Let's talk about advanced cybersecurity controls with Office 365.  We call it modernized security.  Who is ready? Here we go!  Identity is the new security boundary. For many decades, boundaries were dictated by traditional firewalls or routers. That was a simple life. Today, proper identity management is key to securing any environment. It used to be that we controlled what identities came into our networks and applications. It was our directory space. That’s no longer true in today's multi-cloud, multiple-identity world.

## Identity & the Dark Web

Most people associate the “dark web” with a murky underworld where users buy and sell illegal items, such as drugs, counterfeit passports, or weaponry.  It is also proven to be a popular destination for users to traffic in stolen identity data. This includes banking information and online streaming credentials.  As a result, the extent to which our private and financial data is readily available to anyone willing to pay for it is downright scary.

“In the not-so-distant past, the 'dark web' was difficult to access; one could only access these sites if you knew the IP address, and you had to use a proxy to access the sites at all. Today, darknet hacker markets are starting to look more and more like the e-commerce markets that exist everywhere else online. You can purchase an entire identity online for less than the cost of a new iPhone.”

## Protect, Detect, and Respond to Cybersecurity Attacks

Office 365 users are particularly well positioned to protect, detect, and respond to attackers. Although Office 365 does not eliminate your responsibility for data security, it does provide advanced security controls. Each of these security controls was discussed in detail at the workshop.

## PowerShell Baseline & Monitoring

PowerShell (also known as Windows PowerShell) is a command-line environment that's designed specifically for system administration. It helps IT professionals and power users control and automate the administration of the Windows operating system and applications, such as Office 365.
It is complementary to the Office 365 admin center. As a result, the Office 365 admin center

is the out-of-box solution that spans the entire administration lifecycle from setup to support. The Office 365 admin center is designed to handle the most common administration tasks such as adding and editing users and setting common service settings. However, there may be situations such as:

- Adding or editing a large number of users
- Using multiple filters to sort through data
- Exporting data such as user lists and groups
- Configuring less commonly used settings

## Privileged Access Workstations

Privileged Access Workstations (PAWs) provide a dedicated operating system for sensitive tasks that is protected from Internet attacks and threat vectors. Separating these sensitive tasks and accounts from the daily use workstations and devices provides very strong protection from phishing attacks, application and OS vulnerabilities, various impersonation attacks, and credential theft attacks such as keystroke logging, Pass-the-Hash, and Pass-The-Ticket. Learn more about how to protect high-impact privileged accounts here.

## Multi-factor Authentication

Multi-factor authentication is a method of verifying who you are that requires the use of more than just a username and password. Using MFA for Office 365, users are required to acknowledge a phone call, text message, or app notification on their smartphones after correctly entering their passwords. They can sign in only after this second authentication factor has been satisfied. Learn how to set up this security protocol here.

## Data Loss Prevention

To comply with business standards and industry regulations, organizations need to protect sensitive information and prevent its inadvertent disclosure. Examples of sensitive information that you might want to prevent from leaking outside your organization include financial data or personally identifiable information (PII) such as credit card numbers, social security numbers, or health records. With a data loss prevention (DLP) policy in the Office 365 Security & Compliance Center, you can identify, monitor, and automatically protect sensitive information across Office 365. In addition, you can learn more about DLP here.

## Administrator & User Auditing

Exchange administrator audit logging is enabled by default in Office 365.  It logs an event in the Office 365 audit log when an administrator (or a user who has been assigned administrative permissions) makes a change in your Exchange Online organization. Changes made by using the Exchange admin center or by running a cmdlet in Windows PowerShell are logged in the Exchange admin audit log. For more detailed information about admin audit logging in Exchange, see Administrator audit logging here.

---

## Pro Tip for Office 365 Users

The Security & Compliance Center is your one-stop-shop tasks like device management, data loss prevention, eDiscovery, retention, and so on.Permissions in the Security & Compliance Center are based on the Role Based Access Control (RBAC) permissions model. This is the same permissions model that's used by Exchange.  If you're familiar with Exchange, granting permissions in the Security & Compliance Center will be very similar. It's important to remember, however, that Exchange role groups and Security & Compliance Center role groups don't share membership or permissions. While both have an Organization Management role group, they aren't the same. The permissions they grant, and the members of the role groups, are different. There's a list of Security & Compliance Center role groups here.

In addition to the above security features available with Office 365, E5 users have access to these advanced security features:

## Advanced Threat Protection

New malware campaigns are being launched every day, and E5 comes with a solution to help protect your email against them. Thus, with Office 365 Advanced Threat Protection, you can protect your mailboxes against attack, *even zero-day exploits*. It works by scanning links and attachments in real time. If a link or attachment is unsafe, the user is warned not to visit the site or informed that the site has been blocked. Reporting is available, so administrators can track which users clicked a link and when they clicked it.

## Advanced Modernized Security Management

The cloud offers many security benefits to organizations, and also it raises new security considerations. It can also add to existing ones such as shadow IT, the use of software that is not formally sanctioned by the organization. Office 365 Advanced Security Management, a new set of capabilities powered by Microsoft Cloud App Security, gives you greater visibility and control over your Office 365 environment.

Advanced Security Management includes:

- Threat detection—Helps you identify high-risk and abnormal usage and security incidents.
- Enhanced control—Shapes your Office 365 environment leveraging granular controls and security policies.
- Discovery and insights—Get enhanced visibility into your Office 365 usage and shadow IT without installing an endpoint agent.

Take a deep dive on each one of these areas here.

## Modernized Security Conclusion

The Threat is Real!  As a result, cyber attackers spend a median of 8 months on your network before they are ever detected. Oftentimes, it is law enforcement who notifies the business of the malicious behavior. Take the next step to protect your identity by scheduling a one-on-one with a cybersecurity expert. Get in touch.

---

## Next Steps

Review our case studies and engagements where we helped companies just like yours solve a variety of business needs.

---

## About Oakwood

Since 1981, Oakwood has been helping companies of all sizes, across all industries, solve their business problems.  We bring world-class consultants to architect, design and deploy technology solutions to move your company forward.  Our proven approach guarantees better business outcomes.  With flexible engagement options, your project is delivered on-time and on budget.  11,000 satisfied clients can’t be wrong.

**Like what you've read? Please spread the word!**