A CREO WHITE PAPER

Reducing Cloud Security Risks in M365

Potential. Unleashed.

Hard Truths About Cloud Security

Many life sciences organizations are operating under the mistaken perception that their cloud-hosted IT environments are secure. Real-world security studies paint a very different picture.

Cloud-oriented cybersecurity attacks grew over 150% from 2023 to 2024. More than one out of every ten hosts on public clouds currently have high or critical vulnerabilities, and life sciences and healthcare organizations are top targets. If industry leaders think it won't happen to them, a recent survey showed that 80% of companies experienced at least one serious cybersecurity incident within the past 12 months.

Conventional wisdom is that security breaches reflect the creativity and diligence of highly motivated hackers. While true, an organization's own misconfiguration of cloud systems and resources is the third leading cause of data breaches. Almost 23% of all cloud security incidents are a direct result of cloud misconfiguration, and 27% of businesses have encountered security breaches in their public cloud infrastructure. And though many industry leaders mistakenly believe this avoidable vulnerability is their vendors' responsibility, these exposures are a direct reflection of their own operations.

Sources: Checkpoint, Palo Alto Networks, IBM, SYNK, SentinelOne

The Microsoft Footprint

To explore the risks and impacts of cloud technology misconfigurations, it's useful to look at specific examples of industry cloud adoption. For many life sciences organizations, a compelling starting point for assessing their cloud security posture is with their investments in Microsoft technologies.

Microsoft technologies are not inherently less secure than other cloud technologies. On the contrary, Microsoft has been a leader in developing more secure and managed cloud environments and operations for many years. But there are several reasons why Microsoft's technologies represent a good starting point for assessing cloud vulnerabilities:

Huge corporate install base

Microsoft technologies are pervasive across most companies. As such, these products represent popular training and proving grounds for malicious actors.

Large user community

Within most enterprises, Microsoft technologies are used by virtually all employees. That level of coverage means the attack surface and potential victim pools are quite large.

Sophisticated technology services

The Microsoft technology portfolio is complex and deeply integrated. Effective management can be challenging, and breaches in one area can create avenues for deeper attacks.

Changing environments

As organizations grow, migration and integration of Microsoft-related environments and applications is commonplace. These events create opportunities for gaps and errors, and event-related press releases increase the visibility to bad actors.

Critical data

From users to customers to proprietary intellectual property, the data flowing through the Microsoft stack is very sensitive. Protecting the integrity of its data is vital to the health and operations of any life sciences organization.

Shared credentials

The Microsoft technology stack is often the home for user and system accounts within the enterprise. As these accounts provide access to all enterprise resources (e.g., single sign-on), they make attractive targets for attacks.

Considering Microsoft 365

Within the Microsoft product portfolio, the Microsoft 365 (M365) suite is a great place to focus. Representing a broad collection of products and services, M365 is notable for its inclusion of multiple cloud-oriented applications core to many enterprise customers. These include:

- **Microsoft Exchange**: serving as the email and calendaring solution for many enterprises.
- **Microsoft SharePoint**: offering the intranet and knowledge management environment.
- **Microsoft Defender**: delivering antivirus services for Windows-based systems and cloud-based security.
- **Microsoft Teams**: providing collaboration, chat, and calling capabilities.
- **Microsoft Entra ID**: managing identity and access services for systems and users.

As organizations move to adopt these solutions, there is often confusion between two related but distinct security concepts: vulnerability management and configuration management. Vulnerability management focuses on identifying and addressing security weaknesses. Configuration management ensures systems are set up correctly and reflect the operating needs of the organization. Providers of cloud services and other software-as-a-service offerings are usually accountable for addressing vulnerabilities, but they are not experts in how each life sciences organization operates. As such, configuration management is left up to the customer to navigate and maintain.

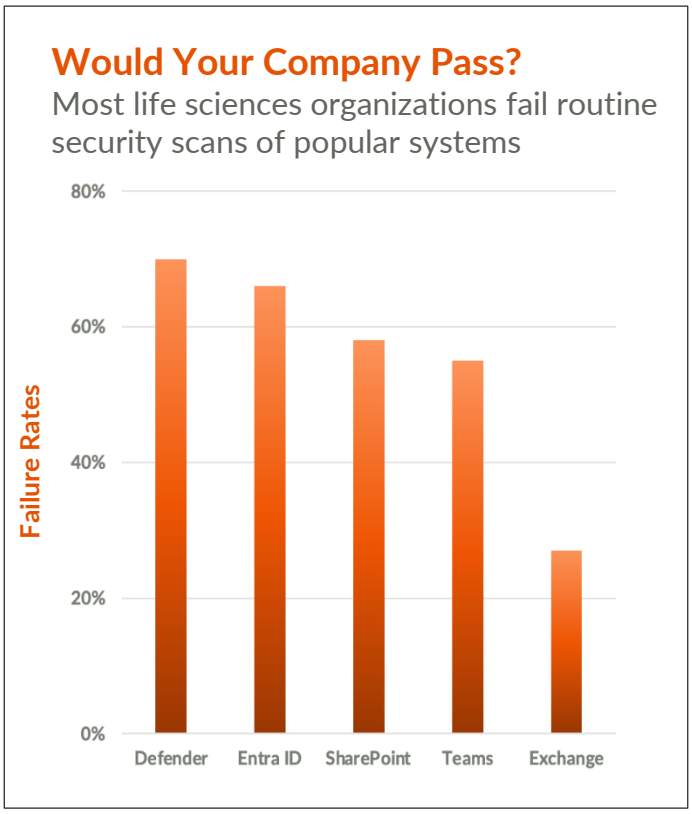
When organizations deploy these solutions and others for the first time, they often accept the default configuration settings offered by the installation and setup routine. Regardless of software manufacturer, installation routines are not generally designed to deploy finely tuned, secure instances of the software. On the contrary, most installation and setup routines are designed to offer functional, easy-to-use versions of the software that can be subsequently configured and tuned to the unique operating requirements of the organization.

Unfortunately, many organizations do not have the technical expertise to secure, tune, and optimize all the various software services being deployed. Individuals may specialize in understanding one or two specific products – Exchange, for example, may be prioritized given the prevalence of email-based threats - but will have much less awareness of exposures in other areas of the architecture. After installation and basic setup, the resulting operating environment is assumed to be successfully deployed by both the life sciences company and the technology vendor, though systems may lack sufficient controls to protect the company's operational integrity, users, and critical data.

Real-World Risks

Analysis of real-world security data confirms that life sciences organizations are often unsuccessful in securing their cloud-oriented environments. When CREO cybersecurity experts analyze security scanning data across M365 customers, less than half of all customers successfully pass the tests. Ironically, the customer's configurations of Microsoft's security-oriented products tend to have more challenges than systems like Exchange. Around two of every three organizations do not pass a security scan of Defender or Entra ID. This gap is understandable when you consider that many organizations are not staffing dedicated security and cloud experts.

Due to the interconnected nature of modern cloud systems, security gaps in these product configurations can quickly escalate to penetration of numerous other systems. For example, many life sciences organizations use the single sign-on (SSO) services provided by Entra ID to authenticate users with non-Microsoft applications such as clinical research systems (e.g., electronic data capture, clinical trials management, drug safety), laboratory information management systems (LIMS), and other solutions. If MS Entra ID is not configured properly, an organization is widening the "impact radius" and possibly allowing an attacker to navigate beyond M365. Organizations may also offer partners "guest" access by delegating authentication; in doing so, they run the risk that exposures in either company can compromise the operational integrity of both.



Hybrid cloud architectures – where organizations leverage cloud software and services from more than one technology provider – further complicate security management. In these scenarios, multiple cloud environments need to be configured, secured and protected. In addition, these environments need the ability to mutually authenticate users, securely connect, and share data. To accomplish these goals without creating additional security vulnerabilities, additional steps are often recommended.

Sources: CREO analysis of proprietary scan findings

The Five Costs of Configuration Failures

The term "configuration error" sounds small, but minor defects can be exploited with dramatic effect. Below are the five costs of failures in secure configurations.

1. Security breaches. Misconfiguration of cloud services provides an open door for malicious actors in business areas assumed to be secure by organizational leaders. For example, multi-factor authentication and antivirus programs can only prevent successful phishing of user accounts when access rules are properly implemented. We have seen unfortunate situations where life sciences data was successfully stolen from a client's SharePoint instance due to these issues.

2. Operational downtime. Security breaches inevitably result in disruptions of services. Machines get taken offline to assess damage. User accounts get locked and password resets issued. Corporate data becomes inaccessible while systems are protected from further loss. The average time to detect and contain an attack is often more than 250 days, so businesses can be facing considerable periods of operational disruption when they occur.

3. Compliance concerns. Given the regulated nature of life sciences operations (e.g., FDA, GDPR, HIPAA), configuration errors and security breaches raise questions about the reliability, stability, and compliance of regulated systems. This issue is especially severe in areas related to authentication and authorization, as organizations may be unable to confidently attest to electronic actions, records, and audit trails.

4. Financial losses. When configuration problems lead to security breaches, organizations are faced with multiple monetary losses. Loss of revenue is obviously a top concern, but recovery costs can also be significant. The average cost of a data breach in the US is now over $9M. And if the breaches include legally protected or sensitive information, the organization could also face fines, civil penalties, and litigation costs as well.

5. Reputation damage. Almost half (46%) of breaches involve theft of customer data. As of 2023, public companies are now required by the US SEC to file a publicly accessible 8-K immediately after a cyber event. And business partner contracts increasingly require immediate disclosure of cybersecurity events. In short, the perception of any life sciences company's brand – by investors, physicians, patients, partners, and regulators – is seriously degraded when their operations and data are put in the hands of criminals.

Sources: IBM, CREO analysis

Strategies for Improvement

1. Leverage Available Best Practices

There are established security benchmarks, standards, and software tools – both open source and commercial – that are readily available to help life sciences organizations secure their environments. Three examples are below.

CIS Microsoft 365 Foundations Benchmark. This benchmark provides prescriptive guidance for establishing a secure configuration posture for Microsoft 365 Cloud offerings running on any OS. This benchmark accounts for the different MS license levels. More information can be found at https://www.cisecurity.org/benchmark/microsoft_365.

CISA ScubaGear. This tool is intended to help secure federal agencies' business application environments and protect federal information. However, the same framework applies to all organizations. It provides a formally packaged scanning tool with easy-to-digest reports that reference CISA Security Baselines (similar to CIS). More information can be found at https://github.com/cisagov/ScubaGear.

Microsoft Security Compliance Toolkit. Microsoft has made great improvements in providing the end user with the ability to scan their own configuration and provide detailed recommendations. There is a numeric "Security Score" that can be used to track progress towards a higher level of security. In addition, with appropriate licenses, other frameworks (e.g., CIS Microsoft 365 Foundations Benchmark) can be run as an "assessment". More information can be found at https://learn.microsoft.com/en-us/windows/security/.

2. Fix Low-Hanging Fruit

CREO's experience in protecting life sciences organizations from security vulnerabilities has shown that many organizations can benefit from easy-to-implement adjustments to their M365 configurations. The following table provides a few examples of enhancements that can improve your security posture.

Defender	• Sensitive accounts should be added to Exchange Online Protection in the strict preset security policy. • User impersonation protection should be enabled for sensitive accounts in both the standard and strict preset policies.
Entra ID	• Disable legacy authentication to limit phishing and brute-force attacks. • Secure MFA's second factor authentication methods such as email and SMS.
SharePoint	• External sharing should be restricted to approved external domains. • External sharing for OneDrive should be limited to existing guests or only people in your organization.
Teams	• Disallow anonymous users from starting meetings. • Unmanaged users should not be enabled to initiate contact with internal users.
Exchange	• Enable native malware scanning alongside 3rd party solutions. • Automatic forwarding to external domains should be disabled.

3. Make Risk-Based Decisions

Life sciences organizations are in a continuous state of change, with new people, products, partners, and IT systems evolving as organizations grow. Given that, periodic security scanning of corporate infrastructure should be mandatory to mitigate emerging risks.

As many organizations lack the time and skills to maintain mastery of this field, it can be helpful to engage a partner to periodically perform this function. A relatively large number of cybersecurity risks can be addressed with a limited number of improvements. The key is knowing the presence and severity of any active vulnerabilities.

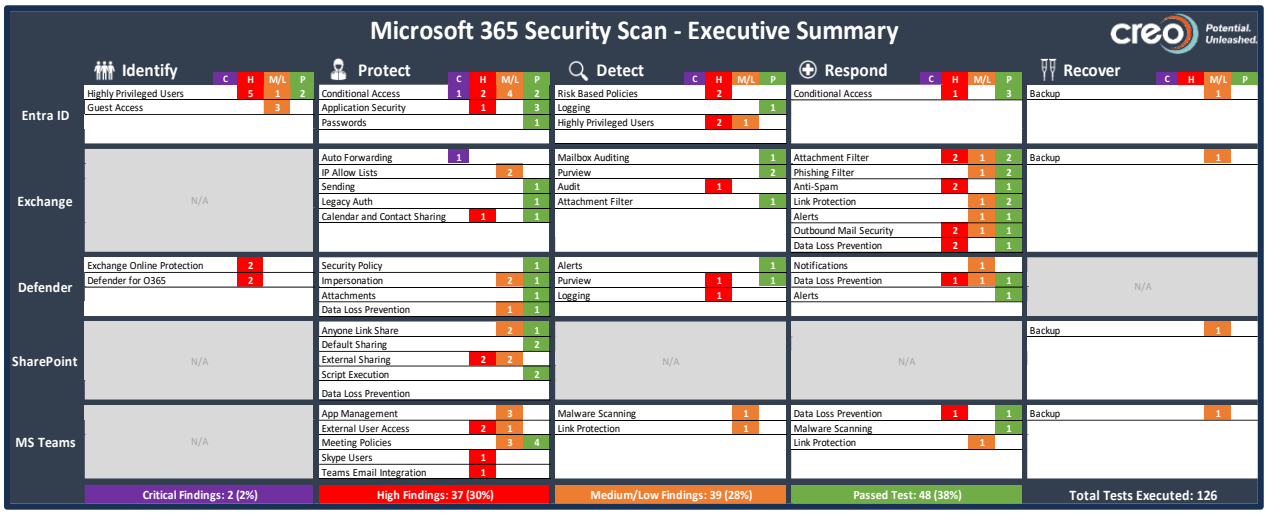


Figure 1. Sample output from CREO's periodic M365 Security Scan

When CREO conducts a M365 health check, we generate an exposure map (see figure) that quantifies the number of exposures and their relative severity across each product in the enterprise. These types of scans take very little time to conduct, and the findings are exceptionally valuable in closing gaps that leave the organization vulnerable. This risk-based approach enables remediation efforts to focus on the most important vulnerabilities.

Securing M365 is not a one-time effort. Organizations should invest in periodic scanning based on updated baseline configurations to confirm 1) any new features are properly controlled and 2) no settings have inadvertently been changed.

If your organization requires assistance with this effort, CREO offers both automated and manual review of your M365 configurations. These can be conducted within just a few days, so please reach out for a discussion.

Ready to get secure?

Schedule a call with one of our life sciences security experts, so that we can:

- Learn more about your company's security needs
- Discuss best practices for developing fit-for-purpose security strategies that grow with your company
- Share case studies of other life sciences organizations that have leveraged our services to decrease their security risks and strengthen their operations

About the Author

Dennis DeWolf is Senior Manager for cybersecurity and technical operations at CREO.