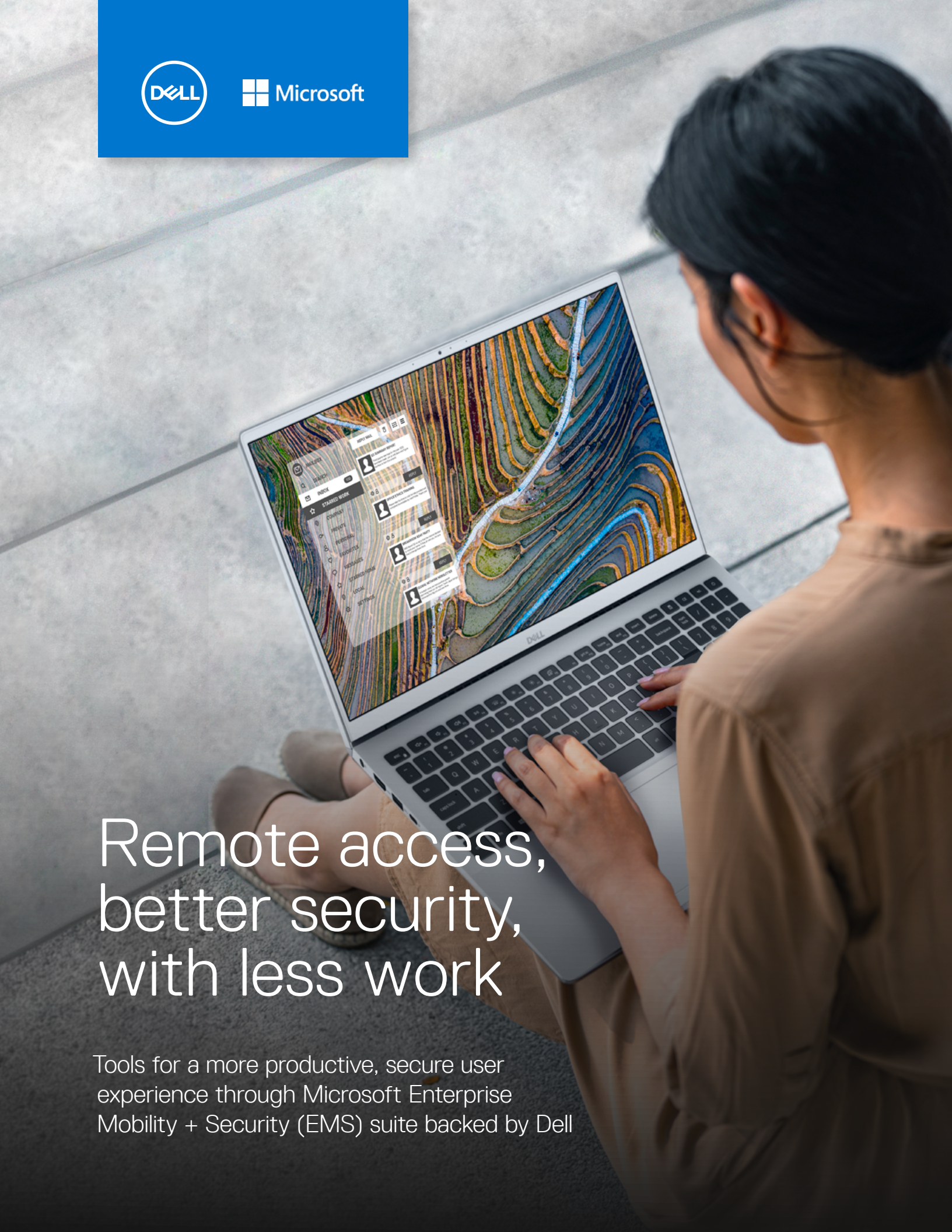

Remote access, better security, with less work

Tools for a more productive, secure user experience through Microsoft Enterprise Mobility + Security (EMS) suite backed by Dell

Improve security for data, users and remote access.

Streamline IT operations with unified user and identity management through Microsoft EMS suite backed by Dell.

In early 2020, IT departments across the globe scrambled to provide remote access to employees to enable working from home. Considered a temporary situation at the time, the reality of remote work has persisted and is not expected to end anytime soon. Organizations have found that many employees enjoy working remotely. According to Pew Research, more than half of employees whose work can be done remotely say they'd like to continue working from home most or all of the time when the pandemic subsides.[1]

Meanwhile, cyber criminals are taking advantage of the situation by ramping up efforts to phish for unauthorized access, leading to a dramatic rise in breaches, malware attacks and ransomware attacks.

In addition, IT departments that were not accustomed to supporting remote workers have had to adjust. Provisioning new users with equipment and software, as well as supporting existing users, has become more complex. Security concerns are now more urgent. Adding to the IT burden is the expectation that users be able to access their work from multiple personal devices.

54% of workers want to work from home even after the pandemic.[2]

DELL Microsoft

Many customers have already adopted Microsoft 365 tools for productivity and collaboration. Now, with the Microsoft EMS suite—part of Microsoft 365 from Dell—you can expand your toolset to include tools to improve management and security for users, data and devices.

The Microsoft EMS suite—delivered by Microsoft and supported by Dell—provides IT departments with the ability to easily enable remote access with better security. At the same time, they can automate many common processes to free up IT resources for more mission-critical work.

Like any new tool, adopting EMS involves a learning curve and a strategy to make the transition. To help you make an informed decision, this white paper outlines some of the changes you can expect in your day-to-day work as it pertains to user management and securing access to your network with EMS from Dell.

Unified user and identity management

Enabling and securing remote work on any device requires a different approach to managing users and identities. In essence, with EMS, Microsoft has modernized certain aspects of Active Directory to enable remote access with better security.

While Active Directory governs access to your on-premises environment using a group policy approach, EMS provides the toolset to unify access across on-premises and the cloud using a centralized identity and access management (IAM) approach that improves visibility and control. With identity governance under EMS, IT departments can control access to applications and data more efficiently to ensure only authorized users have access.

A sync service between your local Active Directory domain controller to Azure Active Directory Premium enables single sign-on (SSO) and multi-factor authentication (MFA) services, which under Active Directory alone would require third-party extensions.

A new way to think about security

Because EMS is cloud based, it can bring cloud-level security to on-premises data. This opens opportunities to provide cloud-like access services and security to your whole environment.

File-level permissions for more granular security

Evolving security challenges require a modernized approach. Under Active Directory, most organizations secure applications and data behind a firewall and use a group policy approach to assign permissions at the server and folder levels.

With EMS, data security is handled at the file level involving classification of data with identity and access management. This gives the entire organization more control over data access to prevent employees from inadvertently accessing the wrong information. It can also make it more difficult for hackers to access sensitive data, even if they get access to your network.

Document classification and tracking in EMS provides the ability to classify, label and protect data based on its sensitivity, giving organizations added security for information sharing. The process can be configured to be fully automatic, driven by users or based on recommendations.

This protection follows the data and end-user access rights. Using EMS enables an adequate balance of security and accessibility in most situations. You can also define what users can do with data, such as allowing a specific user to view or edit specific files but not print or forward.

Evolving security challenges require a modernized approach.

Automated risk detection

To help prevent attacks before they happen, EMS uses automated risk detection to protect your organization with adaptive, built-in intelligence that can detect and prioritize threats to investigate compromised identities and sophisticated attacks. For example, EMS automatically identifies configuration vulnerabilities and provides recommendations on remediation. In addition, prioritized alerts help security teams focus on real threats rather than investigating false positives.

Spend less time and get better results.

By modernizing user management and security through EMS from Dell, IT departments of small and medium-size organizations can implement the same security and identity solutions used by big enterprises. EMS enables IT departments to deliver the flexibility users need, while delivering more granular, intelligent security than legacy solutions that weren't designed with remote work in mind.

Get ahead of shadow IT

Providing flexible access from multiple devices, whether users are at work, at home or are traveling, is more than a convenience to users. It helps prevent frustrated users from developing creative workarounds to access files by emailing or sharing through another method that doesn't follow company policy for secure handling and management of data. With no motivation to invent new processes, users are free to collaborate and share with confidence.

*For more information regarding the various offers, please see Microsoft 365 from Dell Service Description.

Consolidate vendors

In the quest to provide modern conveniences and functionality like SSO, MFA and eDiscovery tools to support litigation, many IT departments have relied on third-party solutions as add-ons to their Active Directory environments. While organizations get the functionality they need, they also get added complexity and cost if the solutions don't work well together or with other installed software or hardware. By consolidating identity management and security through a single platform, IT departments can simplify operations and spend less time dealing with multiple support teams, continually learning new third-party applications and maintaining compatibility with Microsoft applications as they are updated.

Consolidate billing, support and purchasing

By consolidating vendors, you also consolidate billing and support through one partner. Dell provides added value for support with 24/7 availability by phone, email and chat for administrators and users.* When you contact Dell for support, you'll have access to a Dell support representative dedicated to L1/L2 technical support for Microsoft 365 Cloud Solution Provider (CSP) licenses owned.

By monitoring usage through the Microsoft 365 admin portal, IT departments can also optimize licensing and spending. You'll have a clear view of who is or isn't using certain applications and can easily reassign or reduce licenses accordingly.

By consolidating identity management and security through a single platform, IT departments can simplify operations and spend less time dealing with multiple support teams.

Streamline compliance

With modern, intelligent security tools native to Microsoft, organizations can streamline compliance with internal policies, legislation, industry regulations and best practices.

Accelerate cloud adoption

By managing identity and security in the cloud, organizations can get a leg up on cloud adoption. For example, IT managers may find it productive to move certain servers and files to the cloud, allowing them to decommission on-premises infrastructure or free up data center resources for other needs. By moving to the cloud incrementally, you can more effectively manage risk while getting the advantages of cloud security and availability.

With EMS from Dell, end users benefit from fast, seamless access from any device with confidence that they can collaborate securely.

Gain peace of mind with enterprise-grade physical security

Microsoft is able to reduce risk in ways that most enterprises can't afford. That's because a Microsoft data center has many advanced capabilities that are difficult or impossible for companies of any size to replicate, including automatic triplication of data in multiple data centers for high availability and built-in redundancy, and onsite power generation to protect from natural disasters or other interruptions in the power supply.

While it's comforting to be able to reach out and touch a server, physical availability won't help much if it's on fire or underwater.

Benefits to users

With EMS from Dell, end users benefit from fast, seamless access from any device with confidence that they can collaborate securely. SSO and MFA, if enabled, provide added security, convenience and productivity. New employees get fast access to your network with auto-enrollment, and users can even reset their own passwords, taking the burden off IT.

Benefits to your organization

With EMS from Dell, you can bring unity and security to your on-premises infrastructure and cloud-based access needs.

To learn more about how EMS tools, delivered through Microsoft 365 from Dell, can streamline IT operations and improve security, or for more information about the complete Microsoft 365 from Dell offering, contact us at Get_Office365_US@Dell.com to schedule a short discovery call where you can have a discussion personalized to your needs and environment.

[1–2] Parker K, Horowitz JM, Minkin R. "How the Coronavirus Outbreak Has — and Hasn't — Changed the Way Americans Work," Pew Research Center, December 2020.