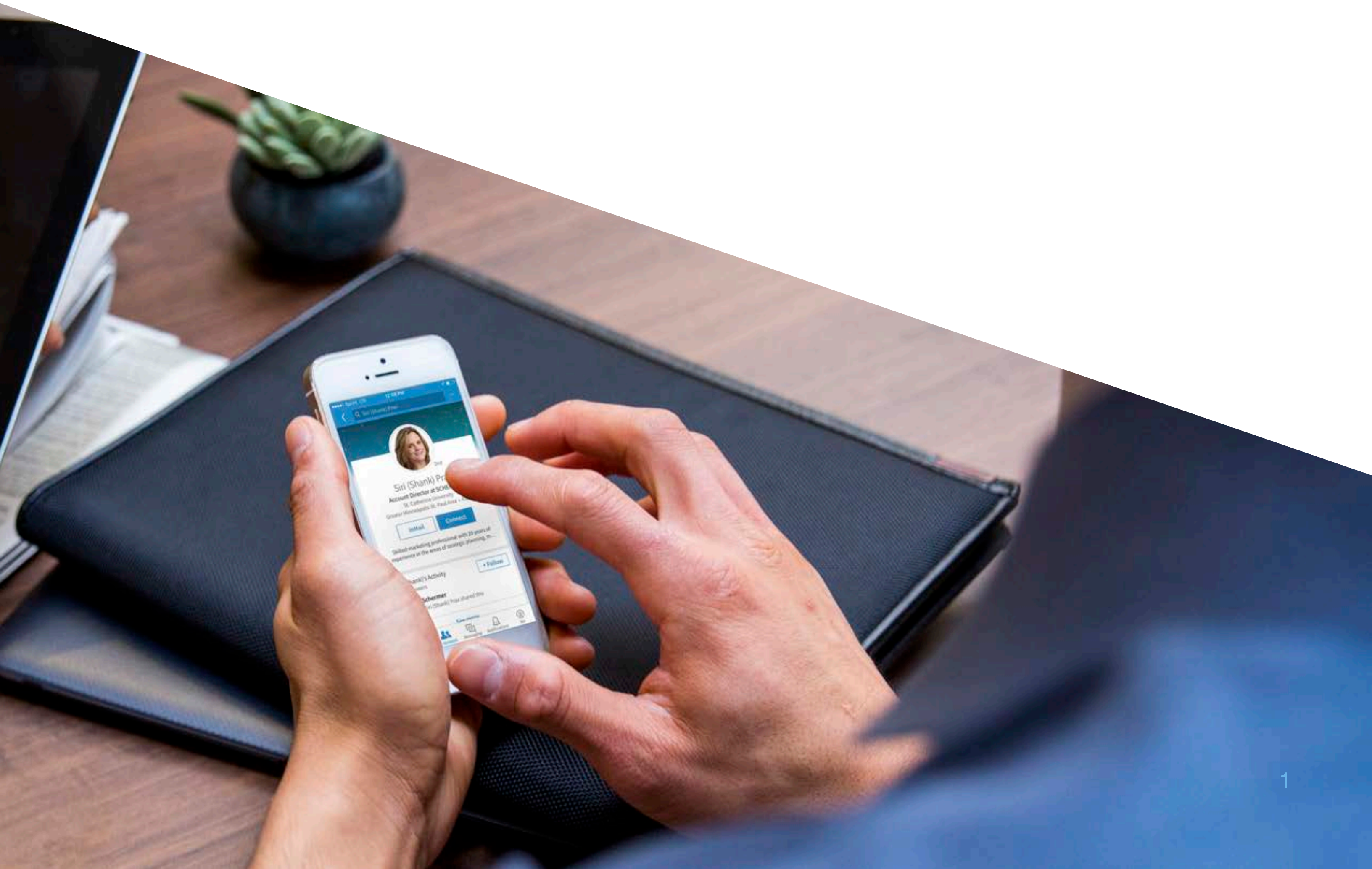
Employee Connectivity vs. Data Security

Today's employees demand the ability to move seamlessly between their professional and personal lives. They're always connected, managing multiple aspects of their lives online; they expect this same level of connectivity and convenience from professional tools and systems. This level of convenience—particularly when it comes to travel and expense (T&E) management—can expose organizations to multiple types of risk. The challenge is finding the right tools and systems that provide connectivity and convenience employees want without sacrificing security in the process.



Employee connectivity

Connectivity is the new normal

For a large part of today's workforce, connectivity is a base-level expectation for everyday productivity.

When it comes to business travel, the expectations get even higher. Employees don't just want to be able to conduct business from their smartphones, tablets or laptops while they're on the road.

They want to use mobile devices to manage their entire trip, from booking plane tickets and ordering cabs to setting up reservations, paying for client meals and taking care of other discretionary purchases.

They expect expense tracking and reporting to be just as simple, with automatic expense capture and automated T&E claims processing. On their return, they want to be able to complete their expense reports with minimal hassle and additional paperwork.

88%

88% of millennial workers want work/life integration.[1]

>50%

More than 50% of workers in North America are mobile: they travel, drive for work, and work virtually.[2]

75%

75% of business travelers use their smartphone for both business and personal during their trip.[3]

Data security ►

Data Security

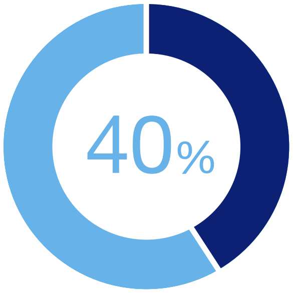
Connectivity opens the door to risk

The ever-increasing use of smartphones and mobile devices for business equals a growing risk to organizations, both in the office and on the go.

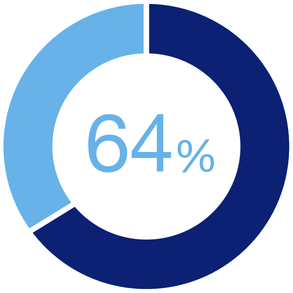
According to a new study by the Ponemon Institute, employee mobile devices are the root cause of many data breaches, whether those devices are used in the office or during business travel.[4]

In a world where mobility and connectivity are the norm, it won't be enough to install IT security at the corporate or server-system level. Even endpoint management software that provides security for all devices attached to a network—including mobile devices—is not foolproof.

Organizations need security that provides point of sale encryption and cloud-based protections to ensure top-notch security of data in real time.



40% of organizations are challenged by security and compliance risks from byod (bring your own device).[5]



64% of organizations are not vigilant in protecting sensitive or confidential data stored on or accessed by mobile devices.[6]

Finding the balance

Connectivity and security: a look forward

Leading organizations are seeking systems that give employees the convenience and connectivity they expect while allowing for the level of security needed to protect the business. Overly restricted employees (who are not able to experience the connectivity they take for granted in everyday life) may not be able to comply easily with policies around prompt and accurate expense reporting. What companies don't want is to trade complete connectivity for the risk of a costly data breach. And with the solutions available today, they don't have to.

[1] Forbes, What Millennials Want in the Workplace (And Why You Should Start Giving It To Them), 2014
[2] Runzheimer, Visibility: Better Insight Leads to Better Cost Control, 2015
[3] Concur, Travel and Expenses Management - How modern How modern finance leaders balance control with employee satisfaction, 2016
[4] Ponemon Institute, The Economic Risk of Confidential Data on Mobile Devices in the Workplace, 2016
[5] Aberdeen Group, Knowledge Tied to Action: How Leaders Combine Deep Network Analytics with Automated Control and Management, 2016
[6] Lookout, Mobile risk is a real number, 2016