IBM **Security**

Have no fear, UEM and MTD are here

Behold a unified endpoint management (UEM) strategy that *includes* mobile threat defense (MTD).

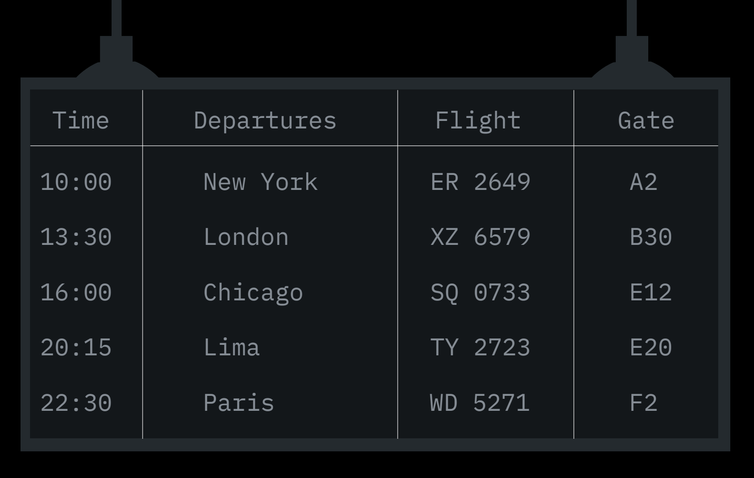
When you think of mobile threats, you're probably thinking about **malware** infecting a device. It may be siphoning data, keylogging or tracking locations. That's a part of the problem, but it's not the whole story.

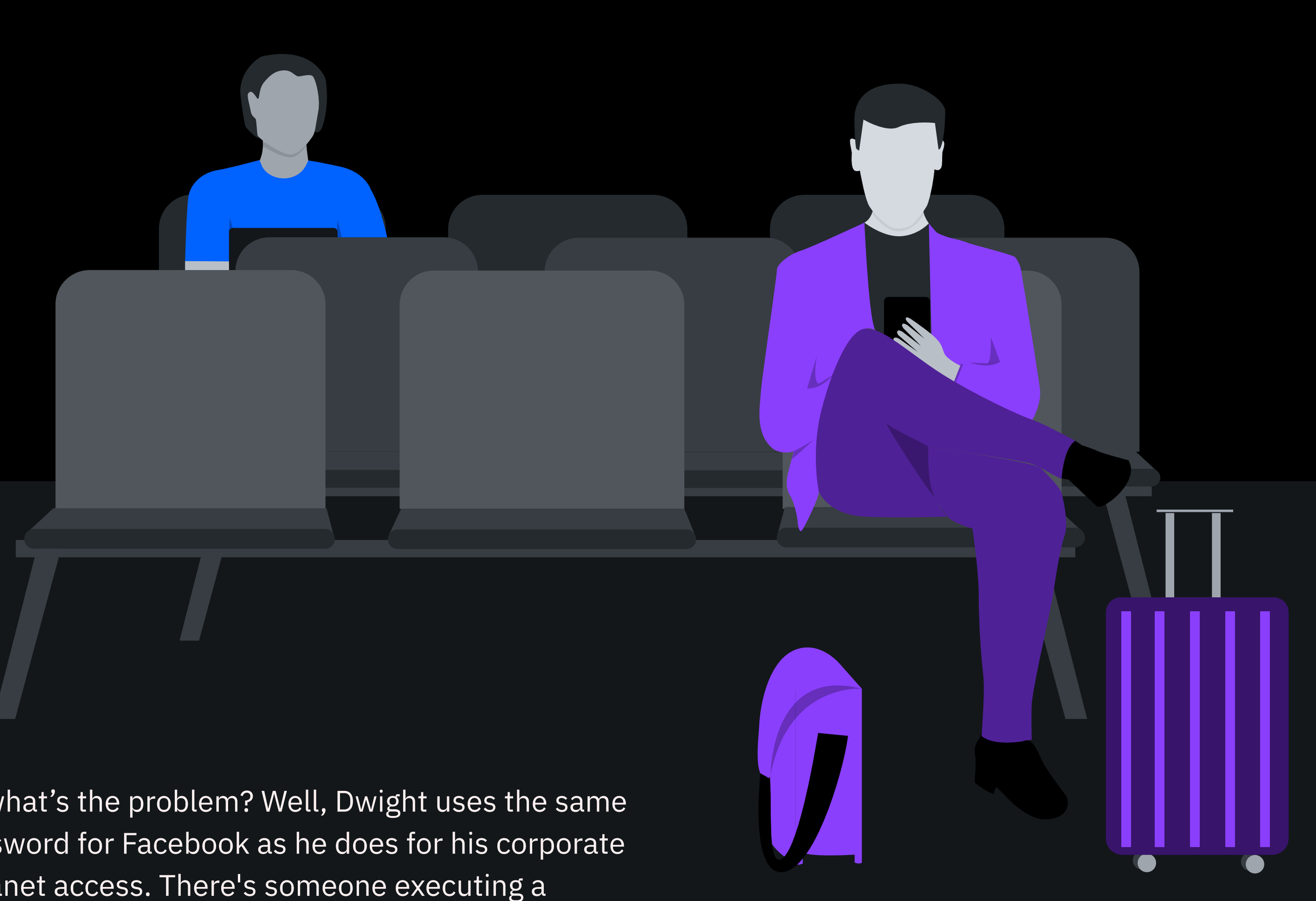
Meet Dwight

Like many workers these days, Dwight has a smartphone, a tablet and a laptop.

Dwight's about to embark on his first business trip, and he was issued a UEM-enrolled and enabled corporate device to use while he's out of office. With a long day of sitting in an airport terminal ahead of him, he downloads a bunch of new social media and entertainment apps.

On the surface, none of these apps seem particularly suspicious. But Dwight, like many in his position would, downloaded them via the first public Wi-Fi connection that popped up on his list of options.

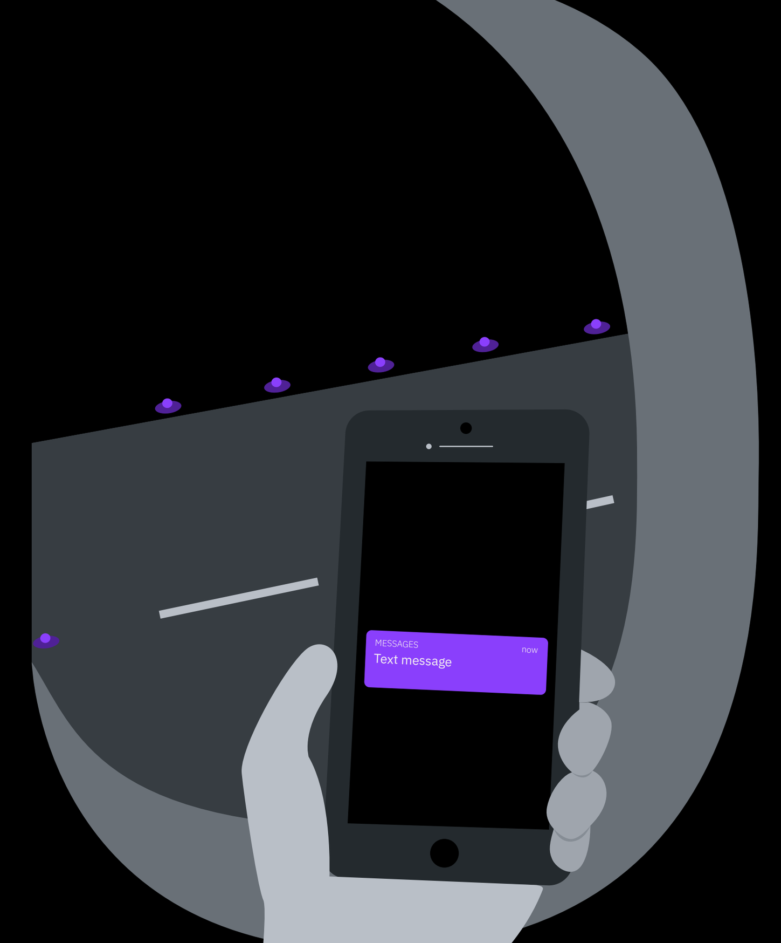


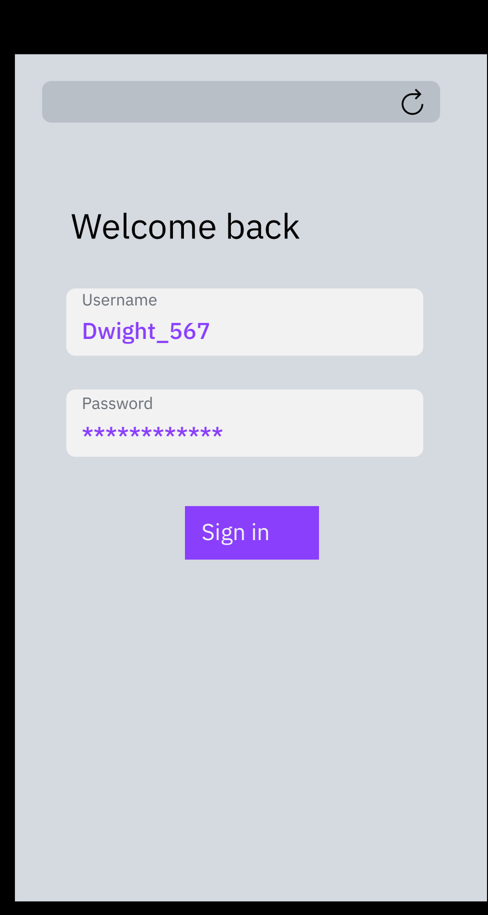


So what's the problem? Well, Dwight uses the same password for Facebook as he does for his corporate intranet access. There's someone executing a **man-in-the-middle attack (MITM)** sitting three seats away from him, intercepting traffic off the public Wi-Fi — including Dwight's credentials.

Strike 1

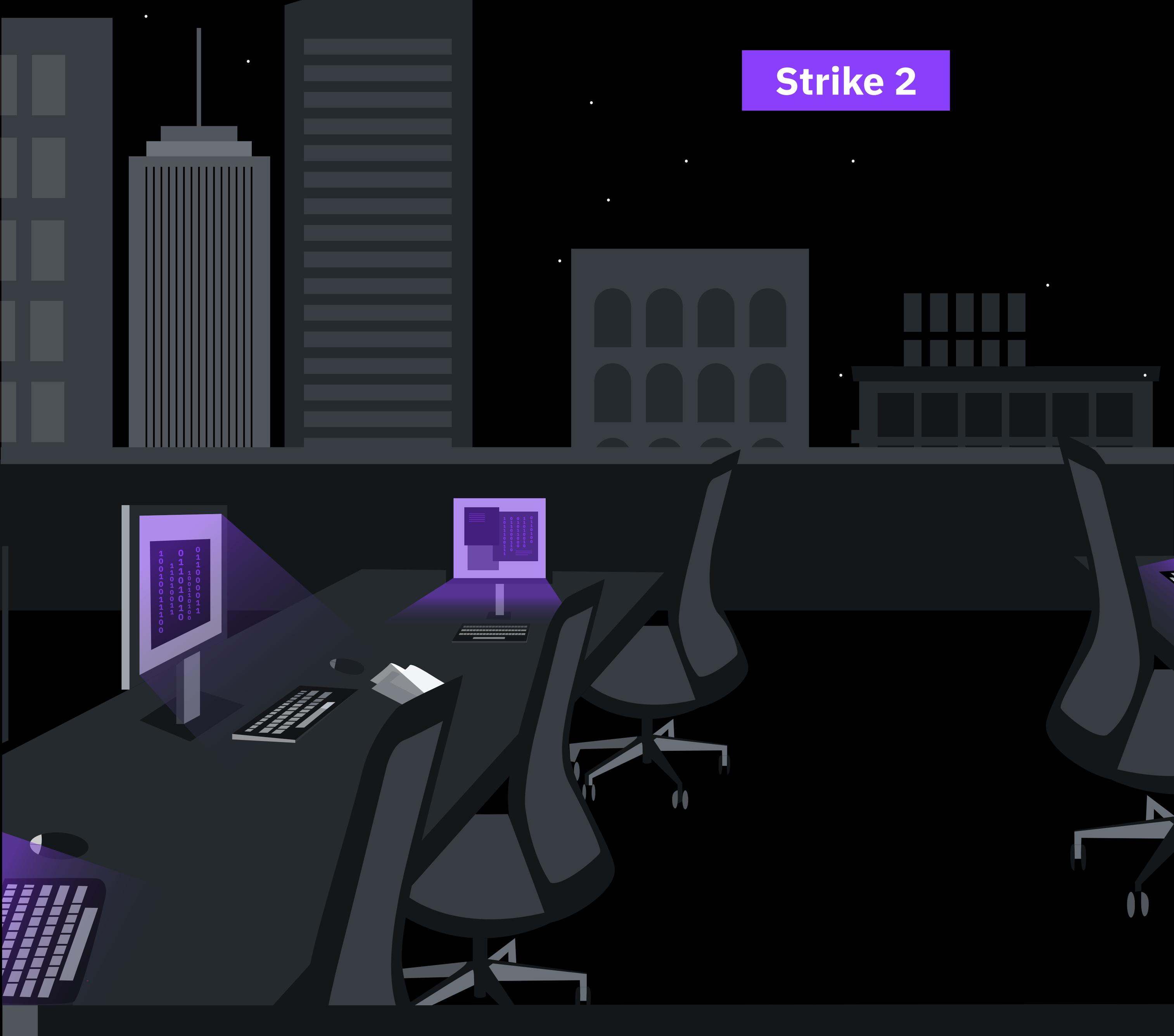
Dwight boards his flight and turns on airplane mode. When he lands, he sees a text from a familiar area code claiming to be his VP. He's groggy from the flight and doesn't notice that his VP's name is misspelled and the link to the corporate website in the text was off by one letter. He hit a landing page he recognized and logged in. Turns out this was a **phishing attack**, and Dwight fell for it — hook, line, and sinker.





For the second time, Dwight's credentials have been stolen, threatening the security posture of his organization. He wasn't acting maliciously, he just wasn't vigilant.

Strike 2

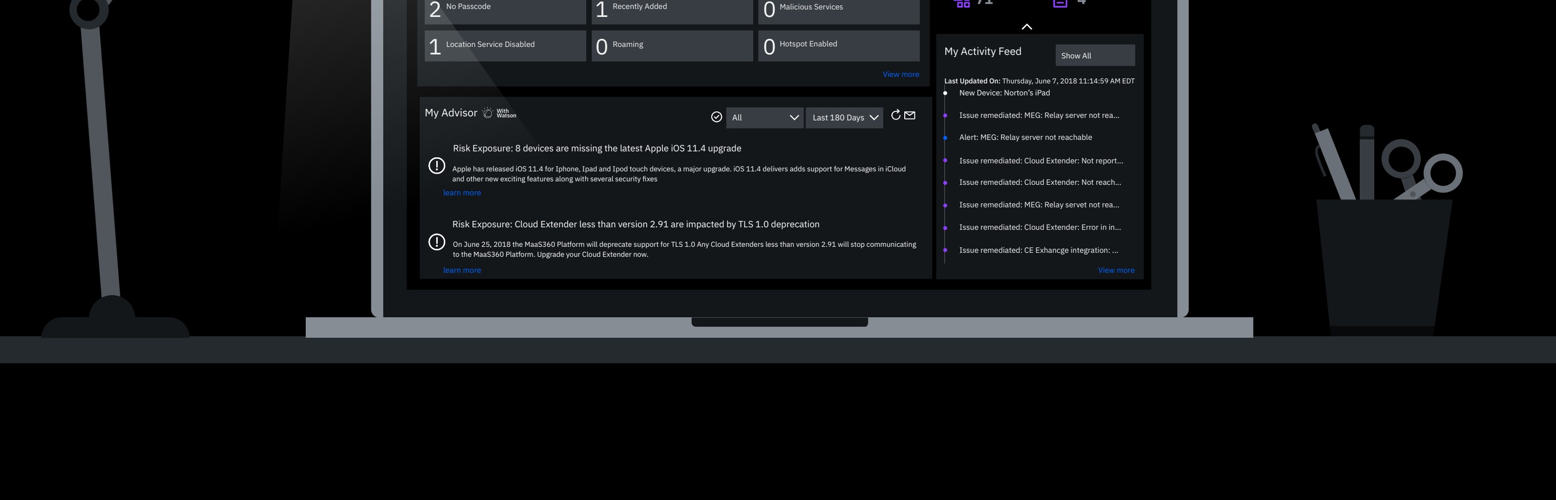


Turns out, things would get worse; he just didn't realize it for a while. After returning home, Dwight found that his new phone's battery kept dying quickly. Dwight was confused — this phone was known for its great battery life.
So, what happened?

Unfortunately, this is a common occurrence, and no fault of Dwight's. It happens that one of the news sites that he regularly uses to stay current was hacked — and used for **cryptojacking**. Dwight's operating system and hardware had been hijacked — and put into overdrive for Bitcoin mining. Ipso facto.

Strike 3

This may be a fictional story, about a fictional guy. But it's a very real example of the modern mobile threat climate and the vulnerabilities your organization can be exposed to without adequate proactive defense.



Offered in combination with Wandera MTD, IBM MaaS360 with Watson UEM helps keep your bases covered across devices, users, apps, data and your network:

- Device scanning
- Jailbreak and rooting detection
- OS attacks
- App scanning (signature-based)
- Advanced non-signature-based malware protection
- Data leak (unencrypted sensitive data) detection
- Mobile phishing protection (covers all apps/browsers)
- Malicious network traffic (c2c, data exfiltration, etc.)
- Risky hotspots detection
- Man-in-the-middle attack detection
- Data protection via encrypted tunnel

Explore the demo today, so folks like Dwight can take flight without fright.

Try demo

IBM