DELL EMC

THE NEED TO THINK DIFFERENTLY ABOUT CYBERSECURITY

September 2017

When evaluating the state of cybersecurity in the federal space, it's easy to get distracted. With an ever-increasing threat landscape, the cybersecurity market is red hot and too many vendors are making too much noise about their latest service, update or release. There is too much focus on product – from incumbent government partners and startups alike – and not enough focus on the underlying challenge that must be addressed: securing data.

Protecting data is what cybersecurity is all about, and that's where the focus always should be. The technology enabling cybersecurity shouldn't get in the way of the mission of protecting sensitive government data. For multiple reasons – workforce mobility, cloud data storage and BYOD, for example – that mission is more difficult today than ever before.

Earlier this year Dimensional Research conducted a study looking at how business professionals handle confidential information. The study included workers in federal IT, and many of the findings were sobering:

- **41 percent** of federal respondents accessed work documents via their personal devices.
- **37 percent** use public Wi-Fi to access government files.
- **76 percent** said they are required to attend training on handling sensitive data, yet only 40 percent are confident they know how to do so and still get their job done.
- **24 percent** feel current IT security processes slow down their work.

When conceptualizing data protection for the federal government, it's useful to differentiate threats from two distinct sources – external and internal.

External Threats

External threats are the ones that you're most likely to read about in news coverage. Activist hackers, criminal syndicates and nation-state actors have all been "weaponizing" their cyberattack capabilities. And unfortunately, the standard front line of defense doesn't provide much protection.

That front line currently comprises of reactive anti-virus and anti-malware solutions, which are estimated to fail about 50 percent of the time. These solutions are signature-based, and need to recognize an existing attack signature before providing protection. Obviously, this is of no help in the case of zero-day attacks and constantly adapting advanced persistent threats. The bad guys have

simply become too good, and this reactive model of data protection doesn't work anymore.

What's needed is a proactive advanced threat protection (ATP) model that leverages the power of machine learning for a much higher level of protection. ATP with machine learning can increase the 50 percent protection performance to 98-99 percent, stopping the vast majority of malware attacks before they happen and allowing security teams to focus on the truly sophisticated attacks. This can be accomplished because unlike anti-virus and anti-malware solutions that rely on an existing signature, ATP looks at the underlying code before it is allowed to execute.

When conceptualizing data protection for the federal government, it's useful to differentiate threats from two distinct sources – external and internal.

"I like to say that anti-virus/malware can be fooled by a bad guy growing a beard, while ATP is like inspecting a person's DNA," says Brett Hansen, VP, Client Software and GM, Dell Data Security. "Usually, the bad guys compromise an endpoint, which they use to penetrate the network. By locking down the endpoints, we are shutting and locking the enterprise's front door."

ATP algorithms are based on huge samples of code, and only need to be updated every few months, as opposed to the almost constant signature updates required by current anti-virus and anti-malware solutions. And since CPU-killing, system-wide scans are no longer required, there is no performance degradation. The intelligence is built into the network endpoint, and for the first time, air-gap networks can leverage ATP. For those networks, the updates are done via a physical medium such as a USB drive rather than a cloud connection.

Moving to an ATP solution also protects against a BIOS attack, a relatively rare but extremely dangerous threat vector. A BIOS attack hijacks a computer at the root level, and malware then gains complete control, and complete trust, of the rest of the network. To prevent this from occurring, a "snapshot" of the original computer BIOS can be taken at time of manufacture and stored remotely via a secure cloud connection for comparison purposes.

Internal Threats

The quieter threats that typically stay out of the headlines are insider threats. These threats can be malicious, but happen more so from simple negligent behavior. A laptop left on the subway, a file emailed to someone trusted which is then mishandled, use of public cloud, etc. On the insider front, a data lockdown mentality has been fighting a losing battle against macro trends such as workforce transformation and the way people must collaborate today to propel innovation and raise productivity.

Federal workers are increasingly mobile, use multiple devices and need to collaborate with colleagues and vendors within and outside of the protected network. Data needs to flow to become insightful and deliver results, which obviously presents security challenges. Trying to build a wall and prevent any data from leaking out is futile and hurts productivity. There needs to be a balance between the end-user friction created and the level of endpoint security attained.

Federal workers are increasingly mobile, use multiple devices and need to collaborate with colleagues and vendors within and outside of the protected network. Data needs to flow to become insightful and deliver results, which obviously presents security challenges.

Just as with the external threat, a different approach to data protection is required. This new approach tears down the ineffectual data wall, and extends data protection to each individual document. An encrypted shell is put around each and every document, and this shell travels with the document everywhere. Each document requires a separate key to access it, providing granular control of who can access that information. By shifting perspective from an indefensible perimeter to each and every document in motion, security is enhanced without hindering workforce productivity.

Each and every document is not only encrypted but also carries policy. Agencies can now protect, control and monitor the status of all documents, from one integrated reporting solution that includes mobile devices. So with this approach detailed reporting is made

possible – status of the document, geolocation and history of those who have accessed it. This usage data can become an entirely new source of analytics, providing rich insight into internal consumption patterns and powering predictive models that combat the intentional insider threat.

Protecting Data at Rest – The Quantum Physics Threat (Solution: ESSE with dual encryption—hence, may want to move up under the first section instead)

The document-specific encryption discussed above uses 256-bit encryption, the current industry standard. Today it would take a powerful computer years to break 256-bit encryption. However, there have been rapid advances in the area of quantum computing that could put 256-bit level encryption in danger within the next year.

Sometimes it's easier to stay with the status quo, even when it's been proven ineffective. Agencies need to cut through the noise and embrace a different understanding of data protection.

Quantum computing is not restricted to simple 1s and 0s, as is traditional computing. Simply explained, an attacker leveraging quantum computing could attempt multiple combinations of numbers simultaneously, greatly reducing the time needed to break 256-bit encryption. Experts estimate quantum computing could reduce the time from years to as little as four months.

"The danger posed to encryption by quantum computing affects many industries, not just government," says Hansen. "Financial institutions would be especially vulnerable. To describe the danger, I use the analogy of a better blowtorch being developed, one that can cut through the strongest steel safe."

To prepare for this danger, Dell has developed a system of dual encryption. Both the system itself and the individual files are encrypted, necessitating breaking both 256-bit encryptions. This pushes out the time dramatically, into decades. But development must continue for this type of solution to become easier for broader implementation.

Recommendations

All of the new approaches to data protection discussed here have been proven in the private sector. Despite this, government agencies have been slow to evolve beyond signature-based anti-virus protection. Sometimes it's easier to stay with the status quo, even when it's been proven ineffective. Agencies need to cut through the noise and embrace a different understanding of data protection.

To make this evolution, the right partner is critical. Government should look for a cybersecurity partner with a proven history of supporting the public sector. Next, agencies should consider the product offerings of potential vendors. Many prominent names in this space have significant vested interests in signature-based solutions, and might not be inclined to help agencies make the transition to more powerful ATP/machine learning solutions.

Cybersecurity is a fast-moving field, and the perfect government partner has the resources and the vision to look ahead and invest in the future. It owns its intellectual property, and combines hardware and software expertise. This foundational partner might bring a number of best-of-breed technologies together, but provides a holistic structure and gives the government customer one phone number to call. Case in point, best-in-class brands Dell Technologies, through its acquisition of EMC, has now pulled in best-in-class endpoint solutions from RSA, Mozy and Airwatch. Examples would be how RSA is now part of Dell Technologies, and Dell's partnership with Cylance.

It's past time government stopped letting the bad guys in through the front door. Understanding that cybersecurity at its core is all about data protection is an important first step. There is no one silver bullet for protecting data, but the remarkable advances in artificial intelligence and machine learning have fundamentally changed cybersecurity. The bad guys won't stop innovating, and it's time for the government to start.

Dell EMC, a part of Dell Inc., helps our government customers modernize, automate and transform their data center using industry-leading converged infrastructure, servers, storage and data protection technologies. This provides a trusted foundation for federal agencies to transform IT, through the creation of a hybrid cloud, and transform their organization through the creation of cloud-native applications and big data solutions. Dell EMC services its customers – including 98 percent of the Fortune 500 – with the industry's broadest, most innovative infrastructure portfolio from edge to core to cloud.

Learn more at **www.dell.com/federal**