Symantec World headquarters

The DoD's embrace of cloud raises security concerns

Cloud-based technologies and the ability to access data on the move has enabled a huge leap forwards in capabilities amongst government and military organizations the world over. However, this use of cloud technology has raised security concerns which desperately need to be addressed, as outlined by Chris Townsend, Vice President Sales and Operations, Federal at Symantec.

For years, officials at the Department of Defense (DoD) have talked about the importance of a defense-in-depth approach to cybersecurity. Now they need to take the approach to its logical conclusion.

With more than 2.7 million employees, including active duty personnel working in potentially hostile environments, the department's need to share information quickly, securely, and without disruption, is almost endless.

And as difficult as it may be to believe, this network only continues to grow. Along with the geographical footprint of the department, the threat surface keeps getting bigger. Cloud computing and mobility have made it so that every employee can access data no matter where they are, creating a seemingly never-ending enterprise comprised of millions of endpoints spread across the globe.

With so much sensitive data spread across such a wide enterprise, even a traditional defense-in-depth approach could leave data vulnerable. A new approach is needed.

The need for data-level security

In the past, the DoD used a traditional perimeter defense approach. With desktop computers bound to a single network, the goal was to simply protect enemy intruders from entering the network in the first place. If they could not gain access to the network, then it could be assumed that the data would be safe. The department has pushed in recent years for a more defense-in-depth approach, a process that it has started taking steps to complete.

While this perimeter-based security architecture had its flaws, it became the standard in both DoD and enterprises around the world. That all, though, has changed rapidly in the last decade. The federal government has pushed cloud computing technologies, and agencies, especially in the DoD, have used it as a strategic tool.

The cloud enables employees to work anywhere at any time, improving efficiency and transforming how employees work. That could be a systems analyst working remotely at a Starbucks branch, or a squadron leader in Afghanistan. For the Department of Defense now to keep data secure, it must employ data-level security.

What exactly does that mean? In short, it is technologies that provide security that goes wherever the data goes. If the data is accessed on a mobile device while an employee waits in line to get a sandwich, it is as secure as if they accessed it on a private station inside the Pentagon.

Protecting against data loss

With people able to access data anywhere they work, there needs to be additional security measures in place. Data Loss Prevention (DLP) technologies have become a popular cloud-security method. DLP secures data by wrapping automatic protection around it. When data leaves an organization and is shared with other devices, DLP technologies will identify any sensitive data to make sure it has the required protections.

This allows organizations to control who can use data, even from unmanaged locations or devices; define what level of access a user has using persistent encryption and digital rights;

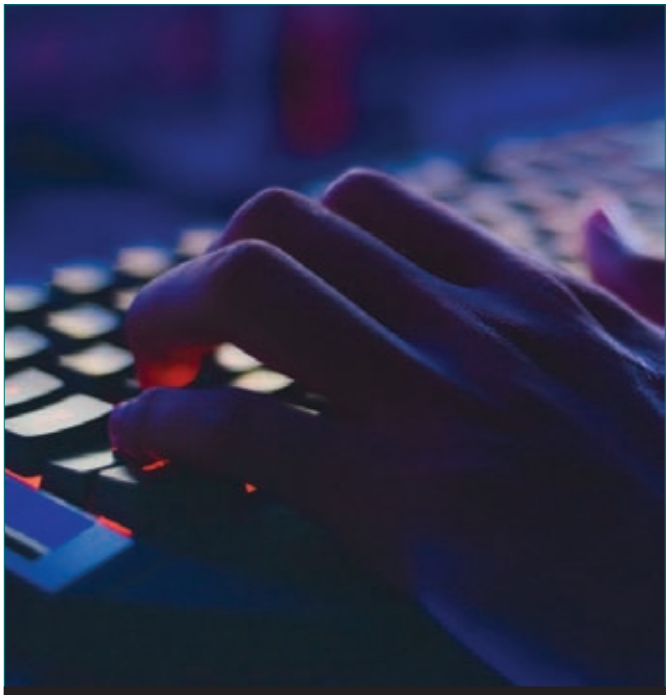

Photo by Soumil Kumar from Pexels

monitor user access to sensitive data to identify risky behaviour; and, remove access to users.

DLP ensures that any data that leaves an enterprise has security that goes along with it. DLP can discover, monitor and protect sensitive data no matter where it is. It gives the owner complete visibility and control across the broadest range of data loss channels, including cloud applications, endpoints, data repositories, emails and web communications.

DLP can ensure that sensitive data remains secure, no matter how it is accessed. DLP can allow defense officials to still allow employees to access data without the fear of it being put at risk.

The need for security in JEDI

The military continues to use cloud computing as a strategic benefit.

In fact, the Defense Department plans to expand its cloud computing use with its 10-year Joint Enterprise Defense Infrastructure contract. Better known as JEDI, this contract will see a private company create a cloud infrastructure for the DoD. It is seen as a major initiative that shows the department's commitment to a cloud-based future.

While security certainly will be baked into the JEDI offering, the DoD will want to add additional security to protect its data. A data-level security approach ensures that no matter where data is accessed, it has a certain level of security. This ensures that cloud is used in a responsible way, such as providing data to service members wherever they are, using data in the field, and staying connected to data analysts wherever they work in the world, and minimizes the possibility of a data breach that could expose sensitive and important data.

A changing paradigm

The DoD's technology will continue to evolve - and so must the way employees view the cloud and cybersecurity. The DoD can no longer stick to a perimeter defense model. The department must adapt to the latest cybersecurity practices and data-level security is key to this adaptation.

The JEDI contract and the department's commitment to cloud computing are encouraging. These projects will expand the department's use of cloud and only add new capabilities that will help employees with the department's largest mission - securing the nation. **GMC**

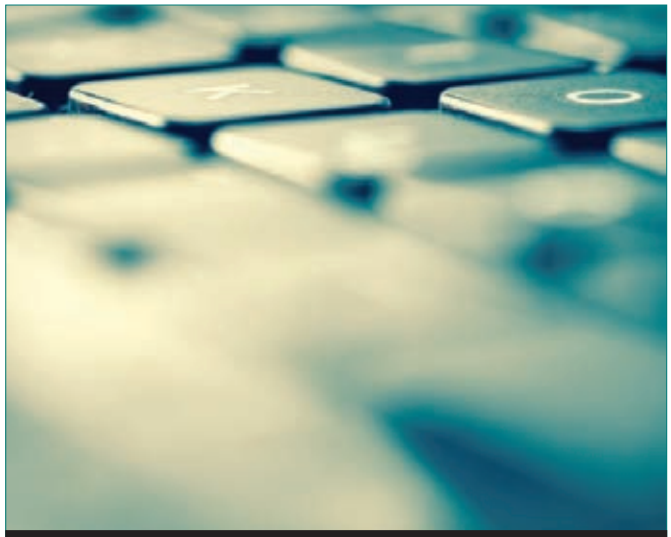

Photo courtesy of Pexels