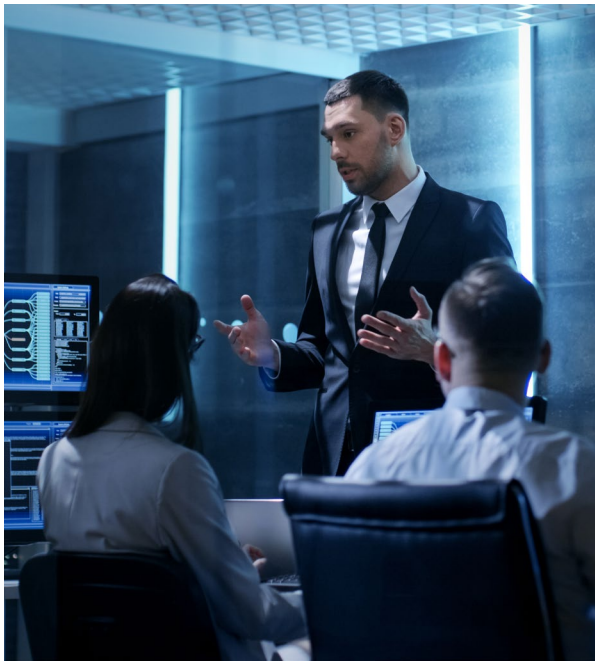
ivanti

AT&T Business

Unified Endpoint Management: A powerful tool for your cybersecurity arsenal

With the added power of zero trust to fight cybercrime



Executive summary

Welcome to the "Everywhere Workplace." It's here thanks to new mobile and cloud computing technologies that empower users to be more productive, on any device, and virtually anywhere they work. Today's workers choose from an extensive range of mobile endpoints, operating systems, applications, and cloud services to access the corporate resources that they need for work.

The Everywhere Workplace makes business more flexible, but it also carries risks. More data is flowing freely across and outside of the enterprise. That's why IT needs to establish trust in a zero-trust world. In other words, you must assume that every user, device, app, network, and cloud is at risk of compromise. Building a zero-trust security environment requires a new mindset and technical approach to security starting with good cyber hygiene and a foundational process. Fortunately, that's something every organization can start doing today.

Risks to business

Today's business environment is more challenging than ever. The dramatic upswing in remote work due to the global pandemic and the allure of Bring Your Own Device (BYOD) present new security challenges, and cybercriminals are exploiting them. Malware, ransomware, and mobile phishing are all on the rise.

The FBI's Internet Crime Complaint Center (IC3) received a record number of complaints (791,790) from the American public in 2020, with reported losses exceeding $4.1 billion. That's a 69% increase in total complaints from 2019.[1]

Malware (including ransomware, trojans, and exploit kits) skyrocketed 78% from March 2019 to March 2020, according to the 2020 Cybersecurity Insiders Endpoint and IoT Zero Trust Report.[2] The number of compromised endpoints has increased by 56%, and compromised credentials are up by 58%.[2] Lack of endpoint enforcement has risen by 47%.[2]

Pain points

Businesses large and small are feeling the squeeze. They must manage a hybrid workforce that consists of workers in the office, at home, and on the go. While BYOD helps solve the challenge of working from home, it also greatly increases scale and number of endpoints connected to the corporate network.

IT personnel now must resolve issues remotely with increased workloads and a scarcity of qualified workers.

In this business environment, cybercriminals are growing bolder and more powerful. The news is filled with stories of ransomware attacks against meat processing plants, gas pipelines, government agencies, hospitals, and universities. These attacks — which use malware to extort money — can cost millions, cripple organizations' ability to operate, and damage reputations. For example, JBS, the world's largest meat processor, recently paid a ransom of $11 million in June 2021 to regain control of its customer data.[3]

It's not just super hackers with extraordinary technical skills who are wreaking havoc. Ransomware as a Service (RaaS), a business model used by ransomware developers, gives just about any aspiring criminal with a few dollars in their pocket the ability to launch attacks and extort cryptocurrency from businesses.

How bad is it? According to 2021 research from MSI-ACI, 95% of organizations have security solutions in place to prevent or mitigate ransomware attacks, but 63% have been a victim of a ransomware attack in the last year. About 38% of those victims lost a week's worth of productivity, and 24% lost more than a month.[4]

What is the No. 1 target for cybersecurity breaches? According to IDC, 70% of cybersecurity breaches originate on endpoints[5] — that is, devices that can be connected to a network: computers, laptops, smartphones, smart watches, tablets, and point-of-sale (POS) systems. Endpoints also include work-related Internet of Things (IoT) devices and personal IoT devices such as smart TVs and health monitors which have been known to accidentally connect to a corporate network.

UEM in the Everywhere Workplace

Unified endpoint management (UEM) can play a huge role in helping organizations transition to a security landscape that's compatible with the Everywhere Workplace. UEM establishes a foundation for a zero-trust environment where employees can confidently embrace modern endpoints, desktops, apps, and cloud services. UEM uses the zero-trust model and policy framework needed to provide secure access to corporate data. The ultimate goal for UEM is to ensure that employees stay productive and happy on the devices of their choice and can work from virtually anywhere — but in a manner that protects your business from the latest threats.

UEM helps ensure that endpoint devices, including laptops and mobile devices, are managed in the same way and with the same security protections and protocols.

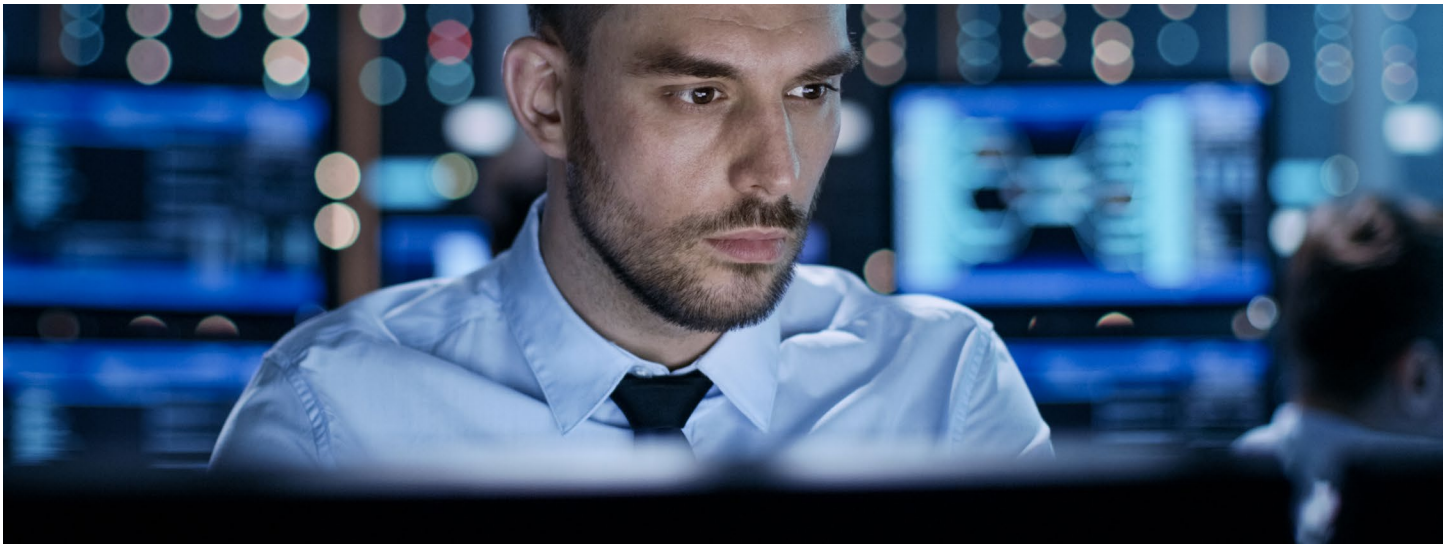
Let's look again at how the workplace has changed. For decades, the IT-controlled desktop was the main productivity tool in the enterprise. Today, mobile workers no longer want to be tethered to locked-down PC workstations, and they expect IT to support the mobile devices and apps they need to stay productive wherever they work.

The trouble is, many companies once had their IT staff in charge of desktop and laptop devices, while smartphones were handled by telecommunications staff. This meant the two teams had different skills, priorities, and perspectives.

Working with multiple management platforms with different vendors, support contracts, and interfaces requires more time, training, and resources than using a single platform. A UEM console creates a single set of user access and security policies and deploys them consistently across all user devices.

UEM helps protect corporate data and applications. Here's what it can do:

- Configure, manage, and protect devices running iOS, macOS, Android, and Windows. UEM tools can also manage wearable endpoints as well as rugged devices often used by frontline workers.
- Deploy applications and user profiles.
- Provide patch and security updates.
- Keep devices compliant and help protect data.
- Provide a single view of users with multiple devices which helps facilitate more efficient end-user support and generate more detailed workplace analytics.
- Act as a coordination point to orchestrate the activities of related endpoint solutions such as identity services and endpoint security infrastructure.



Mobile threat defense and zero sign-on

Businesses should look for a UEM solution that is built on the principle of zero trust. The solution should include mobile threat defense (MTD), which protects organizations from threats on iOS and Android devices and provides protection by preventing, detecting, and remediating attacks. UEM combined with MTD provides threat detection and automated remediation. The following chart shows how they can complement each other.

Feature	UEM	MTD
Identifies jailbroken or rooted devices	P	
Enforces passcodes	P	
VPN and encryption	P	
Detect phishing attempts		P
Detect man in the middle attacks		P
Detect malicious applications		P
Offline detection		P
Security policy enforcement		P*
Automated remediation		P*

The best UEM solutions can also eliminate passwords – the most common initial attack vector in data breaches – to help organizations further transition towards a zero trust architecture. Zero sign-on is a simple authentication capability that replaces passwords with multi-factor authentication (MFA) methods based on FIDO 2 protocols, including biometrics, mobile devices and/or FIDO security keys. This passwordless approach ensures that only verified users, devices, apps, and networks can access business resources.

Benefits of UEM

Think of UEM as "one tool to rule them all." It's a way to provide your end-users with a better experience using a platform that discovers, manages, and protects a wide variety of devices from on-premises to the edge. The potential benefits are vast.

Reduce the complexity and cost of managing endpoints. Single console enables IT administrators to manage and protect any iOS, macOS, Android, or Windows devices across your Everywhere Workplace. With UEM, you can scale to add new features over time as your business needs and budget requirements change.

Freedom of choice. UEM is OS and device agnostic, which allows users to choose their preferred devices, whether corporate-owned or BYOD, to stay productive wherever they work. IT administrators can also deploy either a cloud or on-premises deployment model depending on their business needs. With UEM, you can enable a multi-OS environment to support iOS, macOS, Android, or Windows-based devices. You can also allow users to quickly access enterprise resources such as corporate email, calendar, and cloud services including Microsoft 365 Google Workspace, Dropbox, Box, SharePoint, and more.

Seamless, productive user experience. Establish mobile security protocols that protect your devices, apps, and data without compromising the user experience. When employees experience a familiar, native device and app experience with enterprise tools, they are more likely to accept compliance measures, avoid shadow IT maneuvers, and stay productive.

UEM vs. Mobile Device Management

Perhaps you're thinking: "I already have MDM." Why do I need UEM?"

MDM is a software tool that allows IT administrators to manage mobile endpoints including smartphones, tablets laptops, and IoT devices. As the BYOD trend becomes more of a norm, it's crucial for companies to be able to manage both devices owned by the company and devices owned by employees.

MDM relies on the client/server model to function. Using a management console, the server component allows IT administrators to configure devices and deploy profiles and policies. The client component resides on each mobile device and receives whatever directives have been assigned from the management console.

UEM is a supercharged version of MDM. It can be used to manage all your endpoints, including traditional endpoints such as desktops and printers and not just mobile devices. It also adds capabilities to oversee and secure documents, applications, and content.

UEM solutions also enable over-the-air device configuration to reduce IT involvement and user interaction. UEM supports the major device enrollment programs such as Apple Business Manager, Microsoft Windows AutoPilot, Samsung Knox Mobile Enrollment, and Google zero-touch.

UEM can also integrate with existing Microsoft Active Directory/Lightweight Directory Access Protocol (AD/LDAP) infrastructure and saves time by allowing AD/LDAP records and groups to be imported directly into the UEM.

With a UEM solution, employees can access encrypted content repositories and more safely use third-party sharing solutions like Google Drive, SharePoint, and Box. Compared to basic MDMs, this type of extensive integration and capabilities allows employees to be both productive and secure.

Get started with first-class help

Change can be challenging. Changing your entire approach to cybersecurity can seem especially daunting. Fortunately, AT&T Business can help ease the stress.

We bring value-added services such as professional install, 24/7 support, an assigned UEM consultant, managed technical support, certified professionals, consulting, and mobile security health checks. For an additional fee, we can provide ongoing remote administration for advanced management and policy support. Our consultants will spend time understanding your environment and goals, then implement policies and solutions that align with the needs of the business. Remote administration support can help free up your technical resources for other projects and priorities.

Why Choose AT&T

AT&T Cybersecurity helps reduce the complexity and cost of fighting cybercrime. Together, the power of the AT&T network, our software-as-a-service (SaaS)-based solutions with advanced technologies (including virtualization and actionable threat intelligence from AT&T Alien Labs and the Open Threat Exchange™), and our relationship with more than 40 best-of-breed vendors help accelerate your response to cybersecurity threats. Our experienced consultants and security operations center (SOC) analysts help manage your network transformation to reduce cybersecurity risk and overcome the skills gap.

For more information on how UEM powered by MobileIron and AT&T can help protect your business, please contact your AT&T representative, or visit www.att.com/mobileiron.

[1]Federal Bureau of Investigation Internet Crime Complaint Center's Internet Crime Report 2020 https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

[2]2020 Cybersecurity Insiders Endpoint and IoT Zero Trust Report. https://www.pulsesecure.net/resource/endpoint-iot-securityreport-infographic/

[3]JBS Paid $11 Million to Resolve Ransomware Attack, from https://www.wsj.com/articles/jbs-paid-11-million-to-resolve-ransomware-attack-11623280781

[4]Research was conducted between April 30 – May 29, 2021 by MSI-ACI via an online questionnaire to 1,005 IT Business Professionals in the U.S., U.K., France, Germany, Australia, and Japan.

[5]IDC: 70% of Successful Breaches Originate on the Endpoint, from https://www.rapid7.com/blog/post/2016/03/31/idc-says-70-of-successful-breaches-originate-on-the-endpoint/