Rethink your cybersecurity strategy for the new world

5 steps to secure the enterprise and be fit for a flexible future

avanade

Rethink your cybersecurity strategy for the new world

The COVID-19 pandemic has affected every industry, organization and person. What we buy, how we live and the way we work has **changed forever**, and faster than we could have imagined.

Many organizations have had to implement new, unfamiliar operating models and quickly deploy technologies that support this new environment to ensure business continuity.

Organizations are rethinking their way forward. To do this, we encourage you to focus on these key priorities: cost containment, empowering your employees, protecting the core operations of your business, supporting the needs of your customers and responding to changes that affect your product portfolio. Building a secure and resilient operation is essential to driving these priorities.

Recent shifts such as increased remote working, mean that organizations are facing greater security challenges, with a broader attack surface and greater exposure to threats. For many, their risk posture has fundamentally altered. Now is an ideal time to rethink your security strategy. In this guide, we outline key steps to help you do this – so you can protect the core operations of your business and enable your employees to work securely in this new environment.

Attackers are **exploiting** the increased exposure and according to new research from **Microsoft**, hackers have launched coronavirus-themed cyberattacks in **241 countries** and **territories**

"... we see these challenging times as an opportunity to rethink how we do business ...This will include transforming your company to have an even better customer experience and more efficient operations."

MIT Sloan Center for Information Systems Research
March 31, 2020

Global disruption **exacerbates** security challenges

In this new era, organizations are **grappling** with several security challenges:

Social engineering

Attackers are capitalizing on fears around the crisis and are using COVID-19-themed lures to deliver phishing campaigns and malware. These types of attacks have seen a sharp spike, and this is likely to continue.

Remote workforce

As the remote workforce has increased, so have the risks around securing personal devices, weak passwords, poorly secured home Wi-Fi, routers and patching remote systems. Employees are also collaborating in different ways inside and outside the organization, often using susceptible platforms.

This has opened up vulnerabilities in collaboration tools that can be exploited, resulting in a poor user experience and concerns about privacy and confidentiality. Security leaders also face increased IT costs to support the workforce, with higher network and infrastructure use.

Lack of secure access

Identity and access governance methods have not kept up with new ways of working, including remote workers, multiple devices and the inability to access key applications. The amount of data that's being shared has also multiplied and, as a result, many organizations are asking if they have the right identity infrastructure and governance that gives their employees secure access to the information they need. Remote workforces and remote business models will become the new standard. Goods and services will be exchanged digitally via the API economy, further increasing the potential attack surface and associated risks.

Lack of agility

The unprecedented demand for accessing company resources remotely has put extra pressure on access points and virtual private network (VPN) services. Many organizations have been unable to securely scale existing systems and VPN infrastructure to meet evolving requirements, affecting the user experience and ability to work.

> **Microsoft** is tracking around **60,000** COVID-19-related **malicious** attachments or URLs daily

Navigate through the waves of change

We anticipate that organizations will go through **three waves of change**. It is imperative that you start to take the right steps now, to **protect** the core operations of your business, so that you can build a **resilient** and **scalable** operation that's fit for a flexible future.

Respond

Many organizations are beginning to emerge from this first phase. During this time, organizations have been focused on ensuring business continuity by enabling employees to work, clients to access goods and services while maintaining their core operations and supply chain.

With a shift to a remote workforce, it is important to understand how your organization's risk posture has changed.

Reset

Already we are seeing many of our clients move beyond the respond phase to adopt a reset mindset, to manage through an economic slowdown as a lighter-weight and more agile business. This is likely to involve reconfiguring the product portfolio and the rapid creation of a scalable operating model to support changing market and employee needs.

During this phase, we recommend that you undertake a comprehensive risk assessment, to prioritize how to address identified security risks, starting with the most immediate security gaps. In addition to this, you will need to plan for a security framework based on zero-trust architectures and cost reduction.

Renew

Over the course of the coming 12-18 months, we expect organizations will increasingly shift their attention to how they can renew and position themselves for the future. They will be looking to reinvent their business model to address existing and new opportunities with a stronger, more resilient version of the enterprise.

From a security perspective, you should look to continually adapt to changing business landscapes and remain compliant, ensuring any changes in models, technology and processes adhere to regulatory and emerging compliance requirements. This would also be an ideal time to implement a new security design, based on a robust roadmap that is consistent with your business requirements and risk posture.

5 steps to **rethink** your security strategy

As you go through these three phases, it can be hard to know where to begin to ensure you're taking the necessary actions to secure your enterprise now and in the future.

We outline five steps to help you get started.

#1. Adopt a **zero-trust** mindset and vision

This concept is centered on the belief that an organization should not automatically trust anything inside or outside its perimeters – and that everything must be verified before granting access to systems. The identity of every individual, admin account, application, bot, and process must be validated and managed through a governance process.

We also recommend that you consider tools that address your identity governance and administration (IGA) requirements. Access to digital services from different locations and target platforms should be continually evaluated to support business resilience and continuity objectives.

Case Study

Stellar security unlocks full workplace potential

Challenge: Our client wanted to construct a future-ready digital workplace and introduce a state-of-the-art employee experience, with a secure foundation.

Solution: We implemented a Microsoft 365-powered secure modern workplace, which featured a wide range of solutions, from secure cloud services through, to a mobile workplace and best-of-breed collaboration.

Results: The organization is now seeing compelling business results from the project:

- Two key **security** principles – "Identity as control plane" and "zero trust" – are fully supported.
- Employees are more **productive** and can leverage the same workplace experience across various devices remotely and securely.
- Secure evergreen workplace platforms have helped the client achieve a faster time to market and IT delivery **efficiency**.
- The **employee experience** has greatly improved, with enhanced collaboration and the ability to make better business decisions.

#2. Undertake a comprehensive **risk assessment**

If, like many organizations, you've recently experienced a **rapid change** to your enterprise architecture and the deployment of new collaboration and workforce tools, now is the time to conduct a risk assessment of your environment.

It's hard to evaluate the risk of everything from the outset, so a good place to start is by identifying the assets of most value and understanding what you want to protect. From here, you'll be able to pinpoint the key risks to those assets and come up with a tactical plan to address them.

#3. **Prioritize** security projects, budgets and resources

Understanding the risks to your newly altered ecosystem will allow you to take a **measured** and **thoughtful** approach to security project prioritization, resources and budget.

This is also a good time to review, or develop, a formal security governance framework to ensure that your new operating model is consistent with your new risk posture.

Like most things, security can't be solved by throwing money at the problem. A risk-based approach will help you focus your budget and resources. Many of our clients are now prioritizing their security spend on digital transformation and cloud migration projects to support a remote workforce.

IDC recently reported that it expected spending on security-related professional and managed services to remain strong as organizations attempt to keep operations running during the COVID-19 crisis. This highlights the importance of security as a strategic priority to organizations relative to other areas of IT.

> IDC believes COVID-19 will help to highlight the importance of having **incident response** and **resiliency** plans in place for crisis situations

Impact of COVID-19 on IDC's Projections of Security Services Spend
April 13, 2020

#4. **Simplify** and **enhance** your security landscape

A layered approach to security with the right tools is essential; but look for **opportunities** to cut unneeded controls.

Excessively heterogenous security architectures are difficult to manage, costly and may increase your risk of exposure, so look to leverage any capabilities that are integrated into your cloud provider's platform.

This is especially useful when you need to react quickly to a situation such as enabling a remote workforce. Ensure you're fully leveraging built-in security capabilities, such as those included in Microsoft 365, which will help to reduce unnecessary costs.

#5. **Renew** to realize your security vision over the long term

We recommend that you implement a **holistic** approach to security and make it a part of your organization's digital transformation from the outset.

Build security into the IT solutions and applications, rather than trying to address with the latest cybertech solution, which may soon become redundant.

Whatever systems you put in place, make sure they're secure from a cloud and modern applications standpoint and that you have a good understanding of the level of responsibility the provider (and you) will bear, to make it secure by design.

Security should be a business enabler, so try to balance security and controls to avoid adding barriers and adversely affecting employee productivity. This will allow your organization to operate in an agile way and prepare for whatever comes next.

Make building a strong security culture a priority. Comprehensive, consistent training and education will help you address the security risks inherent with employee behavior. This may require a change management approach backed by ongoing education and role-based training for individuals.

Why **Avanade**?

Leading in today's marketplace demands **outside-in** thinking

At Avanade, we have been actively helping our clients during this difficult time. Since the outbreak of the COVID-19 pandemic, we have migrated over **1 million remote working accounts** for our clients. We are now helping to guide these organizations to a new secure operating model, that is built to adapt and protect them in the future. We're the experts at helping you secure your Microsoft and hybrid IT ecosystems.

Our security services provide a holistic approach through advisory, implementation and managed services. We can help you perform a **risk assessment** and implement a **secure architecture**. As a managed security provider, we can also **augment** your security team and provide the 24/7 monitoring of events and ongoing **operational support** to help you stay ahead of security risks.

We provide proven methodologies, deep expertise and leading-edge technology, and we've been the Microsoft Alliance SI Partner of the Year for 14 years.

AVANADE
IS GOLD FOR
MICROSOFT'S
SECURITY
COMPETENCY

MICROSOFT SECURITY 20/20
SECURITY
ADVISORY
OF THE YEAR
WINNER

MICROSOFT
PARTNER FOR
OFFICE 365
FOR TEN
CONSECUTIVE YEARS

MICROSOFT
ALLIANCE
PARTNER
OF THE YEAR
FOR 14 YEARS

avanade

Get started **today**

If like many of our clients you have had to **rapidly scale** remote working, a good place to start is our security assessment and workshop.

We will work with you to understand your business drivers, existing infrastructure and processes to come up with a holistic assessment of your security landscape and create a roadmap, to help you realize your security vision over the long term.

We offer the following:

Microsoft 365 Security Assessment and Workshop

- We assess your current Microsoft 365 environment from a security perspective to identify gaps and remediation areas.
- We provide a comprehensive analysis and roadmap based on your organization's security controls and business requirements.
- A Secure Score report and dashboard provide details on data protection and governance.
- A holistic assessment provides guidance on mitigating evolving cybersecurity risks.

Identity Infrastructure and Process Assessment

- We provide a comprehensive assessment and automated discovery of risks.
- We evaluate your infrastructure to recommend improvements.

Contact us to learn more or visit **avanade.com/security**

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. With 38,000 professionals in 25 countries, we are the power behind the Accenture Microsoft Business Group, helping companies to engage customers, empower employees, optimize operations and transform products, leveraging the Microsoft platform. Majority owned by Accenture, Avanade was founded in 2000 by Accenture LLP and Microsoft Corporation. Learn more at www.avanade.com.

avanade

avanade