# Securing Remote Work for Whatever Comes Next

An expert security perspective from Fujitsu

The workplace has changed, driven by technology adoption, shifting consumer preferences, and operational considerations – especially in light of COVID-19. In particular, more business processes are becoming digital and more staff are working remotely from widely distributed locations.

These factors make application, data, and device security more complex. Employees need easy access to applications and data from new devices and locations, leaving IT to respond with stronger tools and methods for managing an increasingly complex security landscape.

In this interview, **Fujitsu Distinguished Engineer Andy Baines** shares his insights on how IT can create a security foundation that will unleash employee productivity and business agility while also mitigating data security risks.

## Securing an Adaptive Workplace

**Q: How do you define an adaptive workplace from the perspective of security? Is it just the ability for employees to safely work remotely?**

**A:** An adaptive workplace is about providing users with the ability to work in an agile and secure way irrespective of where they're actually working from. It's about taking a holistic view from a security perspective and enabling appropriate levels of protection, while not hindering productivity. An adaptive workplace provides a flexible and user-centric experience but at the same time can introduce new security risks. It is therefore important that these risks are understood and controls applied to the adaptive workplace environment to mitigate them.

**Q: How have businesses needed to adapt their security measures in response to COVID-19?**

**A:** Most organizations today have a virtual private network (VPN) capability for secure connection to a corporate environment, but not every organization is geared up to allow most of the workforce to connect that way. So, in order to support more remote working as a result of COVID-19, we saw a big increase in customers asking us to help them increase VPN capacity and keeping it secure by adding techniques such as multifactor authentication. Vulnerability scanning and management was another area where customers wanted assurance that their infrastructure was secure and that they were aware of vulnerabilities and had plans in place to address them.

We have also seen an increase in phishing emails that incorporate the COVID-19 theme and some of these attacks are particularly sophisticated, so it's important to remind users of what to look out for and where to get advice and assistance. And to enhance data loss prevention, we have used technology to proactively alert users about behavior that could lead to an inadvertent release of sensitive information.

**Q: What security considerations are important for VPN?**

**A:** The VPN provides an encrypted connection to the corporate environment, but you also need to make sure the user is who you believe them to be. So measures like multifactor authentication and making sure the user's device is secure are important. Techniques to assess the security posture of remotely connecting devices helps ensure that backdoors are not opened which could allow breaches in security. Additionally, the use of virtualized desktops in conjunction with secure remote access can add to the protection provided to mobile users, particularly those not using corporate devices. The centralized security configuration of virtualized systems in conjunction with OS regeneration helps to reduce the likelihood of a security incident.

**Q: Can businesses use other controls to improve data security?**

**A:** A massive challenge for some organizations is knowing where their sensitive data is stored, not just within the corporate environment but also on personal and corporate cloud storage, so tools for data discovery, classification, and labeling are a big help. Security features can apply appropriate controls based on the data's classification, such as requiring the user to obtain approval before sharing or using encryption to protect the data.

## A Focus on Endpoint Security

**Q: Many organizations have allowed personal devices (BYOD) as a way to quickly enable employees to work remotely. What security concerns does this raise and how can advanced security solutions address them?**

**A:** Key concerns are how to avoid users storing corporate data on their own devices and also how to allow non-corporate devices, which may have unpatched vulnerabilities or which may have already been compromised, to connect to the corporate network. With cloud storage, you can enforce a policy that users store data within the corporate cloud environment instead of on a personal device. Compliance management tools can be used to make sure basic security controls are configured on a user's device before it can access the corporate network.

**Q: What changes are you seeing today in how organizations are choosing security solutions, especially for endpoint management?**

**A:** Historically, customers didn't want to get all security solutions from a single vendor, but I think that mindset is changing. Organizations are expecting more from their endpoint security solutions particularly with a focus on improved detection and forensic capabilities. Integration of security solutions allowing them to share data allows for higher levels of threat detection and prevention. Today, customers are looking for the simplified management of a single solution and a partnership of trust and confidence in the vendor.

## Preparing for What May Come Next

**Q: What are future challenges around an adaptive workplace and data security that IT can prepare for now?**

**A:** Employees won't be working from home forever, but there will still be a big shift in allowing people to work in more flexible ways. Employees will want to achieve more through remote connections and use of cloud services, so the security model must support this.

Overall, security is an ongoing challenge and you need to look at it as a continuous journey. Business needs will change even more quickly, so you can't wait for a 12-18-month implementation project. You'll want to work with vendors who can provide agile delivery of new security solutions and features which keep pace with the ever changing risk environment.

## Maximizing Protections with Today's Security Technologies

**Q: What is the role and value of Microsoft 365 features in a customer's security program?**

**A:** Microsoft has an active program for continuously introducing and integrating new security features which improve the overall security posture of Microsoft 365. These new features help improve security visibility and control thereby supporting a move to proactive security management. Fujitsu helps customers understand how to map these Microsoft 365 capabilities to business requirements, resulting in security controls which are specifically configured to an individual customers requirements. Additionally, Microsoft 365 provides considerable amounts of valuable security specific information which needs to be analyzed and dealt with. Fujitsu uses orchestration and automation to turn this security data lake into actionable information which can then be dealt with by the customers or Fujitsu's security team. The scope of all Microsoft 365 capabilities and pace of change can be challenging to implement and manage, so businesses look to outsource the complete solution to a provider like Fujitsu.

---

### About Andy Baines

Andy Baines is the Chief Security Architect for Fujitsu UK and Ireland. Working within the Enterprise and Cyber Security Product Management group, he is primarily responsible for Fujitsu's Microsoft 365 security portfolio. A Fujitsu Distinguished Engineer, Andy has a great breadth of theoretical and practical experience.

### Security Solutions from Fujitsu

Fujitsu is a Microsoft Gold Azure Managed Service Provider (MSP) partner and works with customers to design, implement, and manage security solutions based on Microsoft technologies. Fujitsu's security services ensure business continuity 24/7, while mitigating threats using the latest cyber intelligence.

### About Microsoft

Microsoft (Nasdaq "MSFT" @microsoft) enables digital transformation for the era of an intelligent cloud and an intelligent edge. Its mission is to empower every person and every organization on the planet to achieve more. **www.microsoft.com**

**Learn how Fujitsu can help your business gain value from advanced security services and Microsoft solutions at fujitsu.com/global/themes/security**