Raytheon and Virsec Partner to **Guard the Homeland**

A Partnership to Change the Paradigm

With the Homeland under constant threat of cyberattacks, Raytheon is seeing the value of technology innovations that can change the paradigm, from one of reactive protection to proactive protection, where it counts most, the high value and sought after workload.

The malware that blacked out parts of Kiev, Ukraine was a ticking time bomb.

It slipped inside the networks of electrical substations through a flaw in an obscure device. It built back doors to other parts of those networks and waited. Then, at a time chosen by its programmers and written into its code, it destroyed. It commandeered circuit breakers, shut down relays and hobbled the control software.

The malware, known as both CrashOverride and Industroyer, showed how hackers not only understand the arcane networks of the energy industry, but are using that knowledge to carry out devastating cyber offensives. It also showed how urgently the keepers of critical infrastructure need to shore up their defenses.

To speed that along, Raytheon is working with innovative companies like Silicon Valley cybersecurity firm Virsec to license network-saving technology to government agencies and large enterprises including healthcare companies, financial institutions and utility providers. That partnership,answers a call in the U.S.National Defense Strategy for the defense industry to deliver new technologies faster. For Virsec, it also accelerates the long, difficult acquisition process smaller companies often encounter when breaking into the federal and international markets.

"Commercial tools from companies like Virsec can help bridge the gap for our global government and commercial customers and provide effective protection against the growing cyber threat."

John D. Simone, Vice President of Cybersecurity and Special Missions, Raytheon

"Raytheon is clearly in favor of changing the paradigm to put our Homeland in a proactive posture versus one that is reactionary. I think we emphasize TIME element that we close, thus shortening the window for nation states to disrupt critical mission workloads," said Ray Demeo, co-founder and chief operating officer of Virsec. "Without partners like Raytheon, the U.S. government would not be able to access essential and immediately needed technology. And this is important to all of us and its allies as citizens, the ability to change our defense posture. It really is a day-to-day battle."

At the heart of the Raytheon-Virsec agreement is a defense against "memory-based" cyberattacks, or those that exploit weaknesses in legitimate applications, rather than installing malware. Well- known examples include the WannaCry and NotPetya ransomware attacks, which exploited a PC feature called Server Message Block that allows computers on a network to access shared resources such as printers.

Virsec calls its defense against memory-based attacks "Trusted Execution," and it basically works like this: It learns what applications should and shouldn't do, and when it sees an application executing an abnormal script, for example, it flags the activity and sends an alert that enables security to shut down the rogue function immediately.

The technology does fill a critical need, said John DeSimone, vice president of cybersecurity and special missions at Raytheon. "Commercial tools from companies like Virsec can help bridge the gap for our global government and commercial customers and provide effective protection against the growing cyber threat," he said.

"Raytheon is clearly adept at changing that paradigm and bringing newer technologies and solution sets more quickly to its customer base."

Dave Furneaux, CEO, Virsec

Server and Application Workload Protection

The cyber battleground today is on the server. 80% of breaches happen on the server, and the weapon of choice is the Remote Code Execution (RCE) attack. When attackers bypass perimeter and detect-and-respond security tools, Virsec prevents exploitation of software vulnerabilities in unpatched, out-of-support and modern server workloads.

Eliminate Zero-Day Threats

Protect workloads from zero-days and other unknown attacks.

Take Adversary Dwell Time to Zero

Put an end to long-term data damage and loss.

Embrace Zero Noise

Give your analysts low false positives, high accuracy.

Discover

Scan workload for all executable files

Analyze

Verify executable's reputation & dependencies

Map

Automated allow-listing & executable memory mapping

Enforce

Stop malicious code execution

(file, file-less, memory injection, buffer error & web attacks)

Securing the World's Most Critical Applications

Virsec is deployed globally protecting mission-critical applications and infrastructure in industries including financial services, healthcare, government, defense, power, oil & gas, transportation, telco, technology, and more.

Server & Application Workload Protection

Application-Aware Mapping Technology

No Signatures, No Tuning, No Noise

Zero Dwell Time

Recognition

Cyber Catalyst · CRN · Cyber Defense Magazine Global Awards 2019 Winner · Gartner · Cyber Security Excellence Awards Winner 2020 · MITRE · Info Security Products Guide 2020 Global Excellence Gold · Ovum

Enterprise

InfoArmor · Bottomline · Raytheon Technologies · GE Healthcare · Bloomenergy · BROADCOM · FREEDOMPAY · TATA

Commercial / SMB

GroundProbe · GreenLight Biosciences · Karnataka Bank Ltd. · Boston Red Sox · LUMICELL · Independence Contract Drilling · Godrej · QDB · inspirage · Vivriti Capital

Public Sector

U.S. Department of Homeland Security · Alabama A&M University · U.S. Department of Energy · Salvarita Arizona · Gwinnett · भारत सरकार Government of India · SVCW · United Arab Emirates Government of Fujairah E-Government

About Virsec

Virsec offers continuous protection for application workloads, stopping known and unknown attacks—including zero days. With our patented technology, we take a defense-in-depth approach with a Zero-Trust model that allows only authorized code and executables to run and nothing else. Battle-tested against 200+ of the top government red-teamers and trusted by several Fortune100 companies, Virsec has repeatedly proven a protection-first model works. Virsec is headquartered in San Jose, California, with offices worldwide. For more information, please visit **virsec.com**.