cloud or in proprietary computer hardware like firewalls. Why secure the network endpoints or desktop computers?

Virtually every hack you have read about in the past decade began as a network endpoint exploit. Endpoints have many vectors for exploits and by making the endpoints secure you eliminate the ability of an exploit to persist beyond the session, or to propagate across networks and to other computers. Because VMunity makes it impossible for exploits to propagate or persist, it eliminates the fundamental ability that exploits use to cause damage and steal digital assets and information. In short,

they are isolated and stopped before they can even get started, and even before they are ever identified as threats.

Exactly how does the Vir2us VMunity Platform secure network endpoints?

The Vir2us controller is a lightweight client that resides within the kernel, below the OS, and attests the computers bios on boot up to eliminate low-level exploits and corruption. This sealed controller serves up virtual isolated computer environments in containers from pristine application templates, which are disposed of after each use and governed by an enterprise-wide security profile. All applications, files and processes are isolated and controlled by a sophisticated service hierarchy and class matrix that determines at the most granular level what can be done with that file and application.

How do these virtual isolated containers ensure secure computing and thwart hackers?

VMunity isolates files and applications being processed from the actual computer system. Either the hacker's exploit will simply be unable to run or, if it is allowed to run, it will not be able to access any computer resources outside its virtual isolated computing environment. When the session process is completed, Vir2us disposes of that individual environment which will never be reused. Disposing of the virtual computing environment destroys any infection that might have occurred through browsing, opening an infected email or any other vector. This inherently secure process makes it impossible for viruses and other malicious software to propagate across a network of computers or to persist on the computer where the exploit gained entry.

This seems too good to be true. Where did these concepts come from and how do we know they will withstand the test of time?

While the VMunity Platform is novel, innovative and unique in its approach to secure computing, the underlying principles that it employs have withstood the test of time. As an early pioneer of the digital telecommunications industry, I worked for over a decade with one of the largest government contractors and network telecommunications providers in the U.S. During that time, I personally architected and deployed over one hundred national and international digital telecommunications networks for the agencies including the FAA, U.S. Department of Energy and many power utilities as well as international carriers and Fortune 100 firms. These networks rarely experienced any security issues as they employed the fundamental security principals embodied in the VMunity Platform.

So many large organizations and critical infrastructure firms have legacy computer systems and OS software that are not compatible with the latest cyber security solutions. How can the VMunity Platform help?

I was invited by NIST back in 2010 to sit on the R&D board of the interoperability panel that created the security specifications for Smart Grid (*NISTIR 7628 Guidelines for Smart Grid Cyber Security v1.0 – July 2010).* As part of that project, we reviewed virtually every configuration that is used for industrial controls in the nation's power grid. This informed us as to what would be required to rapidly secure this national network in the face of legacy computer controls dating back more twenty years. Part of NIST's decision to include the specifications for VMunity in its ultimate recommendations for securing the power grid had to do with VMunity's lightweight client (Zero-CPU) and built-in secure processes, which would enable its use in computers going back nearly twenty years.

Many organizations have custom software programs and bespoke software applications that cyber security solution providers simply do not support. How does VMunity address this?

When we first spoke with the NYSE about securing all Bloomberg trading terminals from a national network of securities dealers and brokers they informed us "that more than 50% of applications used on trading exchanges were bespoke and custom software applications". They also told us that VMunity was

the only solution they had seen that addressed securing custom applications, an absolute necessity for financial services and critical infrastructure applications.

We are hearing that foreign language malware can't even be detected by the most popular cyber security solutions market leaders. Can the VMunity Platform identify this type of exploit?

It is estimated that foreign language malware represents more than 50% of the exploits being delivered today. This little-known fact is quickly bringing to light the need for the different and more comprehensive approach to secure computing that is exemplified in the VMunity Platform. VMunity uses inherently secure processes that eliminate the need to identify threats making the language of these exploits irrelevant.

Have any government agencies looked at this technology and weighed in what the impact of this technology might be?

Vir2us VMunity technology was first recognized as a breakthrough in cyber security in 2008 by Richard Clarke, former head of national security for several Presidential administrations. Mike Jacobs, former NSA Deputy Director and NSA's most senior technologists dubbed VMunity as "game changing". Even the White House in 2010 recognized Vir2us VMunity, stating that it could end the game with hackers for the Federal Government.

Many people believe that no system can be secured and that there is no silver bullet to the problem of cyber security. What would you say to these people?

I think it is hard to be accurate about the finite capabilities of groups of engineers when trying to solve complex problems. I think the most honest thing each of us can say when faced with a new and complex problem is that we simply do not know what the answer is, but there may be someone else who does. Putting aside the silver bullet analogy for a moment, there are quite a few case studies that show that genuine security is achievable when fundamental principles of security are followed. One example of this is the secure radio communication technology that the U.S. employed in WWII known as Spread-Spectrum, and which the enemy was never able to break.

We're hearing more about the need for remediation as part of the cyber security puzzle. What is remediation and why is it so important?

Remediation is the ability to provide 100% assurance that computing is uncompromised and the ability to turn computers back to a day-one pristine state automatically when and if they become compromised. This is important because cyber security solutions like antivirus, firewalls, cloud-based and list-based solutions provide no protection whatsoever for previously compromised computing environments, and they simply don't remediate computers. Some major solutions firms are offering their clients manual remediation but this is not a real-time solution and can take months or even years. Firms like Sony, Saudi Aramco, NYSE, University of Michigan and others are still attempting to remediate computers from hacks that happened months or years ago. Even if these firms ultimately succeed in manually remediating their systems they still have not solved the fundamental problem and they could easily be infected again.

So if computers are already compromised, and firms are unaware of it because the threats have not yet been identified, all their security measures are helpless to stop or remove the threat. Is that correct?

That is the reality, and one of the key reasons firms are struggling to implement genuine cyber security. The final revelation is that, even if firms take the time to remediate computers manually, once they are reconnected to the network they are in danger of becoming compromised again very quickly if they have not secured their endpoints.

Precisely how does the VMunity Platform eliminate this seemingly insurmountable problem for mangers and their firms?

The VMunity Platform is the only cyber security platform solution in the market today that has built-in, real-time remediation that returns computers to a day-one pristine state from the cloud or secure server automatically. This process simultaneously implements the VMunity Platform ensuring these systems can't be compromised again.