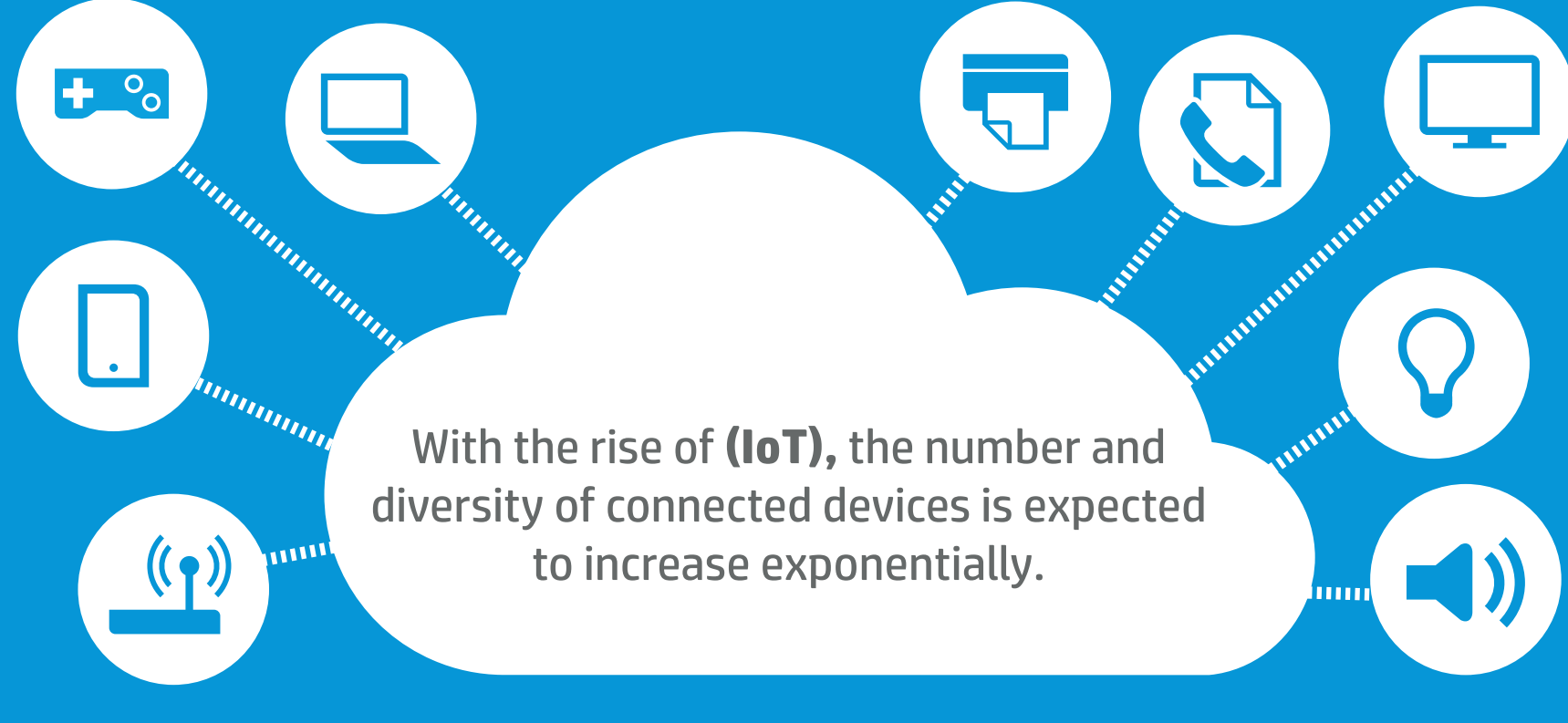




HP Study Reveals 70% of Internet of Things (IoT) Devices Vulnerable to Attack

(IoT) devices averaged **25 vulnerabilities per product**, indicating expanding attack surface for adversaries



26
billion devices
connected to the
internet by 2020

\$300
billion in
incremental value¹

While this increase in **(IoT)** devices promises benefits to consumers, it also opens the doors for security threats ranging from software vulnerabilities to **Denial-of-Service (DOS)** attacks to weak passwords and cross-site scripting vulnerabilities.

HP Fortify on Demand scans found that



Each **(IoT)** device averaged 25 vulnerabilities with a total of **250 concerns** across all tested products.

50% of the devices' mobile apps displayed issues with unencrypted communications to the cloud, internet or local network.



Top 10 security problems with (IoT) devices

1. Insecure web interface
2. Insufficient authentication
3. Insecure network services
4. Lack of transport encryptions
5. Privacy concerns
6. Insecure cloud interface
7. Insecure mobile interface
8. Insufficient security configurability
9. Insecure software
10. Poor physical security

Source: OWASP

More details at:
https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project#tab=OWASP_Internet_of_Things_Top_10_for_2014

Most Common and Easily Addressable Vulnerability Sources Reported:



Vulnerability	Description
Privacy	80% raised privacy concerns regarding the collection of data such as name, email address, home address, date of birth, credit card credentials, and health information
Authorization	80% failed to require passwords of sufficient complexity and length, with most devices allowing passwords such as "1234" or "5678"
Encryption	70% did not encrypt communications to the internet and local network, while 50% of their mobile applications performed unencrypted communications to the cloud, internet or local network
Web Interface	60% raised security concerns with their user interfaces such as persistent XSS, poor session management, weak default credentials and credentials transmitted in clear text
Software	60% did not use encryption when downloading software updates—some downloads could even be intercepted, extracted and mounted, allowing the full code to be viewed or modified

Source: HP Fortify

To protect against security hazards that come along with the rise of **(IoT)**, it is imperative for organizations to implement an end-to-end approach to identify software vulnerabilities before they are exploited. Solutions like **HP Fortify on Demand** enable organizations to test the security of software quickly, accurately, affordably, and without any software to install or manage – proactively eliminating the immediate risk in legacy applications and the systemic risk in application development.

➡ Read the full report at hp.com/go/fortifyresearch/iot



¹ According to Gartner