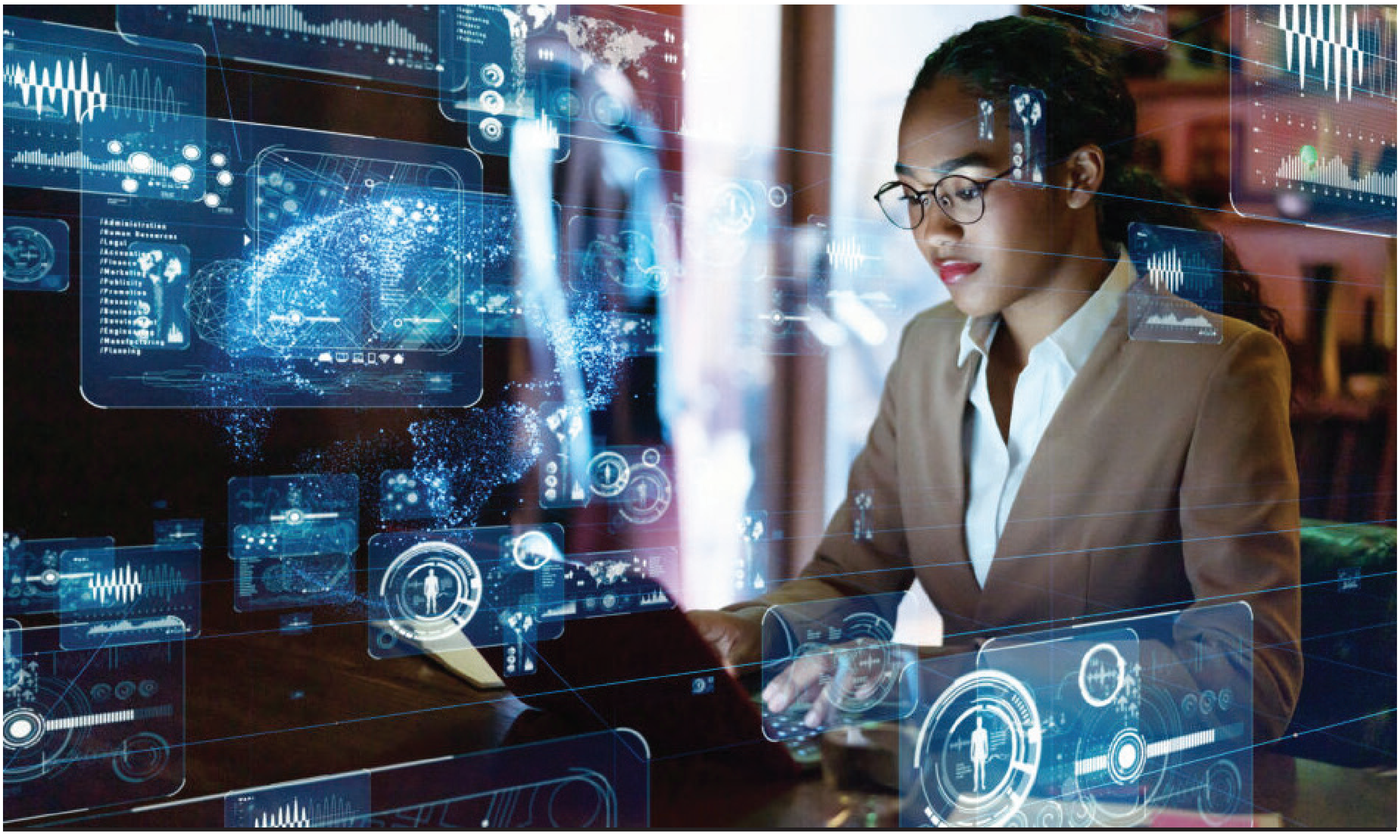
Gov Data Download

Higher Education IT Departments Working to Unlock the Entire Potential of their Data Management



By Bob Burwell
CTO, State, Local Government & Education

When the COVID-19 pandemic reached American higher education institutions, universities and colleges across the nation scrambled to adopt modernized technologies that would enable students, faculty, and staff to transition to remote learning, teaching, and work. But the digitally transformed environments that they migrated to were, in large part, intended to keep universities up and running and allow students to continue their secondary education pursuits in a healthy and safe way. Many institutions were simply trying to find a way forward during this unprecedented black swan event. So, at the time, they were not necessarily exploring the full potential of their new IT and data management solutions, and what they could offer to students and faculty.

Now that the dust from the pandemic has settled, and institutions have a certain comfort level with their modernized networks, university IT departments are beginning to look into all of the benefits of the technologies and solutions they quickly adopted in 2020. They have realized there is tremendous potential to do more with them and are looking to get the most out of those investments. This has resulted in higher ed IT professionals and decision-makers analyzing how they're utilizing these technologies, if they are maximizing the potential of their IT modernization efforts, and how they are protecting their data centers – and the massive influx of new data their systems have been gathering since 2020 – from being exploited by malicious cyber actors.

This was a theme that I heard during all of my interactions at last year's EDUCAUSE Conference, and something that I certainly anticipate will be a priority for university IT departments through the rest of 2023.

How universities are unlocking their entire IT potential

Bob Burwell
CTO, State, Local Government & Education

Whether it's trying to figure out where VMware is heading, implementing containers, deploying Kubernetes to automate, scale, and manage their applications, or simply trying to figure how they can tie the hybrid cloud into their daily operations, colleges and universities are focused on modernizing their operations and delivering the most out of their entire IT infrastructure.

But they are not just doing this for modernization's sake. Higher ed institutions have realized that their pre-pandemic legacy systems are creating more IT challenges than solutions for their students and faculty. Legacy applications, systems, and databases are no longer able to securely hold all the data digitally transformed universities are now storing.

Because of this, institutions are asking how they can use their data center – and cloud services from hyperscalers – to holistically maximize efficiency while simultaneously reducing costs. University IT departments are discovering that there is a plethora of solutions that have either been underused – or not used at all – since being adopted at the start of the pandemic. Higher ed IT professionals should be encouraged to explore the baked-in potential of their current data centers, as it can possibly support their data governance and management initiatives with more streamlined and optimized solutions, while also saving their budgets.

Databases are juicy ransomware targets

Managing and storing the mountains of data that they have been aggregating since the start of the pandemic is just the beginning of their problems, however. The greatest looming threat hanging over today's databases is ransomware.

Ransomware attacks are no longer reserved for juggernaut corporations and federal government agencies. Due to the massive influx of data that accompanied the digital transformation efforts in 2020, university databases are now becoming juicy targets for hackers to exploit. As a result, higher ed institutions must now view ransomware protection as a table-stakes conversation within their overall data governance and cybersecurity framework.

IT and cybersecurity teams are no longer in charge of protecting and securing well-defined perimeters. Remote students and faculty, satellite campuses, and university medical centers are now sharing and working on the same IT networks and databases in various locations around the country, and – in some cases – around the world.

This type of digital transformation has been both a blessing and a curse for higher ed institutions. The services, applications, and databases have drastically improved the quality of life for students and faculty. However these next-generation technologies – if not adopted, deployed, and protected properly – can create vulnerabilities and holes throughout the entire IT infrastructure, forming new paths and attack vectors that cybercriminals can navigate to penetrate university databases.

Universities must now carefully strategize how to wrap data governance and cybersecurity together, while also segmenting data in secure locations. This is extremely important for universities that hold sensitive GDPR, PII, and HIPAA data.

If institutions do not have a bolstered cybersecurity posture and a strong data governance plan in place, they are leaving their institutions vulnerable to ransomware attacks, which will not only come with a monetary cost for the institution, but a cost to the students and faculty that heavily rely on university services. They also risk hurting their reputation among prospective students and faculty.

Discovering vulnerabilities before the hackers do

Prior to the pandemic, many higher ed institutions were beginning to consider moving their IT environments into the cloud. A challenge arose when IT departments realized that they didn't have a full grasp and understanding of their environments at the time, nor did they understand the IT requirements that they had.

When the pandemic forced institutions to expand the perimeter of their datacenters, the exponential proliferation of IoT connections – alone – made IT departments aware that they didn't have a full picture of their operating environments.

Through solutions and tools, like NetApp's BlueXP and Cloud Data Sense, university DBAs and cybersecurity professionals can now peer not only into their cloud environment but get a better grasp of their on-premises environment, as well. As a result, universities are discovering opportunities to segment and lock down certain environments.

IT departments must scrutinize their data and the locations where their data resides. By doing so, they may discover that they have sensitive data in locations that they weren't even aware of. And if this data, unfortunately, happens to be PII or HIPAA data, it could become a public relations nightmare for a university.

Utilizing the digitally transformative tools that stemmed from the COVID pandemic is definitely a step in the right direction, but deploying tools like BlueXP can give universities an in-depth view into where their data estate, enabling them to begin securing and locking down those vulnerabilities.

Tools like BlueXP can build baselines to detect abnormalities or patterns that are beginning to occur within their data. From there, IT and cybersecurity teams can take the appropriate steps to resolve and remedy these issues.