WHITE PAPER

State of Microsoft 365 Security

VECTRA®
SECURITY THAT THINKS

TABLE OF CONTENTS

Overview 2
Dark Halo – A Watershed M365 Security Incident....................3
New Dark Halo Techniques In the Wild 4
Defend Beyond Default 5
Scan Deep – Fix Fast 7
Comprehensive and Compliant 8
Collaborate with Confidence....................9

Overview

The rapid increase in the use of Microsoft's cloud services has occurred without appropriate security governance, policies and controls in most cases. This has resulted in attackers turning their attention to Microsoft 365 (M365) as a primary attack point for everything from industrial espionage[i], ransomware delivery[ii], and interruption of military operations[iii].

> The absence of a centralized, scalable and objective view of M365 security can overwhelm security teams.

The M365 platform does provide unparalleled capabilities for collaboration, and enterprises around the world have come to depend on Exchange Online, OneDrive and Teams as critical platforms to keep their businesses running. Research in 2021 suggests that over 80% of enterprises rely on at least one component of Microsoft's 365 platform. Whether it's just a simple Azure Active Directory synchronization to enable Office 365 licensing, Exchange Online for messaging, or Teams for collaboration and meetings[iv]. However, with thousands of settings available to configure for each user, security teams can be overwhelmed due to the lack of a centralized, scalable and objective view of security within M365.

Dark Halo – A Watershed M365 Security Incident

The first M365 security incident to grab the attention of security leaders at a global scale was the Dark Halo campaign which made headlines in December 2020[v]. Dark Halo was a set of attack techniques that piggybacked on the Solar Winds supply chain compromise, where federated identity credentials were stolen from on-premises identity platforms such as Okta, Duo and Active Directory Federated Services[vi]. The APT29[vii] crew used compromised privileged federated identity credentials to burrow into target organizations' M365 platform to gain unauthorized access to user identities and sensitive data.

#include <iostream>
#include <string>
using namespace std;
upload __datacollector_2_0_9
string encodeSecurity(string str, int shift);
int main()
{
string str, encoded_string;
int shift;

Once the attackers had administrative privileges within the target's M365 tenant, they ran a playbook to use M365 services as part of their campaign. Using PowerShell, the attackers' tactics ranged across MITRE ATT&CK Framework techniques[viii]. An example of how these techniques were used against a US Civilian Government Department to gain unauthorized access to material information relating to the US Government's response to the COVID-19 pandemic include:

- **Initial Access** – Exchange Administrator's credentials cloned by harvesting Duo MFA Authentication Server API keys and issuing authentication tokens that appeared legitimate to the target's M365 Exchange Administration portal
- **Defense Evasion** – Disabling of key auditing and logging settings for Exchange Online Admins and material users' mailboxes within the M365 tenant
- **Credential Access** – Creation of an Exchange Online Admin user for the Attackers' use
- **Collection** – Enabling of legacy email protocols (such as IMAP) to allow the Attackers to gain access to mailboxes in near real-time without requiring MFA
- **Exfiltration** – Creation of Power Automate flows to exfiltrate data on a scheduled basis to bypass DLP policies within the M365 tenant

The net result of these activities was the loss of material information relating to the US Government's COVID-19 response policy[ix].

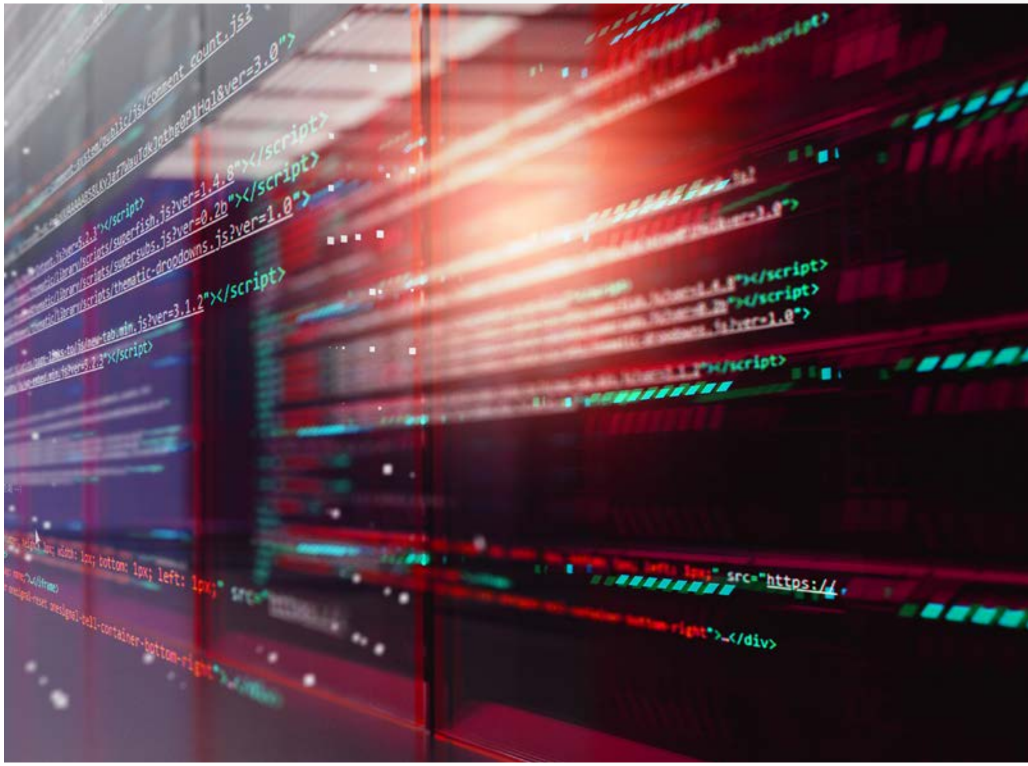
New Dark Halo Techniques In the Wild

In early 2021, the effects of the Hafnium campaign made the news and most organizations focused on the impact that the malware had within on-premises Exchange Servers. In research Vectra conducted with Jake Williams, Executive Director of Cyber Threat Intelligence at SCYTHE, the use of Hafnium exploits are to gain access to Exchange on-premises and then pivot into M365 tenants. This attack pattern was identified among organizations relying on hybrid Exchange architectures.

The attacks would begin with exploiting the Outlook Web Access vulnerability, elevating privilege on the Exchange Server, scraping credentials from that environment and then using those credentials to connect to M365. Once within M365, the attackers could then use techniques associated with Dark Halo campaigns to evade detection and expand unauthorized access to Azure AD identities and data stored within M365.

By late 2021, another global attack campaign, Nobelium, had impacted tens of thousands of additional M365 customers.

As with any cyberweapon, the techniques originally unleashed by the APT29 group rapidly proliferated to being used by even the least-sophisticated ransomware groups. They have now been used to compromise hundreds of thousands of organizations' M365 tenants around the world. Combined with the Hafnium and Nobelium techniques, there are very few M365 customers who have NOT been impacted in some way by these attacks.



Unfortunately, the vast majority of organizations have relied on the default settings within M365 within their tenants. As has been proven by the scale of the exploits seen over the last 2 years, these default settings are not enough to protect against these rapidly evolving attacks.

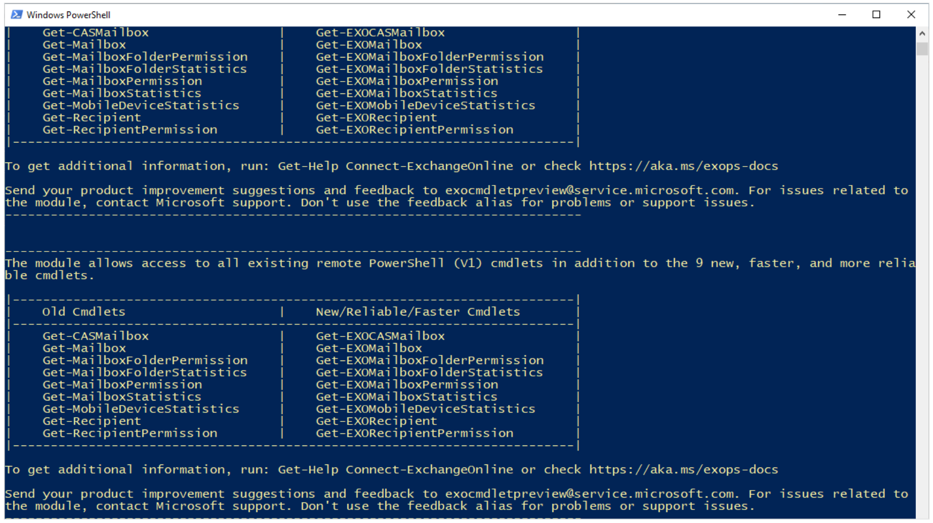
Defend Beyond Default

Just as you would not keep the same keys as the previous renters of an apartment, why would organizations rely on the default settings for the most critical of business tools? Part of the reason why organizations have left these default settings in place is due to the extraordinary complexity of the M365 platform, the obscurity of M365 security settings documentation and the lack of technically-skilled staff to manage these settings at scale.

In research conducted by Vectra, we have identified over 7,500 potential settings within even the middle-of-the-road E3 license of M365. Organizations with E5 licenses have significantly more settings to manage-per-user. Some of these settings are trivial from a security perspective, such as whether a user has selected to view OneNote in Dark Mode[x]. Others such as enabling Azure Active Directory to generate or rely on legacy SAML tokens can create significant security exposure within your tenant[xi].

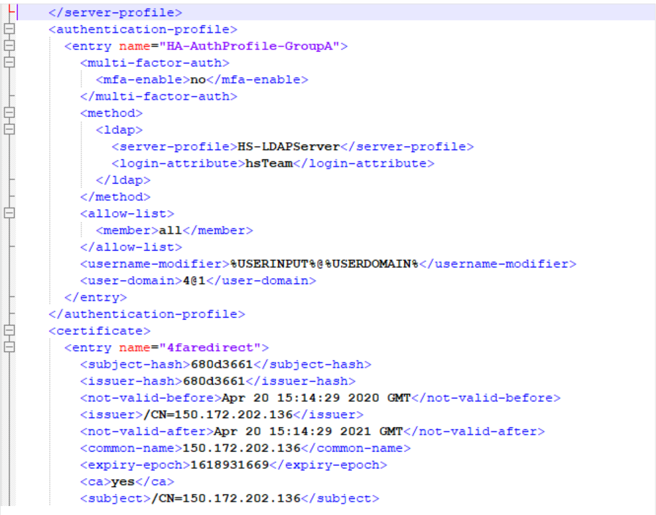
Even small organizations with a few hundred M365 users now have to deal with hundreds of thousands of settings on a per-user basis. The sheer scale of the task confronting security teams when it comes to locking down M365 has created a sense of dread among even the best-resourced enterprise security teams. Part of the problem is the fact that it is very difficult to gain full visibility into security settings for each user as PowerShell is the only tool that can be used for wholistic control of settings. Most of the time these settings are buried behind a clunky M365 portal user interface and worse still, not all setting are exposed.

Forcing security teams to use a command-line interface for complex security tasks like threat hunting, material change detection and Indictor of Compromise (IOC) analysis can lead to significant security analyst dissatisfaction and frustration.



```
|     Get-CASMailbox                        |     Get-EXOCASMailbox                     |
|     Get-Mailbox                           |     Get-EXOMailbox                        |
|     Get-MailboxFolderPermission           |     Get-EXOMailboxFolderPermission        |
|     Get-MailboxFolderStatistics           |     Get-EXOMailboxFolderStatistics        |
|     Get-MailboxPermission                 |     Get-EXOMailboxPermission              |
|     Get-MailboxStatistics                 |     Get-EXOMailboxStatistics              |
|     Get-MobileDeviceStatistics            |     Get-EXOMobileDeviceStatistics         |
|     Get-Recipient                         |     Get-EXORecipient                      |
|     Get-RecipientPermission               |     Get-EXORecipientPermission            |
|---------------------------------------------------------------------------------------|

To get additional information, run: Get-Help Connect-ExchangeOnline or check https://aka.ms/exops-docs

Send your product improvement suggestions and feedback to exocmdletpreview@service.microsoft.com. For issues related to
the module, contact Microsoft support. Don't use the feedback alias for problems or support issues.
-----------------------------------------------------------------------------------------


-----------------------------------------------------------------------------------------
The module allows access to all existing remote PowerShell (V1) cmdlets in addition to the 9 new, faster, and more relia
ble cmdlets.

|---------------------------------------------------------------------------------------|
|     Old Cmdlets                           |     New/Reliable/Faster Cmdlets           |
|---------------------------------------------------------------------------------------|
|     Get-CASMailbox                        |     Get-EXOCASMailbox                     |
|     Get-Mailbox                           |     Get-EXOMailbox                        |
|     Get-MailboxFolderPermission           |     Get-EXOMailboxFolderPermission        |
|     Get-MailboxFolderStatistics           |     Get-EXOMailboxFolderStatistics        |
|     Get-MailboxPermission                 |     Get-EXOMailboxPermission              |
|     Get-MailboxStatistics                 |     Get-EXOMailboxStatistics              |
|     Get-MobileDeviceStatistics            |     Get-EXOMobileDeviceStatistics         |
|     Get-Recipient                         |     Get-EXORecipient                      |
|     Get-RecipientPermission               |     Get-EXORecipientPermission            |
|---------------------------------------------------------------------------------------|

To get additional information, run: Get-Help Connect-ExchangeOnline or check https://aka.ms/exops-docs

Send your product improvement suggestions and feedback to exocmdletpreview@service.microsoft.com. For issues related to
the module, contact Microsoft support. Don't use the feedback alias for problems or support issues.
```

Figure 1: PowerShell Interface to Exchange Online



```
  </server-profile>
  <authentication-profile>
    <entry name="HA-AuthProfile-GroupA">
      <multi-factor-auth>
        <mfa-enable>no</mfa-enable>
      </multi-factor-auth>
      <method>
        <ldap>
          <server-profile>HS-LDAPServer</server-profile>
          <login-attribute>hsTeam</login-attribute>
        </ldap>
      </method>
      <allow-list>
        <member>all</member>
      </allow-list>
      <username-modifier>%USERINPUT%@%USERDOMAIN%</username-modifier>
      <user-domain>4@1</user-domain>
    </entry>
  </authentication-profile>
  <certificate>
    <entry name="4faredirect">
      <subject-hash>680d3661</subject-hash>
      <issuer-hash>680d3661</issuer-hash>
      <not-valid-before>Apr 20 15:14:29 2020 GMT</not-valid-before>
      <issuer>/CN=150.172.202.136</issuer>
      <not-valid-after>Apr 20 15:14:29 2021 GMT</not-valid-after>
      <common-name>150.172.202.136</common-name>
      <expiry-epoch>1618931669</expiry-epoch>
      <ca>yes</ca>
      <subject>/CN=150.172.202.136</subject>
```

Figure 2: Sample M365 User Manifest

Each user has thousands of configuration options which can be manipulated through PowerShell, and domain expertise in this area is very difficult to come by. Additionally, Microsoft has not released comprehensive administration or security guidance on how to optimize security settings within M365. Forcing security teams to look through mountains of user configuration manifests is not an effective or scalable way to defend an M365 tenant from even low-sophisticated threat actors like miscreants in ransomware gangs.

When security teams begin to dig into the M365 security problem, they rapidly discover that there is no single-view into the security posture of M365 as a whole. In fact, Microsoft still has two completely distinct and separate interfaces that security teams need to monitor for every user, the Graph API and PowerShell Modules within M365[xii]. While Microsoft has created the Defender suite of tools and services such as the Microsoft Secure Score, in many cases these recommendations are designed to motivate an organization to upgrade their Microsoft license instead of optimizing the security settings that can be configured within their existing license entitlement.

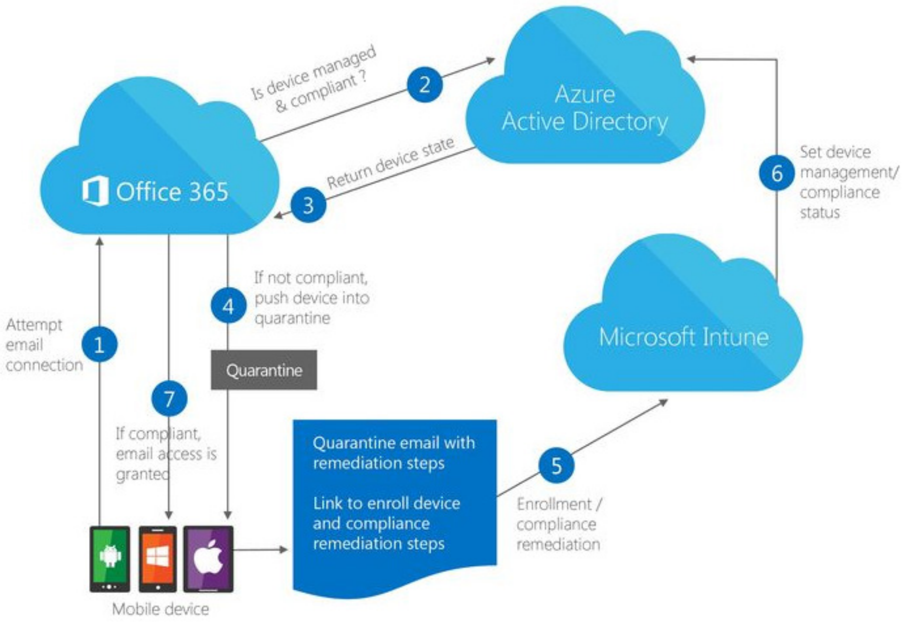

Office 365
Is device managed & compliant ?
2
Azure Active Directory
Return device state
3
6
Set device management/ compliance status
Attempt email connection
1
4
If not compliant, push device into quarantine
Quarantine
Microsoft Intune
7
If compliant, email access is granted
Quarantine email with remediation steps
Link to enroll device and compliance remediation steps
5
Enrollment / compliance remediation
Mobile device

Figure 3: Conditional Access Sample Flow

For example, the Microsoft Secure Score[xiii] only checks 23 configuration settings within an M365 environment, and many of those are only evaluated at a global tenant level, not from a per-user or per-mailbox perspective. The Secure Score does not have the option to enable for material change detection, nor does it provide the capability to model conditional access policies to evaluate the actual effective settings versus what an M365 administrator perceives as the policy that has been configured.

The complexities of Conditional Access[xiv] can vex even the best M365 administrators, this is due to the fact that the most-permissive policy is the effective policy for a user. For example, in a case where a security team has configured a conditional access policy to block the use of legacy email protocols like IMAP, it is configured for ‘all users’ in the tenant. A knowledgeable attacker can create a Conditional Access policy which enables IMAP for the CEO’s and CFO’s mailboxes, those two users’ accounts are now vulnerable to MFA bypass, as IMAP only requires the simple combination of a username and password via basic authentication.

The M365 PowerShell Module integrations within Vectra Protect facilitate the only scan specifically designed for managing the complexities of Conditional Access policies within Azure AD to uncover identity vulnerabilities in cloud tools and connections.

The complexities of M365 combined with the lack of documentation and security team expertise creates a fog around M365 security for most organizations. Analysis paralysis would be the best label for what thousands of organizations are dealing with today for M365 security. Any security leader understands the criticality of M365 to their business, but very few have a comprehensive strategy to take effective action.

Scan Deep – Fix Fast

Cloud-based tools are essential for remote and hybrid work environments, but the on-premises approach to security and access management is no longer adequate. For example, most vulnerability management programs do not include scanning the infrastructure as code that exists on a per-user basis within the M365 cloud. Only Vectra has developed a security scan engine that is capable of enumerating security settings for users across the Graph API and PowerShell Modules within M365.

This depth of discovery provides security teams with unparalleled visibility into the overall risks associated not only with global M365 settings like those provided by Microsoft Secure Score, but also per-user and per-mailbox vulnerabilities that can be left exposed with M365 default settings. The only way to manage these problems at scale is through the use of posture management tools, like Vectra Protect.

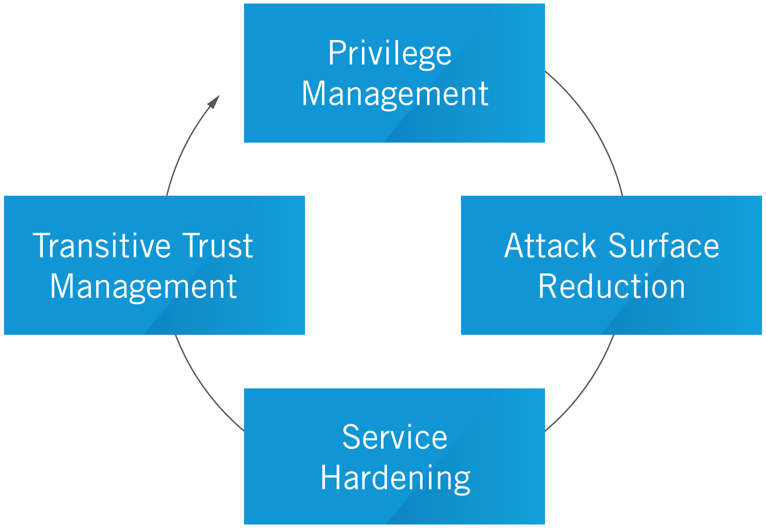


Figure 4: Vectra Protect Multi-Stage Methodology

With Vectra Protect, scan deeper and fix faster to bridge the gap between default settings and a truly hardened M365 environment.

Vectra has incorporated the results of over 50,000 hours of research and development of M365 and its security settings, attack paths, security incident root cause analysis and red team activities to produce the first posture management solution designed specifically for Azure Active Directory and the M365 services that ride on top of it. Our multi-stage methodology shows security teams actionable results that previously were available only through costly and time-consuming consulting engagements. Once configured, a Vectra Protect for M365 scan takes just a matter of hours to complete, even for the largest of enterprises and provides a detailed risk assessment of the scanned M365 tenant.

Rather than burying security teams with alert and event overload through a constant stream of data, the Vectra Protect scan engine provides a clear summary report with a prioritized list of mitigation strategies, including granular details about specific user accounts that may have excess privileges, mailboxes that have been configured to allow unauthorized access to emails, SharePoint sites which allow for anonymous access to data and Teams policies which could facilitate data loss, to name a few.

These clearly prioritized findings help security teams move from analysis paralysis to immediate actions that can be accomplished working alongside M365 operations teams. In addition to clear prioritization of findings, Vectra Protect includes specific commands that can be run from PowerShell to scalably address findings as well as step-by-step guidance if M365 administrators want to remediate risks through the M365 admin portals.

With Vectra Protect, scan deeper and fix faster to bridge the gap between default settings and a truly hardened M365 environment. Obtain the full potential of M365 without subjecting your organization to unnecessary risks.

Comprehensive and Compliant

Based upon best-in-class automation, every Vectra Protect scan creates an M365 security assessment that is tailored for your business. While there are configurations guides, such as those available from the Center from Internet Security (CIS)[xv], they require interpretation and action plans. For large organizations, the development of remediation plans based upon the CIS Benchmark for M365 can take weeks, even months. The Vectra Protect scan automates the creation of remediation plans, reducing the time to develop a plan to a matter of hours. The CIS Benchmark also does not include insights into the operational user impacts for their recommendations. Only the Vectra Protect scan provides visibility into the friction that could be introduced to M365 users if security settings are hardened.

Through the unique combination of security risk impact ratings and user operational impact scoring, technology teams can collaborate to tackle the simplest and highest-impact security settings first, then build remediation approaches to deal with the more complex security issues that could have significant operational impact on users and business processes.

Vectra Protect enables effective M365 security governance, so security teams can meet and the highest industry standards.

Vectra Protect delivers clear security guidance that enables security teams to build effective M365 security governance approaches like never before. With that security governance in hand, monitoring for drifts and anomalies can be achieved through the use of the Vectra Protect continuous scanning module. Security teams can monitor for material changes within the tenant, which then provides a much higher level of assurance that the identities and data within M365 are continuously protected.

Security teams using Vectra Protect for M365 can provide IT and business leaders with proof that security policies that were developed are actually effective and that the organization is adhering to the highest industry standards for M365 security, exceeding regulatory requirements. Vectra Protect customers can use scan reports in their regulatory compliance reports and include them in cyber insurance questionnaires to prove that M365 security is a priority for the organization.

Auditors trust Vectra as recognized leader in the Microsoft partner ecosystem[xvi], a member of the exclusive Microsoft Intelligent Security Association (MISA)[xvii] and the only Azure AD scan that has been approved for inclusion in the Azure Marketplace[xvii].

Collaborate with Confidence

Organizations can only fully realize the advantages of M365 if it is properly secured. Vectra Protect empowers CIOs and CISOs with context and key data points to fulfill the promise of secure cloud technology deployments. We help them make it possible for their businesses to operate essential tools in the state that technology leaders expect – secure and assured.

The sooner that your M365 tenant is hardened, the faster your users can increase their productivity and efficiency in M365. By ditching the default settings and aligning operations with a clear set of security priorities and sustainable security processes the less friction and more efficient your M365 deployment becomes. Get the most out of your technology investment by protecting it and your employees with Vectra Protect.

Organizations can only fully realize the advantages of M365 if it is properly secured.

Vectra Protect removes ambiguity and provides clarity on security misconfigurations and risks within M365. By delivering clear and actionable security recommendations with transparent operational impact analysis all members of the M365 operations and security teams can understand the risk severity and operational impact of the vulnerabilities. Remediation can then be prioritized based on risk appetite and business needs.

The Vectra Protect scan delivers rich context around why each misconfiguration is important. Security teams do not need to become M365 experts and can rely on industry leading threat research and remediation information. Operations teams are provided information to implement the right fix and continuous scanning capabilities to ensure drift does not occur. And CIOs and CISOs can be confident in the security posture of their M365 technologies and focus on driving their business forward.

[i] https://www.theregister.com/2022/05/04/microsoft_exchange_mergers/
[ii] https://gadget.co.za/ransomware-rises-in-kenya-as-office-365-targeted/
[iii] https://www.cisa.gov/news/2022/02/16/new-cybersecurity-advisory-protecting-cleared-defense-contractor-networks-against
[iv] https://www.zdnet.com/article/microsoft-teams-now-has-more-than-270-million-monthly-active-users/
[v] https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/
[vi] https://media.defense.gov/2020/Dec/17/2002554125/-1/-1/0/AUTHENTICATION_MECHANISMS_CSA_U_OO_198854_20.PDF
[vii] https://attack.mitre.org/groups/G0016/
[viii] https://medium.com/mitre-attack/identifying-unc2452-related-techniques-9f7b6c7f3714
[ix] https://www.theguardian.com/technology/2020/dec/13/us-treasury-hacked-group-backed-by-foreign-government-report
[x] https://techcommunity.microsoft.com/t5/office-365-blog/go-dark-mode-and-more-on-onenote/ba-p/653056
[xi] https://docs.microsoft.com/en-us/azure/active-directory/saas-apps/saml-tutorial
[xii] https://o365reports.com/2022/04/27/get-mfa-status-of-office-365-users-using-microsoft-graph-powershell/
[xiii] https://docs.microsoft.com/en-us/microsoft-365/security/defender/microsoft-secure-score?view=o365-worldwide
[xiv] https://practical365.com/planning-for-azure-ad-conditional-access-policies/
[xv] https://www.cisecurity.org/benchmark/microsoft_365
[xvi] https://www.vectra.ai/news/vectra-ai-recognized-as-a-microsoft-security-excellence-awards-finalist-for-security-isv-of-the-year
[xvii] https://www.microsoft.com/security/blog/2020/09/21/vectra-microsoft-join-forces-step-up-detection-response/
[xviii] https://azuremarketplace.microsoft.com/en-us/marketplace/apps/aad.siriuxcustomerdashboard

Email info@vectra.ai vectra.ai