WORKPLACE EXPERIENCE

avanade

CIO Guide: Five essentials of a secure modern workplace

Unleash productivity, while minimizing the risk

Transforming the workplace experience, securely

Modernizing the workplace comes with a new set of security challenges. Your employees need anywhere, anytime access to their data, across devices and environments. Meanwhile, security teams face more complex and sophisticated threats. Even the most innovative solutions can fall apart without the right security strategies.

Simply put: CIOs and digital leaders must modernize the workplace, without sacrificing security. Rigorous security solutions are needed. But those same strategies cannot be implemented in a way that hampers the realization of a more collaborative, innovative workplace.

The good news: You can strike this balance by following a holistic, cyclical approach to modern workplace security. By leveraging the five essentials outlined in this guide, you can help to deliver the culture, tools and operational environment you need to transform the workplace experience, with confidence.

avanade

Workplace experience drives business success

Recent research from the MIT's Center for Information Systems Research (CISR) shows that companies with the best employee experiences see dramatic business benefits. The top quartile performers in employee experience saw these gains:

Double the customer satisfaction (industry adjusted Net Promoter Score, NPS)

Twice the innovation in terms of percentage of revenues from new products and services

25% greater profitability compared to competitors

Source: "Building business value with employee experience," Kristine Dery and Ina M. Sebastian, MIT Sloan Center of Information Systems Research (CISR), Research Briefing, Volume XVII, Number 6, June 2017

01 Focus on culture

02 Understand exposure

03 Simplify landscape

04 Implement wisely

05 Leverage intelligence

Keeping your workplace secure is a fluid, ongoing process

Why Avanade?

About Avanade Security Services

01 Foster a strong security culture, everywhere

A security culture is fundamental to a successful modern workplace. Without it, your end users expose your organization to undue risk. Think falling for phishing scams or plugging in unencrypted USBs; the possibilities for human error are endless. Not only that, but your IT teams will be under-prepared in the event of a breach. All of which can be catastrophic.

With the right security culture, though, your employees can be your greatest asset. As CIO, your job is to help build up a security mindset and behaviors across the organization, as you move to modern platforms. Doing so demands collaboration, ongoing attention and an innate understanding of the human-risk factor:

User-centric security: Design workplace solutions with the needs and real-life experiences of end-users in mind – reducing friction and improving adoption of new, secure technology. IT moves past traditional ideas of perimeter-based security and builds solutions for people to work productively.

Awareness and education: Risk-avoidance programs, such as internal phishing campaigns or warning against using unencrypted USB drives, incentivize safer behaviors (and stigmatize the risky ones).

Preparedness and training: From "secure by design" methodologies, to incident response training, IT and operations must also embrace holistic and real-time security practices. With SecDevOps, for example, business apps are designed with security in mind from day one.

With a strong security culture in place, your workplace can thrive. Employees will naturally adopt new, safer solutions, with ease. Education and awareness will prevent unnecessary mistakes and human error. And IT can react quickly and confidently to breaches, minimizing damages and protecting your brand.

33%

of employees receive no cybersecurity training at work – Eset

02 Clearly map out your exposure, today

You need to know where you are today, to understand where to go next. Without an objective view of existing vulnerabilities, you will struggle to move to modern platforms, securely. You also risk layering on expensive point solutions without addressing underlying issues.

Clearly mapping out your existing security landscape, before moving forward, is essential. To gain a full view of your security maturity level, you will work across departments to assemble a complete, objective-driven picture of your current state:

Map your footprint: Map out the consumption and usage of existing workloads and vulnerabilities, including endpoints and mobile devices, as well as compliance and upgrade requirements.

Application rationalization: Determine which applications are ready to move to the cloud as is, and which ones require updates or total replacement to remain compliant and reduce risk.

Shared responsibility: Work with cloud providers to understand where your responsibilities begin and end, to effectively protect applications and data.

Consider this a fact-finding phase. With objective, data-driven insights, you will start to understand exactly where your risks lie. You will gain clarity about your current compliance needs and how your security policies need to evolve for a future state. Simply put, you will understand what actions are needed to keep your organization safe, as it evolves.

Cybercrime will cost the world $6 trillion annually by 2021
– CyberSecurity Ventures

03 Simplify the security landscape

Don't make the mistake of piling on numerous, disconnected security solutions as you modernize your platforms. Doing so results in overlapping and redundant solutions, limiting visibility and control.

Simplicity is the best remedy. As you pursue workplace modernization, you will aim to reduce the complexity of your security solutions and boost your visibility. This stage calls on you to:

Reduce your footprint: Identify the most optimal way to plug the gaps and securely manage your future state, while reducing the total number of solutions.

Improve insight and control: Unify visibility and controls across cloud and on-premises environments.

Cut waste: Find opportunities to cut waste and needless third-party tools, by fully leveraging the built-in capabilities of modern workplace platforms, such as enterprise mobility security tools included in Microsoft 365.

A simplified approach to securing the workplace has enormous impact across the organization. Not only does it unlock more control and visibility, it eliminates unnecessary costs.

The average enterprise has over 80 security solutions to manage – HelpNetSecurity

04 Implement wisely

It's not just what you do. It's how you do it. In fact, misconfiguration is one of the most pressing security challenges for CIOs pursuing a modern workplace. You risk doing too little – and maintaining legacy risks. Or doing too much, overwhelming users with too much change all at once.

As CIO, your mission is to lead a measured, strategic implementation. One that is aligned to business priorities and operational realities. This "crawl, walk, run" approach will be unique to your environment and requires the following:

Low-hanging fruit: Prioritize capabilities and applications that deliver results, without requiring a major overhaul from day one, in the way work gets done.

Minimal effective policies: Turn on only the policies and controls needed to meet data and compliance requirements, while ensuring the desired productivity and collaboration.

Targeted rollout: Begin with a proof of concept on a specific, feasible workload, geography or user group. Or, drip out deployment of modern security policies, such as multi factor authentication and password reset policies.

Change management: Help drive adoption and new, secure behaviors by educating users on why the change is happening and how it aligns to larger business outcomes.

When done correctly, a modern workplace will be implemented in a way that eases employees into a new way of doing work, without overburdening IT with endless support calls. You only have one shot to get the implementation right, so take your time and plan accordingly.

Only

50%

organizations have basic security practices in place, such as password rules and multifactor authentication.

And just

33%

are using single sign-on to secure and simplify user access.

Avanade Trendlines, "Keeping pace with emerging technologies," 2019

05 Get smart, stay smart

Staying secure is not a static undertaking. As employees evolve, so do the threats and capabilities of bad actors.

To stay ahead of the curve, your job is to help IT and users embrace emerging technologies, and the full, built-in capabilities of modern platforms. Here, you will leverage real-time intelligence and inspire IT operations to adopt a risk-based approach to ongoing security management.

Analytics and intelligence: Leverage analytics and globally sourced intelligence to spot trends and prevent threats before they make their way into your environment, or to remediate without delay.

Embrace evergreen: Tap evergreen, automatic features of cloud platforms to seamlessly update, patch vulnerabilities and identify breaches, across endpoints and environments.

Focus on innovation: With less manual time needed on maintenance, ask your IT team to focus on innovation, support and productivity.

Foster excellence: Establish a Cybersecurity Operations Center or Center of Excellence, to maintain, scale and sharpen your workplace security know-how over time.

Even the most advanced security solutions turn obsolete without the proper care. Automation, analytics and intelligence help drive advanced threat protection, prevent data loss and ultimately support a more innovative, productive workplace, into the future.

Only

52%

of executives believe that new security technologies are keeping ahead of new security threats.

Avanade Trendlines, "Keeping pace with emerging technologies," 2019

avanade

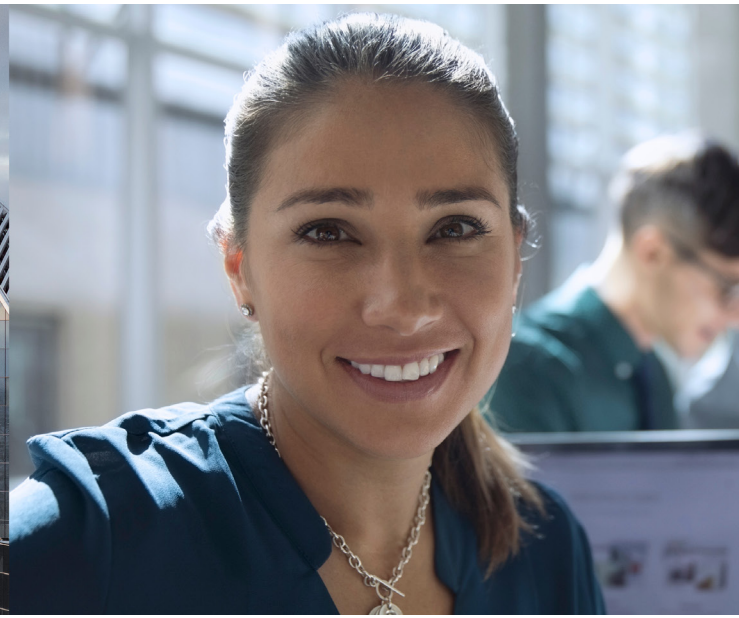
Keeping your workplace secure is a fluid, ongoing process

In this guide, we have outlined the five essentials that are the components of a fluid, cyclical process to help you transform the workplace experience. One that continues as your workplace evolves.

To secure the modern workplace, you must begin at the root: culture. A strong, balanced security culture ensures both users and IT are empowered to maintain a posture of cyber-resilience and compliance. Next, you must identify your existing vulnerabilities to map out a simplified, efficient security roadmap.

Only then can you implement and configure workplace platforms wisely, taking into account the needs of busy employees and administrators. Here you will balance data risk with the required usability goals of the new workplace, in a methodical approach. Once there, you can take full advantage of emerging technologies, automating, optimizing and bringing more intelligence into your workplace platforms.

Visit www.avanade.com/security to find out more.



Avanade's Secure Workplace solution

Avanade helps design and maintain a robust security posture, modernize applications with an evergreen platform and create a thriving security culture across the organization.

Our holistic solution spans:

- Identity and access management
- Information protection
- Threat protection
- Security management

From start to finish, our unparalleled Microsoft 365 and Azure expertise and certified partnerships – with Symantec, Tanium, CyberArk, Okta, SailPoint and many others – help you build and secure your modern workplace.

Learn more about our Secure Workplace solutions

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 and cloud services, business solutions and design-led experiences on the Microsoft ecosystem. Our professionals bring bold, fresh thinking combined with technology, business and industry expertise to help make a human impact on our clients, their customers and their employees. We are the power behind the Accenture Microsoft Business Group which combines the skills of 45,000 professionals around the world, helping companies to engage customers, empower employees, optimize operations and transform products, leveraging the Microsoft platform. Avanade has offices in 24 countries, bringing clients our best thinking through a collaborative culture that honors diversity and reflects the communities in which we operate. Majority owned by Accenture, Avanade was founded in 2000 by Accenture LLP and Microsoft Corporation. Learn more at www.avanade.com

© 2019 Avanade Inc. All rights reserved. The Avanade name and logo are registered trademarks in the U.S. and other countries. Other brand and product names are trademarks of their respective owners.

avanade