

WORKSPACE

changing perception from within

MODERN WORKPLACE

# INTO THE ERA OF SECURE REMOTE WORK

A business guide to cloud security  
for the new remote workplace





# Business opportunities and security risks associated with the rapid shift to remote work

Something many small and medium-sized businesses have discovered during the rapid shift to remote everything: There's a lot to be gained by not relying on a physical space. It can save overhead, reduce travel expense and some studies have found it has increased worker productivity (one found a 13% performance boost among at-home workers).<sup>1</sup> As a result, many businesses are seriously considering tools and strategies to make the non-physical workplace a permanent part of their businesses.

To succeed, this transformation of physical businesses will require new structures and processes, especially for smaller businesses that were not used to working remotely. Regardless of size, all companies now need to think about securing remote endpoints and IT resources. Employees need to be more vigilant than ever. Cyberattackers have made it clear they're not taking any time off.

<sup>1</sup> "Remote Working: The New Normal?" Casey Rue, Forbes, May 20, 2020.

<sup>2</sup> "GCHQ calls on public to report coronavirus-related phishing emails," Alex Hern, The Guardian, April 20, 2020.

Many of us saw the additional security risks of the remote work explosion.

Video data breaches represent only the visible fraction of other, less flamboyant, but more costly threats enabled by the new scale of endpoint devices in use. Over just a single initial month of the crisis, the National Cyber Crime Security Centre detected:

- **555 malware distribution sites set up** to cause significant damage to visitors
- **200 phishing sites** seeking personal information such as passwords and credit card details
- **832 advance-fee frauds** where a large sum of money is promised in return for a set-up payment<sup>2</sup>

And that's only in the UK. Bad actors aren't taking time off, so you, your IT teams and end users all need to be ready now for the increased security risks in this new age.

# A two-part security challenge: Volume and security

---

Like so many other companies making the decision to shift to remote everything, your company's first challenge was how to ensure unimpeded performance for your remote workers who are trying to access their tools and data—or just find a reliable internet connection.

Following close on this first issue is the question of security. Suddenly it's the ultimate bring-your-own-device (BYOD) world. Every employee is now remote, and more focused on being productive than following your pesky security procedures. They'll access the data they need however they can; often bypassing VPNs to access cloud services or grabbing hotspots wherever they can—secured or not. This do-it-yourself attitude can lead to risky activities beyond your control, such as employees downloading software on their own.

With everyone using whatever devices are handy—personal phones, home computers, even kids' tablets (it has happened!)—the situation is especially perilous. One wrong click can instantly launch an attack that could jeopardise your entire business.

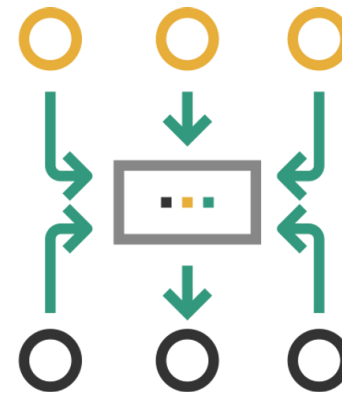
Given the limited capabilities of traditional perimeter firewall and VPN solutions to protect against these remote threats, companies need new security measures, new levels of expertise and new technologies to protect their assets. And the good news is you can build on current measures to get there.

# Time is not on your side: Get a handle on your security picture

If you haven't had time to perform basic endpoint hygiene and connectivity performance checks on your computers and devices, better late than never. In addition to confirming all your laptops have the necessary endpoint protection configurations for all this new off-LAN activity, ensure your employees are following recommended security practices by asking these three important questions:



**1. Have you reviewed and adjusted the security settings of your cloud tenant and your organisation's internal network?**



**2. Have you made sure the security settings and measures for remote users are appropriate for current and foreseeable levels of usage?**



**3. Are your team proficient in all of the latest security threats or do they need help?**



# Make remote workers the centre of attention

---

Remote workers are now the core of your productivity. The devices they work on can no longer exist at the edge of your security planning; they are dead centre and must be treated as such starting now. All that mixing and matching of personal devices with company equipment demands different practices and elevated controls. That means much more than the basic antivirus and antispyware protection, including multi-factor authentication (MFA) and onboard endpoint detection and response (EDR) capabilities.

Not only should your remote workers be aware of these new measures, but the tools and safeguards you use to attain and remain at a new level of endpoint and data security should meet those needs.

With the world rapidly—and permanently—changing, now is the time to enlist the help of a partner that has already worked out the best practices to face it. Without this critical help, you can't be sure each endpoint requesting access to internal resources meets security policy requirements. You need the right tools to track and enforce policy on all devices and with employees everywhere, while delivering easy user onboarding and offboarding.

**We can help.**

# Plot your strategic technology roadmap

---

## True security demands increased agility

Business success requires a combination of long-term strategic thinking with the agility to address challenges and new opportunities head on. Stridon can help you create a strategic technology roadmap that will support your vision and deliver your required business outcomes while keeping your business data secure and compliant in an ever-changing cyber threat landscape.

## Add the human element to cybersecurity

The Stridon team maintains the highest level of expertise in Microsoft security solutions. We hold the elite Microsoft Silver Partner certification. But technological expertise alone isn't enough. The only way to protect your singular business journey is through a deep understanding of your business needs, your mission and your culture. We take the time to align completely with your vision before making recommendations.



# Enhanced security responses for the new remote work environment

---

The decentralisation of the workplace makes endpoint security more critical than ever. And the new tactics used by malicious actors require focus on different tools and solutions. If your organisation uses Windows 10 or later, **odds are you already have access to the world-class antivirus and antimalware solution already built into the operating system**. You also probably have the cloud licence to activate the centralised management and greater capabilities of Microsoft Defender.

Microsoft Defender for Endpoint gives you unmatched breach remediation and research capabilities. With a graphical representation, this tool enables security teams to map the precise point at which an

attacker entered your network, how the attacker moved once inside and the activities they engaged in. It is one thing to remediate a network breach but having the rich details of exactly how the breach occurred enables you to make sure any vulnerabilities in the network are found and corrected to prevent future breaches.

Here are three ways we can help you immediately to leverage your current Microsoft Defender technologies to face security challenges now and in the future:

# Three ways to enhance security now

---

## 1. Phishing: Be the one that got away

Social engineering has always been a successful vector for malicious actors. But now with more employees working on their own, the bad guys have more targets of opportunity. With cloud providers hardening their security more than ever, phishing for credentials and spoofable material is becoming a path of least resistance. Once they have convinced a user to give up their sign-in information, hackers can accurately spoof the emails of internal users. The user receives an internal email, clicks on the link and that's it. The links lead to websites that look very real. For example, they might mimic the Microsoft Office 365 sign-in page. When a user enters credentials on this site to sign in, the bad actor then has access to your environment for further attacks.

Phishing is successful because even with the proper training, anyone can be fooled. So training must be regularly performed and reinforced through simulated activities—just like fire drills—to remind users to be sceptical of any email they receive.

If a single phishing attack gets through, it can cost your organisation hundreds of thousands of pounds and a reputation damaged beyond repair. Just look at the news in the last several years. For training that's unmatched, Attack Simulator for Office 365 uses the Microsoft Intelligent Security Graph. It's constantly learning from global signals received from one of the largest telemetry systems on the planet. For example, Microsoft Office 365 scans 400 billion emails every month and finds a large number of malicious spear-phishing emails. The Attack Simulator carefully crafts simulated spear-phishing emails based on this real data, ensuring the most realistic attack experience for your user population. It then tracks and reports on user responses to the simulated email security events, providing invaluable data on how to better secure the organisation.



# Three ways to enhance security now (continued)

---

## 2. Watch out for well-intentioned 'shadow IT'

As we've said, the new remote world of work is full of bright end users. They're bound to think they have better tools than those your IT department authorises. And they will use them. Sometimes a tool can go internally viral, becoming the app-of-choice before IT can stop it, or even become aware of its existence. Though your users see these as smart and cool new solutions, and see themselves as taking initiative to deploy them, they're dangerous to your data security and can obviously become the source of network breaches. We can help you through our managed security service to continuously monitor for these unsanctioned applications and the 'shadow IT' they engender.

## 3. Keep your defences strong

We can help. Your known tools can help protect you from unknown new threats—if you know how to use them. Our team of security experts will help ensure that your company's critical data protection is innovative enough to stay ahead of the threat environment with tactics that include:

- Security alert monitoring of Office 365 with Security Score
- Baiting and trapping of threats using honey pots
- Setup of antivirus active threat monitoring and mitigation
- App installation monitoring to prevent 'shadow IT' behaviours with Device Guard
- User data classification setup
- Simulations of email phishing attacks raising awareness
- Simulated password spray and brute force password attacks to better secure credentials

## Case Study:

# Getting out in front of a pandemic

## Wedlake Bell

### Company

Wedlake Bell LLP is a London-based law firm with 70 partners supported by over 170 lawyers and support staff. Their model is based on four practice areas: private client, business services, real estate and dispute resolution.

### Challenge

Wedlake Bell's vision was to completely modernise how they worked internally and with clients through technology. Their new approach meant rethinking everything from the design of their new offices, how they collaborated, and how they delivered legal services to their clients. Underpinning this new way of working would be a complete, future-proofed technology refresh. Central to the strategy was the ability to work anywhere with the assurance that consistent security policies are in place to protect company and client data.

### Solution

Stridon worked with Wedlake Bell on a complete network and infrastructure refresh of their new central London office. Security is integral to the solution design to ensure compliance with data protection laws, and to protect the

business from ever-changing and sophisticated cyber threats. Secure Wi-Fi coverage throughout the office and meeting rooms ensures that employees can work seamlessly with the same level of service and a consistent experience. Bring-your-own-device security policies were put in place to protect company data and assets as the business shifted to a higher number of remote workers. Wedlake Bell's transformation strategy was underpinned by Microsoft Modern Workplace, with collaboration tools such as Teams which proved critical to the firm's ability to keep running during the COVID-19 pandemic.

### Results

Based on our partnership, Wedlake Bell now has a technology roadmap that is fully aligned with their business goals, with the agility and flexibility to meet evolving client needs. The decision to implement Microsoft Teams has transformed how the firm collaborates and communicates both internally and externally with clients—from secure conference calls to messaging and file sharing. Productivity has increased and decisions can be made faster, which ultimately leads to a better experience and outcome for clients.



# START

changing perception from within

## Start your IT journey here

Just as a journey starts with a simple step. A better IT future begins with a quick conversation. Let's talk about your plan.

[GET STARTED](#)

