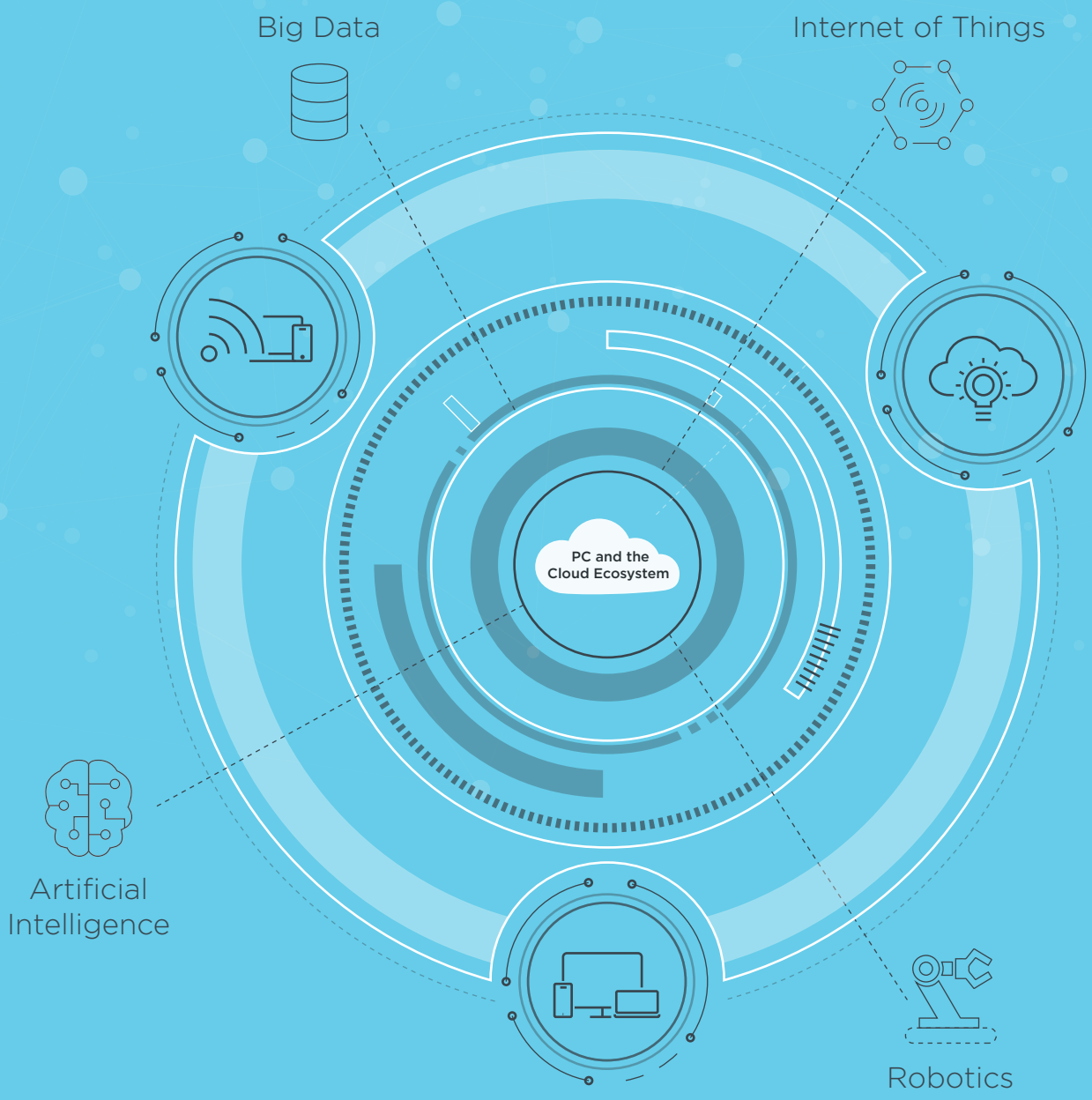
# CLOUD SECURITY THROUGH ENDPOINT DEVICES

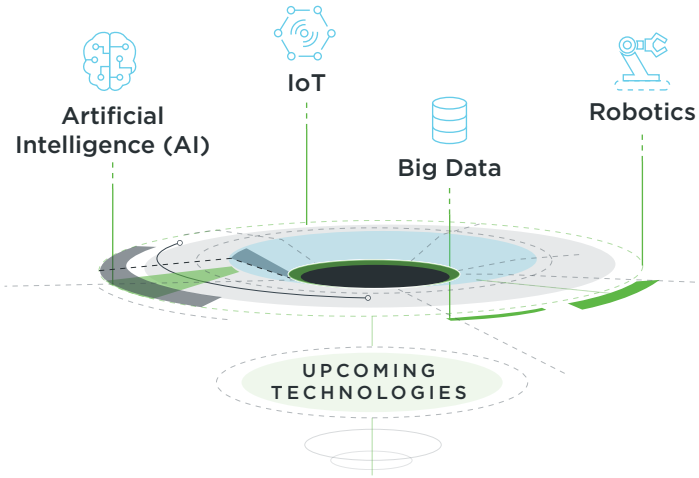



Powered by Intel®.
Intel Inside®.
Powerful Productivity Outside.

www.lenovo.com


Most of the upcoming technologies like **Big Bata, cognitive computing, IoT, AI, and robotics** are underpinned by Cloud. So, Cloud is one of the most critical investment decisions that any organization can make.

Given that it's the foundation for so many of the technologies that any organization will eventually adapt (if they have not already), looking at a Cloud investment decision in silo can be detrimental to business.




Endpoint devices are an important aspect of the PC and the Cloud Ecosystem. Most organizations today are realizing the importance of providing endpoint devices specific to the job requirements. For example, for account executives who are on the move most of the time and need to get a lot accomplished on-the-go, devices which are lightweight, durable, flexible like convertibles are a good choice for them.

But beyond choosing the right device for the jobs, the endpoint device strategy is critical because they also decide the security readiness of your organization.

## THREE ESSENTIALS OF AN EFFECTIVE CLOUD STRATEGY

**The Right Endpoint Devices: for your mobile, non-mobile, and specialist users.**

**A Good Cloud Solution:** choosing the right one for your business.

**Effective Device Management and Security:** choosing the right one for your business.

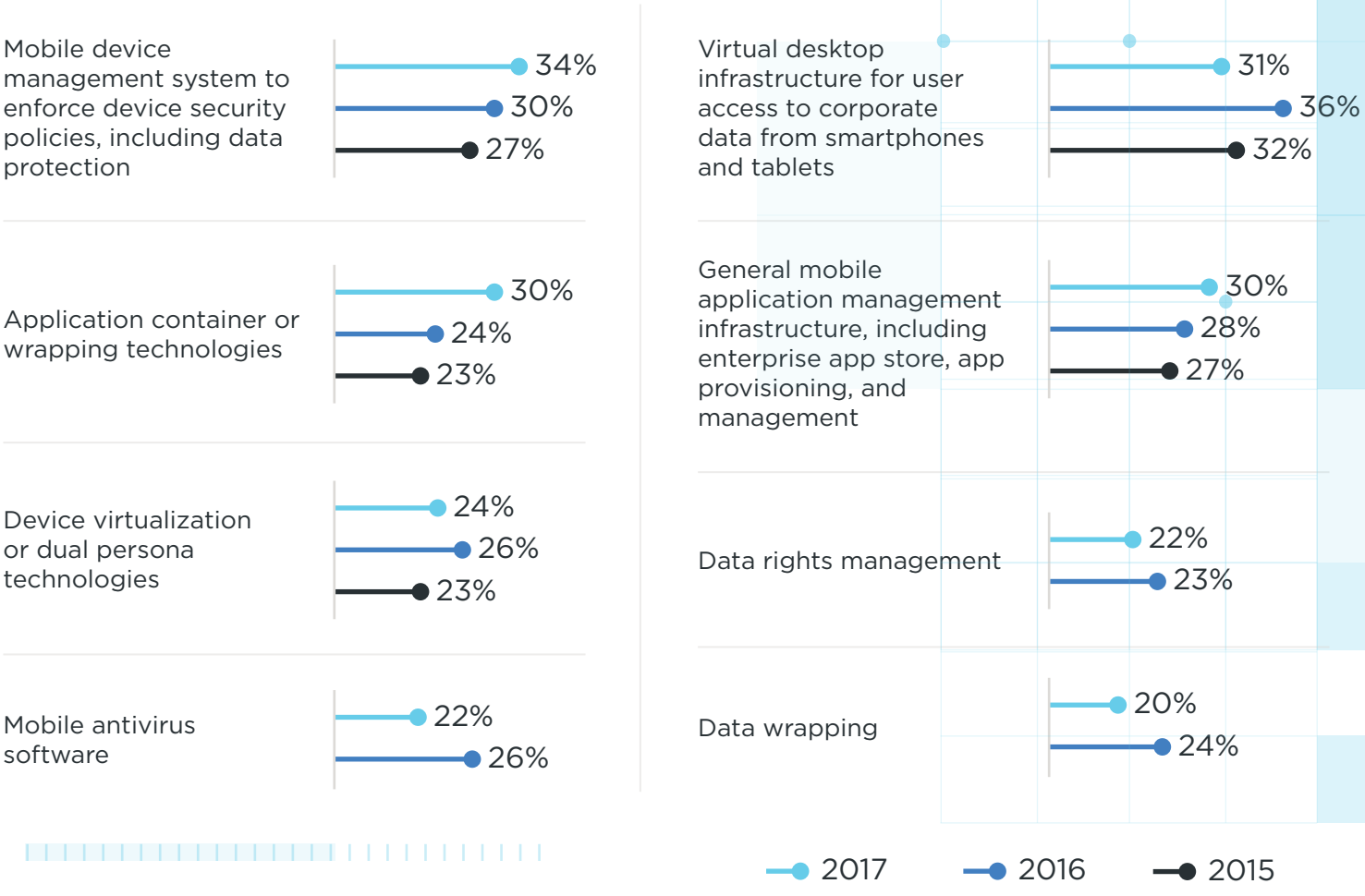


**Click here** to explore Lenovo's Security Solutions

# DEVICES ARE DECISIVE

Endpoint devices are the gateway into your organization's network. So, while investing in your security strategy, don't forget that your infrastructure is only as strong as its weakest link. And don't let that weakest link be the end user devices.

## Mobile Security Technology Adoption




Source:
Forrester Data Global Business Technographics® Security survey, 2017-2015

Powered by Intel®.
Intel Inside®.
Powerful Productivity Outside.

**Click here** to explore Lenovo's Security Solutions

The modern workforce needs to work from multiple locations such as airport, client site, cafe, etc. Cloud has become a huge enabler of productivity and efficiency. But along with that it has also opened avenues for security breaches.

- Unauthorized Device Access
- Using Public WiFi
- Downloading Applications/Software from Unauthorized Sources
- Accidental Damage
- Device Theft/Loss

**About 62% of security breaches today stem from employee error.[1]**

Source: https://www.tektonikamag.com/index.php/2017/07/24/security-breaches

Powered by Intel®.
Intel Inside®.
Powerful Productivity Outside.

**Click here** to explore Lenovo's Security Solutions

# Unauthorized Device Access


Just trying to protect device access through passwords might not be the best way to secure endpoint devices from unauthorized access.

**Almost 40% of SMBs are planning on investing in two-factor authentication approaches in the next 12 months.**

Aspects to look for in your device to prevent unauthorized access:

### Biometric Authentication
Advanced multifactor user authentication like facial recognition and fingerprint reader technologies to protect users and their data.

### Keep Spies Away
Technology that keeps prying eyes from getting access to sensitive data.

### Restricted Port Access
Prevent data theft through USB ports by allowing access to only authorized users.

**ThinkPad T480s**

### Match on Chip Fingerprint Reader Powered by Intel® Authenticate
Protect your data with advanced biometric security solutions.

### Windows Hello and ThinkPad Glance
This advanced facial recognition feature helps keep unwanted users at bay.

### Smart Card Access
A highly secure way of storing login information in tamper-proof cards without using passwords.

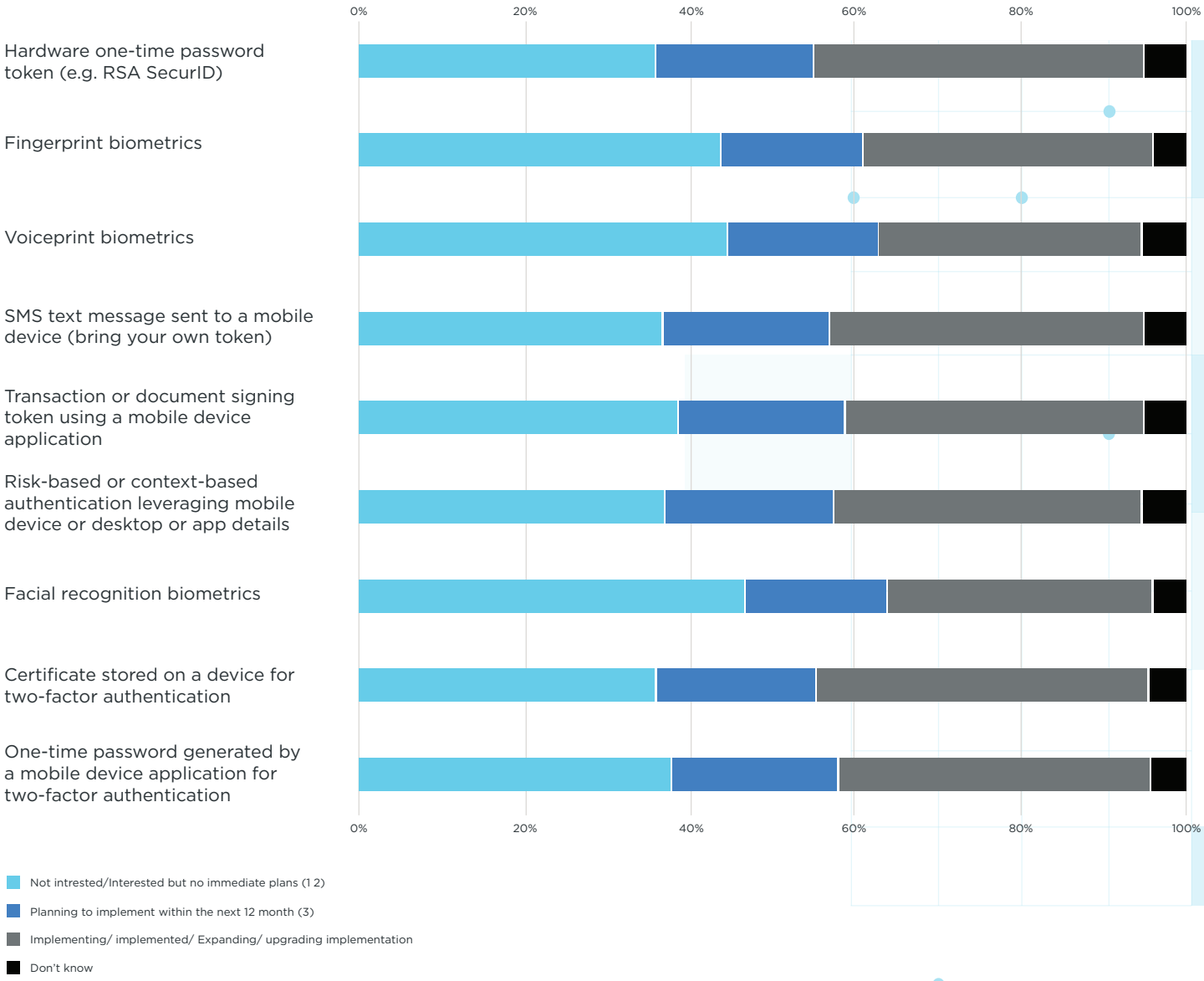
### Smart USB Protect
Prevent data compromise by restricting port access.

Powered by Intel®.
Intel Inside®.
Powerful Productivity Outside.

**Click here** to explore Lenovo's Security Solutions

# Unauthorized Device Access


**What are your firm's plans to adopt the following two-factor authentication approaches? (Expanded/expanding + Implemented/implementing Respondents Recode)**




Source:
Forrester Data Global Business Technographics®
Security survey, 2017



**Click here** to explore Lenovo's Security Solutions

# Using Public WiFi


Most of us don't think twice before connecting to public WiFi networks. Public networks pose multiple types of threats starting from Man-in-the-Middle (MitM) attacks where hackers intercept the data, to rogue WiFi networks where hackers set up WiFi networks that seem legitimate, endpoint attacks where hackers can access your laptop, and worms that transmit viruses to your device.

Whatever be the mode, **Verizon's annual Data Breach Investigation Report has found that 89% of all cyber-attacks involve financial or espionage motives[2].** Clearly no organization wants to fall victim to that.

So, to prevent malicious attacks on your data, devices should have:

**Safe WiFi Access**
In-built solution to recognize secure WiFi networks.

**Contained Threats**
Apps which ensure that malware does not enter devices directly.

**Data Encryption**
Apps that encrypt data in the Cloud and provide secure authentication.

**ThinkPad X1 Carbon**

**Lenovo Vantage**
Monitor WiFi security real-time to keep away from risky and malicious networks.

**BUFFERZONE®**
This feature creates a secure, isolated environment for accessing content from any potentially risky source*.

**Go-Trust®**
Enable multifactor authentication with your fingerprint and phone to unlock your devices and Cloud accounts*.

*not preloaded

Powered by Intel®.
Intel Inside®.
Powerful Productivity Outside.

Source:
https://www.mishcon.com/news/firm_news/89_of_breaches_had_a_financial_or_espionage_motive_04_2016

**Click here** to explore Lenovo's Security Solutions

# Downloading Applications/ Software from Unauthorized Sources


**80% of IT security professionals say their greatest threats are from rogue employees, malware exploits or unauthorized software.[3]**

**An estimated 57% of employees install unauthorized software on company computers, and over two-thirds of that software brings viruses and other malware along with it.[4]**

Hence, it is important for endpoint devices to have:

**In-built Security Features**
Software that allows devices to recognize unsafe apps.

**IT Visibility and Control**
Improve security by allowing IT teams to have device and network visibility.

**Mobile Device Management**
Ensure that data is always secure whether it is stored on a device or in the Cloud.

**Lenovo Vantage**
Enable IT to detect threats near the laptop and take necessary action.

**Coronet**
Secure your Cloud operations by allowing only trusted devices, networks, and Cloud services to access your data.

**Intel® Active Management Technology (Intel AMT)**
Remotely access a device to discover, activate, monitor, protect, and manage it despite its power state.

**MobileIron**
Secure data-at-rest and data-in-motion on devices, networks, and in the Cloud.

Source:
3: https://www.avecto.com/news-and-events/news/80-of-it-security-professionals-say-their-greatest-threats-are-from-rogue-employees-malware-exploits-or-unauthorized-software

4: https://blog.samanage.com/it-asset-management/alert-unauthorized-software-on-network/

Powered by Intel®.
Intel Inside®.
Powerful Productivity Outside.

**Click here** to explore Lenovo's Security Solutions

# Accidental Damage


Data loss doesn't take place only because of theft or unsafe WiFi. Devices and liquids do not complement each other. Something as trivial as a sudden coffee spill can ruin your device and in turn, the data in it. Unforeseen drops can also damage your device. Thus, it is important for businesses to go that extra mile to ensure device safety.

Complete device safety can be ensured with:

**Durable and Reliable Devices**
Devices that are tough to endure whatever comes their way.

**Automatic Backup**
Devices that backup data instantly to prevent downtime.

**Services for Unforeseen Damages**
A warranty service that covers for unintentional damages.

**MIL-SPEC Tested**
ThinkPads are tested against 12 military-grade requirements and pass more than 200 durability tests.

OLDB

**Online Data Backup (OLDB)**
With this solution, ensure automatic backup and recovery of your data.

**Accidental Damage Protection (ADP)**
Enable device protection due to unintentional electrical surge, liquid spills, drops or bumps, and LCD damage.



**Click here** to explore Lenovo's Security Solutions

# Device Theft/Loss


Modern CPUs are relatively smaller; a plus for users and thieves too. It is not just laptops, but desktops and HD drives are subject to theft too. Another challenge for organizations is loss of a device which in most cases happens for laptops and tablets. In such a situation, it is not only the device which is compromised, but your organization's data in the Cloud is also at risk if your device is not secure enough.

**According to a new survey by NetEnrich, 42% of IT pros said their organizations suffered key corporate data loss from a mobile device.[5]**

Thus, organizations can prevent data breach through:

**Data Encryption**
Technology to encrypt data to prevent hacking and theft.

**Physical Data Theft**
Device innovations that prevent hard drive theft.

**Remote Data Erase**
Technology that allows IT to control devices and erase data remotely.

ThinkCentre M910 Tower

**Discrete Trusted Platform Module (dTPM)**
Encrypt your data, passwords, and more for better security.

**Removable HDD**
Physically remove your hard drive for enhanced security.

**Intel® Active Management Technology (Intel® AMT)**
Remotely erase data from a compromised device to prevent malware attack on other devices.

Powered by Intel®.
Intel Inside®.
Powerful Productivity Outside.

Source:
https://blogs.absolute.com/the-impact-of-corporate-data-loss-from-mobile-devices/

**Click here** to explore Lenovo's Security Solutions

# CONCLUSION

The right endpoint device strategy can benefit your organization at multiple stages:

- Make sure that endpoint devices are not the vulnerable link to your organization's IT infrastructure.
- Complement the employees with the right tools and technology to help them do their jobs productively and efficiently.
- The modern workforce looks forward to technology and devices that complement their work style and isn't dated.

  According to a Microsoft survey, 93% of workers said technology helps them thrive at work and that having modern and up-to-date technology in the office is important.[6]


## So choose with care.

Source:
https://toggl.com/employee-retention-strategies-millennials



**Click here** to explore Lenovo's Security Solutions

# 5 reasons
## why Lenovo is a difference maker

Trusted around the world

Expertise across categories

Confidence in our products

Business-boosting technology

Flexible support network

Powered by Intel®.
Intel Inside®.
Powerful Productivity Outside.

**Brand-Specific Trademark Acknowledgment Line**

Intel and the Intel logo are trademarks of Intel Corporation or its subsidiaries in the U.S. and/or other countries.

www.lenovo.com