avanade

Creating a secure workplace in the life sciences ecosystem

Prevent cyberattacks with zero trust security model

Do what matters

Paradigm Shift: Moving from assuming trust to proving trust

Cyber attackers are constantly evolving and as life sciences organizations become increasingly connected and digitized it is becoming critically important to **secure the workplace in the life sciences ecosystem.**

Security models used within the workplace for life sciences organizations must assume that there has been compromise somewhere in the system and adopt a defensive posture against it.

Life sciences organizations need to move away from trust-based models that used to work before a digital workplace emerged and instead adopt a zero-trust security model.

85% of respondents said their organizations had allocated a moderate or, in some cases, a significant year-over-year increase in budget for Zero Trust initiative.

Zero trust security is based on **five fundamental pillars, users, networks, devices, applications, and data,** supported by a strong foundation of automation and analytics to enable it to scale.

Forrester describes zero trust simply as **"a model for information security that denies access to applications and data by default"** and that implementing it requires more than a model, it needs a change in mindset.

Building a zero-trust security model for a digital workplace

1. Users

Know who has access to your systems

Automated processes to prevent unauthorized or unknown users from gaining access must be in place.

Multi-factor authentication (MFA)

For connected life sciences ecosystem service providers, additional identity confirmation should be used. Low friction mechanisms such as fingerprint, pin codes or one-time passwords are acceptable methods of providing multi-factor authentication without impacting the user experience.

Centralized role based access control (RBAC)

Each individual identity must be associated with a user group relevant to their role. Each identity in a user group derives their access rights from that group If their role changes and they require different access rights, they must be moved to a user group with the appropriate access rights.

2. Networks

Control who and what can connect

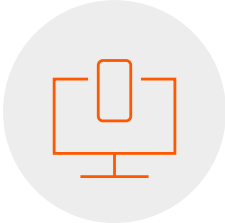
Controlling who and what can connect your internal networks is of paramount importance.

Internal network segmentation

Additional network defenses can be realized through internal network segmentation, which means that rather than having a flat network topology, your network is segregated into access-controlled subnetworks with predefined and automated access rules.

Access rights by role

Each individual identity must be associated with a user group relevant to their role. Each identity in a user group derives their access rights from that group. If their role changes and they require different access rights, they must be moved to a user group with the appropriate access rights.



3. Devices

Establish automatic enforceable rules

Establish automatic enforceable rules to strengthen ecosystem security and lower costs to maintain.

Devices with valid, authenticated identities

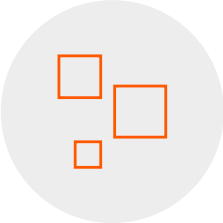
Only devices with valid and authenticated identities can connect to your systems. Use high entropy identification mechanisms so that if the identity of one device becomes known, the identities of other devices cannot be easily guessed.

BYO device security

Adapt mobile device security policies to accommodate ‘bring your own’ BYO devices so that employees can use their own mobile devices to connect to company networks and use them for work activities. Integration of BYO devices must ensure that only company-approved applications can access corporate resources.

With the average cost of a data breach in the pharmaceutical industry surpassing $10 million in 2022, it has become the highest costly data breach across all industries and sectors.

Building a zero-trust security model for a digital workplace



4. Applications

Allow only approved applications

Control access to information and systems by only allowing approved applications to be used.

Controlled access to networks and information systems

Access to your networks and information systems must be controlled by automatically preventing access if the application is: (a) not approved or authorized by your information technology department; (b) does not have a valid, approved signature; (c) is not the most current, approved version; (d) is running on an unrecognized/ unauthorized device.

Minimal user set up

The applications should require minimal user set up to enable them to perform their role and should be developed using a secure software development lifecycle and b e penetration tested to ensure that all interfaces are secure. It is also important to adopt the principles of data minimization by not collecting or storing non-essential information.

5. Data

Ensure sensitive data is protected

Data is the most critical asset. Strong data governance isrequired to ensure that all sensitive data is adequately protected.

Data protection in motion and at rest

Appropriate encryption methods are used to protect data in motion and at rest. Automated access monitoring and logging is used to detect, report and prevent anomalous data access/use. Regular testing of backup and restore mechanisms takes place to ensure their effectiveness.

Governance around protecting data

All sensitive data is identified and automated rules are in place to restrict its access and use. Sensitive data should be protected by additional authentication mechanisms, and anonymization and pseudonymization technologies used to protect personal health information and other sensitive personal information.

At Avanade, we're proud to have been recognized as Zero Trust champion at the Microsoft Security Excellence awards in 2022, for helping clients accelerate their zero-trust journey.

Two times winner of the Zero Trust Champion Award

Zero Trust assessment and high-level definition of the target architecture based on Zero Trust principles.

A leading medical product manufacturer wanted to embark on a Zero Trust journey but had limited visibility into the maturity and how the current infrastructure will support the Zero Trust approach.

Through a series of deep dive workshops, Avanade worked collaboratively with the organization's subject matter experts to assess the maturity of the IT infrastructure.

Avanade developed high level Zero Trust architecture and an individual client project roadmap based on the assessment results and on future state hypothesis and aligned it with the organization's special market experts.

Considering the organization's current IT investments, we developed a prioritized set of recommendations to embark on the Zero Trust journey.

Avanade can help you enhance the current and future state of your cybersecurity tools, technologies and adoption.

Where to start?

1. The first step is a Zero Trust assessment. This provides a holistic evaluation of your security posture and uncovers key risks, compliance and regulatory requirements as well as advice on how to prioritize these with a roadmap.

2. Disparate and redundant applications may be exposing you to greater security risks. We can help you to optimize your Microsoft licensing mix and align your technology strategy with Microsoft's solutions to simplify your security landscape.

3. If like many life sciences companies, you are not getting the best value from security tools you already have, we can help extend your Microsoft Security solutions utilizing automation and intelligence to protect your information, detect and respond to threats.

4. We know that staying ahead of emerging threats can be extremely challenging. We provide effective security monitoring at scale with Managed Security Services that combines top security talent with innovative technology.

Avanade is the leading Microsoft Security Services partner

Avanade is a recognized leader in delivering Microsoft solutions to health and life sciences organizations. We bring together advisory, technology and experiences within Avanade combined with industry understanding and expertise.

We have advanced Microsoft security specializations in cloud security, identity and access management, information protection and governance and threat protection.

For more than 20 years, we have worked with organizations worldwide developing and implementing solutions. In fact, 90% of life sciences companies in the Fortune 500 are our clients.

Contact Avanade

North America
Seattle
Phone +1 206 239 5600
America@avanade.com

South America
Sao Paulo
AvanadeBrasil@avanade.com

Asia-Pacific
Australia
Phone +61 2 9005 5900
AsiaPac@avanade.com

Europe
London
Phone +44 0 20 7025 1000
Europe@avanade.com

About Avanade
Avanade is the leading provider of innovative digital, cloud and advisory services, industry solutions and design-led experiences across the Microsoft ecosystem. Every day, our 60,000 professionals in 26 countries make a genuine human impact for our clients, their employees and their customers. Avanade was founded in 2000 by Accenture LLP and Microsoft Corporation. Learn more at www.avanade.com.

avanade

Do what matters