16 Microsoft Office 365 Management & Security Tips for Higher Ed

CoreView

Colleges and universities already face tough IT challenges – students always coming and going, supporting on-campus and extensive distance learning, and facing security issues from serving up so many end users, many of whom love to practice their emerging hacking skills.

Now that remote work and distance learning are the new mandates, there are even more difficult challenges for Higher Education IT to deal with.

In this whitepaper, we examine Microsoft Office 365 in Higher Education, and offer advice on overcoming obstacles and maximizing benefits.

Microsoft Office 365 (which is being renamed Microsoft 365) already has enormous benefits for Higher Education institutions. Most colleges and universities have buildings spread across often far-flung campuses as well as remote locations, making managing and securing legacy on-premises productivity applications difficult.

The cloud-based Microsoft Office 365 eliminates the need for IT to manage software installed on each machine, allows for use from anywhere and on almost any device, and comes with all the applications and services to make faculty, administrators, staff, and students productive and connected.

Growing Microsoft Office 365 installations, however, come with challenges, chief among them:

- Maximizing Higher Ed IT Economics
- Toughening Security
- Tackling the Insider Threat From Mischievous Students
- Managing Remote Work and Distance Learning
- Managing Remote Devices
- Dealing with External Users
- Identity Management
- Governance
- Adoption and Full Usage of Tools such as Microsoft Teams
- License Management
- M365 Provisioning
- Compliance
- Dealing with Distance Learning
- VPNs
- Managing Remote O365 Admins
- Configuring Teams Voice

Let us take all 16 of these, one-by-one.

1. Dealing with a Tough Economic Environment

The cost of higher education rose 250% over the last 30 years, while family incomes only went up 16% in that same time. Cost savings is one way to control tuition costs. This has led to the IT mandate of harnessing technology to capture new, cost-effective and creative ways to educate.

“It is no surprise that a lot of educational institutions and school districts are getting caught up in the newest technology, but don’t have the infrastructure to support it. Education IT leaders are looking for solutions and guidance about how others have solved their infrastructure issues to move teaching and learning into the digital world,” said The Center for Digital Education in its Market Forecast.

Software is one area of waste and inefficiency. IT often spends more on licenses than it needs to, overbuying licenses so it will not get caught short and not reassigning licenses when people leave.

2. Battening M365 Security Hatches

Microsoft Office 365 holds a vast amount of your institution’s data, perhaps even a majority. This information must be fully secured to protect confidential information, and ensure compliance with relevant regulations. Security is a constant concern, and hackers take advantage of every tragedy such as coronavirus as an opportunity to do harm. Increasing remote access makes this situation all the more dangerous.

CoreView guards against these cybercriminal efforts by logging all O365 actions, and reporting on nefarious outside attacks or sketchy end user behavior. When a malicious attack or other security event occurs, CoreView can go back and show exactly what happened. This way IT can tighten that area down and defend against the next activity.

Here are security items that must be addressed:

- Ensuring the use of complex, regularly changed passwords
- Appropriate and safe M365 administration and end user privileges
- Detection of security holes
- Identifying malware vectors
- Risk reduction
- Proactively monitoring for security hazards
- Making Sure MFA is used
- Granting proper O365 admin rights based on least privilege
- Controlling file sharing

3. Security – When Students are the Insider Threat

Universities are a hotbed for hacking. Students in computer science are learning advanced IT techniques. These same students are curious and want to see if they can get around security controls. The result? Students pose a dangerous insider threat.

Suffering breaches from insiders, including students, staff, and IT itself, is something too rarely talked about. These breaches are far too common, as the annual Verizon Data Breach Investigations report finds that 14% of breaches come from insiders. Insiders are more dangerous than most outsiders are. Insiders are already on the network, and sometimes with high-level privileges. There are different types of insiders who pose specific and varied risks. For instance, many insiders, such as human resources professionals, IT staff, and high-level managers – all have higher-level computer privileges.

To fight off the insider threat, you need a full approach to security, along with the ability to address Microsoft Office 365-specific vulnerabilities. A key issue is knowing what is going on in the network and controlling dangerous activity.

Verizon advises IT to implement strong access controls and provide access levels fitted to true needs, trust, and levels of responsibility. “Having identified the positions with access to sensitive data, implement a process to review account activity when those employees give notice or have been released,” Verizon suggested.

The answer is to identify internal and external threats to your environment — then step up your defenses. Here, CoreSecurity alerts give you an early warning system for internal and external threats to your Microsoft Office 365 environment, so you can identify and defend yourself against security breaches before they occur.

Meanwhile, CoreView reporting is fine grained so data can be analyzed by department, business unit, country, and more, so it is easier to determine exactly where breaches first occur.

4. Dealing with SaaS/Cloud Risks from Remote Work and Distance Learning

Moving to the cloud exposes schools to new and additional risks, and remote work and distance learning add to that security burden. With the move to remote access, it is not just allowing workers from within the institutional environment to access data assets and the cloud, but now the school is opening up to remote employees and students coming in from their own home networks and their own devices, the so-called bring your own device (BYOD) machines.

But how does IT determine that these remote users are proper? The answer is to know who is accessing your tenant, making sure you have proper identity management, know where remote users are coming from and exactly what they are doing.

5. Managing Remote Devices

Even though M365 end users are on SaaS, proper IT security still requires device management. In fact, earlier this year, the United States National Security Agency and Department of Homeland Security ordered every US government agency to report on what version of Microsoft Windows was on each device, and to prove it was fully patched. This rush to report was due to the discovery of a major Windows vulnerability.

CoreView makes this kind of device management easy by inventorying all devices that are joined to Microsoft Office 365 or Azure Active Directory. CoreView reports on who has what devices, what version they are on, and then, even more importantly, what those users are doing with those devices and even what user has what mobile device and with what MDM policy.

If your school's users access Microsoft Teams, CoreView knows when that was, from what IP address, if they did a file transfer, the name of the file, and which conditional access policies were applied as they were trying to sign in. All that data comes from many sources within the Microsoft cloud ecosystem. CoreView consolidates that data, put it into a single report, allows you to zoom out and see from a macro view, and then zoom in to specific transactions and see exactly what's going on.

6. The Problem with External Users

As remote work and distance learning takes hold, the number of external users connecting somehow to O365 increases dramatically – even multiplies.

When COVID-19 hit the U.S. this spring (2020), one CoreView customer had a huge spike over the first 30 days in external collaboration due to remote work and quarantining. The CoreView report below shows the dramatic increase in third party dial-in and dial-out, as well as IM, audio and video — and even application sharing.

Fortunately, with CoreView, you can analyze the behavior of these external users. For instance, IT could see that a professor created a document, put it on his OneDrive share, and shared it externally. Since not every user was an M365 authenticated user, he shared it anonymously.

That is usually not a concern, as most documents do not have confidential data. However, sometimes they do. For those instances, CoreView reports on not only the activity, but if something goes wrong, shows precisely where the access came from. CoreView can also show what has been shared externally in the past, and let IT and internal managers determine if this sharing is still appropriate, and decide if they want to leave that path open, or if it is time to close it down.

7. Identity Management

One of the hackers' favorite exploits is to steal the identity of a user. Proper identity management stops that. It starts with strong complex passwords that are regularly changed. Time strapped Higher Ed IT admins do not always know what is going on with user passwords. They need a way to discover who has weak passwords, who had turned off password expiration, and then automatically enforce strong password policies.

On top of this should be multi-factor authentication (MFA). Unlike password only with a single form of identification, MFA adds another or form or more – this could be a security code sent to a smartphone, biometric, or asking the end user something only they would know.

To make MFA fully work, it must be implemented across all end users, which requires that IT has insight into each user's security state and profile.

8. Instituting Good Governance

Gartner defines IT Governance (ITG) “as the processes that ensure the effective and efficient use of IT in enabling an organization to achieve its goals.” Given that, Microsoft Office 365 is already a leap forward for IT governance of productivity and collaboration applications. However, Higher Ed IT can do better.

For one, IT can streamline Microsoft Office 365 deployment. SaaS tends to be easier to deploy than their on-premises equivalents, but IT should ensure that all end users have the proper set of services with support, training, and easy access.

Most Higher Ed Institutions have cash-strapped IT departments, so managing and maximizing assets are a top concern. You can maximize the value of software and intellectual assets while protecting your information and environment with the CoreView SaaS Management Platform (SMP). CoreView ensures safe and appropriate use of your institution’s data and services, and reports on employee usage and behavior.

And because Higher Ed staffs are often short-handed, both central and distributed IT groups buy duplicates of IT technologies and services, and at the same time, incur higher than needed deployment costs. That is not good governance. The CoreView single pane of glass SaaS management solution gives visibility and supports IT governance policies and priorities, and offers control and true ownership of the O365 environment.

9. Adoption, Productivity, Change Management, and Maximizing Investment

A big part of proper Higher Education governance is fully exploiting the software the institution has in place to maximize productivity. However, did you know that in the typical Microsoft Office 365 environment, 56% of licenses are either inactive, unassigned, or oversized for what the end user actually does? This is a waste of precious Higher Ed IT dollars, and a source of massive unrealized productivity.

To make your faculty, staff and students truly excel, they need to harness the full power of Microsoft Office 365. With CoreView's CoreAdoption, IT knows with real usage data what applications are being exploited. Plus, your workers will apply the right application to a particular task, such as creating meetings with Teams rather than Skype, or Yammer instead of standard broadcast emails.

With Just in Time Learning (JITL) through context sensitive videos, end users will be shown how to work with applications such as Teams for collaboration, or OneDrive for cloud storage.

10. License Management for Savings and Efficiency

Managing M365 end user licenses is a difficult task. One major U.S. university had central IT managing all the M365 licenses for the departments, as many of these groups did not have IT associated with them. Going through central IT to make an O365 license change or assignment can take up to 48 hours.

This school needed a tool to segment their M365 tenant and simplify licensing. With such an approach, each department could be viewed as their own individual virtual tenant, and a local departmental admin could be created and given access to their users to manage their department such as assigning and unassigning O365 licenses.

A European university had a similar license issue. Like with many schools, for this university, student licenses are free. Even so, these licenses still have to be managed. A large or even mid-size college or university can have thousands and thousands of licenses. With so many M365 users, schools often use students to do administrative activities. This school did not want to give admin rights, which under the Microsoft O365 Admin Center means global rights, to students. It did not want students to access teacher information, or touch accounts they have no business even reaching.

The answer was to set it up so student admins only get student info and license info. Other admins were similarly defined and there limited to managing only teachers or school administrators.

“CoreView has enabled us to securely delegate reduced Admin Rights so other departments could have segmented access to our large tenant. This was never possible with the native tools in Microsoft Office 365,” the university’s IT Services Manager explained.

Security was also improved. “Using CoreView we have effectively reduced our response time to research security related incidents from hours and days, to under 10 minutes for most issues,” the university IT pro said. Lastly, CoreView helps the university know how M365 is used across the tenant. “The reports and dashboards inside CoreView have been invaluable for analyzing information on each departments’ Microsoft Office 365 user activities. We have access to troubleshooting data and metrics that we were never able to see before,” the manager said.

11. The Problem with O365 Provisioning

A big pain point at colleges and universities is provisioning and deprovisioning of users, an issue greatly exacerbated by the pandemic and the dramatic shift to remote work and distance learning. Schools often have large student bodies, so this is a problem at a great scale. Not only that, provisioning and deprovisioning cycles are cyclical, so these tasks come all at once versus being spread out over the year. When enrollment for a semester starts, there is a flood of activity. In fact, a lot of educational organizations will put a change freeze on for user provisioning during the slow summer months, and a lot of IT projects are actually executed during these months when activity is low.

This provisioning is quite complex. Depending on where you are in the school matriculation process, students get access to different services. For instance, students may be full or part time. Students may be attending multiple campuses, so part of their classes are at the main campus, but they also go to a satellite campus.

Then as they finish their matriculation, they become alumni. Alumni are a valuable resource to Higher Ed as a funding source, so the schools want to keep tabs on them. Schools often let graduates keep mailboxes, mail addresses, accounts, and may even give them access to online learning going forward.

Making issues more complex, students may become faculty assistants, and then may become faculty, and faculty may be taking classes as students. This deep provisioning is quite complex. For instance, do users keep their data as they move from status to status?

12. Compliance

Higher Ed has to deal with compliance as much as any other vertical. Institutions with medical schools need to deal with HIPAA. The Family Educational Rights and Privacy Act (FERPA), which ensures basic privacy rights for students, also must be dealt with.

Compliance is a big security and economic issue. There are almost daily incidents of fines occurring due to GDPR and other issues, and IT is not usually able to respond quickly.

If you are not aligned with what your top peers are saying and doing, it is a sign of security weakness. How does a shop know how well it handles security? Looking at peers shows you have at least done your due diligence. If we have not approached best practices and compliance, if we cannot measure ourselves with how others are doing in the industry, then we are likely at a severe deficit. That is a career-limiting move.

The way that CoreView surfaces this information is through our enhanced version of Secure Score, which shows exactly how Microsoft Office 365 shops are doing against their peers, measuring items such as doing proper configuration management, applying least privileged access, and handling compliance.

Many compliance regulations ask shops to collect data logs for a specified period of time. However, Microsoft gives you only the last 30 days of data logs (now moving to a full year for E5 licenses). So how do you manage this regulatory requirement? CoreView stores logs for a year at a minimum – and can store them indefinitely.

CoreView tracks and stores all this log information for both admins and end users. On the admin side, for instance, CoreView can produce a report in seconds of every single administrative action an IT staffer has taken on the Microsoft Office 365 platform since they started. End users are tracked in a similar way.

13. Dealing with Distance Learning

With the growth of schools such as the University of Phoenix, distance learning is all the rage. Nowadays, that is even more the case. The technology alternatives for distance learning are increasingly coming down to the Google Classroom and Microsoft Teams for Education. The other big player was Zoom, but Zoom faces troubling security concerns.

Microsoft is poised to benefit from growing work from home security concerns. The reason Microsoft Teams has been accepted by the business community, as well as education, is Teams' authenticated communications. You cannot create fake users. Instead, you have to have an Active Directory account that is under control by the IT team and subject to identity management processes.

That way you know that the person you are talking to really is that person.

14. To VPN or Not to VPN

In order to securely support remote access, many Higher Ed institutions implement virtual private networks (VPN). That might not be a great idea. "I'm seeing an awful lot of educational institutions and corporate organizations making what I think is a huge mistake in trying to deploy VPNs out to these end user devices," said Matt Smith, CoreView Solution Architect. Supporting a VPN is a logistical nightmare with remote users depending on an array of devices and trying to get the VPN client to work across all those disparate machines.

More critical, VPNs bypass the controls Microsoft has at the edge for threat intelligence and the advanced security protocols that come with the Cloud Access Security Broker (CASB) that Microsoft put in place to ensure valid access. A VPN is a backdoor into your institutional network, which gives potentially insecure devices access to the entire network. Not only that, it makes it appear as if that user is originating from inside the network.

If they did come in through the VPN, IT could not pinpoint the ISP or origin, show IP addresses where that user is actually coming from, and which device they are using.

"I'd strongly encourage educational institutions that are rolling out work at home or educate from home — don't do it via VPN. Come in through the internet and take advantage of Microsoft's edge security components to get that access," Smith argued. "Then CoreView's reporting comes into play as far as what they're actually doing and how they're actually configured. We can report on if devices controls such as multi-factor authentication (MFA) are in place."

CoreView also dives deep into the state of M365 security. For instance, as IT starts to put in Microsoft security controls such as conditional access policies, CoreView shows on each session which policies get applied and which do not. CoreView also reports on when schools get sign in attempts from areas where they do not have students, and if their conditional access policy that should be blocking by country location is not being applied.

15. What Happens When IT Administrators Themselves are Remote?

In the early days of O365, most Microsoft Office 365 admins were physically on campus. Now remote work also includes admins who still need to get all their SaaS management duties taken care of. In the case of COVID-19, this remote work is due to a disaster, and constitutes part of a business continuity and disaster recovery effort.

"If all my admins are in the basement of the administration building, and they're the only folks that can provision users and change passwords and so on, that's a big problem. What CoreView allows you to do is distribute out the administrative functions very securely and very granularly to people throughout the organization," Smith explained.

With CoreView, workers in specific departments or groups can gain admin rights, but only to do certain things. "We can securely delegate admin functions out without giving them too much access. CoreView can disperse administrative functionality outside the region, outside the location that is moving aggressively to remote work. You can create a workflow within CoreView that gives workers the ability to do something they don't normally do, such as change passwords," Smith said.

In emergencies, CoreView can offer these administrative rights for a short period, even 15 to 30 minutes. "When emergency situations come up, CoreView can securely delegate specific admin functions out, and minimize the concentration of risk from the traditional M365 administrative model," Smith said.

16. Teams Voice Done Easy and Right

With more telework and telecommuting, having an agile approach to voice configuration is critical, as are using Microsoft Teams voice and collaboration features themselves.

When disaster strikes, Teams is the ideal backup communications method. If workers do not have access to their desktops in the office, they should still get to Teams – and have access to VoIP over Teams. "For those customers who haven't looked at using Teams as a virtual PBX, I strongly advise them to do that even for just its disaster recovery capability. While it could be the replacement for the primary phone system, if it is not — it is still the ideal backup. Along with that capability, Teams has the ability to function as a PBX, to have an auto attendant that says, for instance, 'Hi, thanks for calling ABC University. Please press one for alumni, or two for student services.'" Smith explained.

Having these voice capabilities and fully using them are two different things. Fortunately, CoreView has the unique ability to delegate out the right to create call queues and to upload auto attendants. "Imagine we're dispersed right now within education. You have the college of business, the college of medicine, the college of physical sciences, and so forth. Each one can be delegated their ability to create their own auto attendant and define what the call queue is. When you push one for Alumni Relations, it is going to go out to one of five people. However, those five people have likely changed. If I am sending this all back to a central admin who is the Teams administrator, he has to manage the call queues, and the auto attendant for the entire organization. They are going to be overwhelmed. They can't react nimbly to it," Smith said. "What CoreView allows you to do is delegate that out securely to individuals just for their department, and allow them to manage that themselves."

This is not only faster and more fluid, but central IT does not necessarily have the knowledge of how all these voice systems are set up, and may have trouble reacting to emergencies.

The Role of a SaaS Management Platform (SMP)

SaaS applications have their own native IT administrative consoles, requiring administrators to use multiple consoles to manage their SaaS applications. Microsoft O365 is a bundle of different SaaS solutions, and each service has its own console.

The SaaS Management Platform (SMP) eases these management and administrative tasks. SMPs, as defined by Gartner, have six major functional categories: administration, IT role-based access control, policy management, license management, workflow automation, and reporting. The CoreView SMP enriches these capabilities with two additional functional categories: Change Management and Learning to help customers to maximize their ROI from Microsoft M365 and improve users' digital dexterity and productivity.

Learn More About O365 and Higher Education

Learn to maximize your O365 services with a CoreView demo.