Hewlett Packard Enterprise

Solution brief

Find weak links in connected devices

HPE Security Fortify on Demand—Securing the Internet of Things

The security testing service for Internet of Things from HPE Security Fortify on Demand enables organizations to get to market quickly—without risking security

The IoT will be the largest device market in the world. We estimate that by 2019 it will be more than double the size of the smartphone, PC, tablet, connected car, and the wearable market combined.[1]

The Federal Trade Commission (FTC) recommends that IoT device manufacturers incorporate security into the design of connected products.[2]

An ecosystem of risk

The Internet of Things (IoT) is poised for exponential growth in the next few years. Companies that were making simple consumer products not so long ago, are now manufacturing devices that are communicating over Web, cloud, and mobile networks. Unfortunately, while the intention of these interconnected devices is to make life easier, they have also created new attack vectors for hackers. And as the type of data that these devices store can now include everything from social security numbers to banking information, their attractiveness as targets will only continue to grow.

With such challenges, how do companies begin to secure the IoT—and without slowing production? Begin by understanding how vulnerabilities in IoT devices can be leveraged to exploit vulnerabilities in other components like applications, mobile devices, and even the server due to their connectivity. Then, engage a partner who can manage the security testing process, alleviating the need to do it in-house.

Devices by themselves can contain a slew of insecurities. IoT security issues are compounded by the number of interconnected points on one device. A couple of security concerns on a single device can quickly turn to innumerable concerns when considering multiple IoT devices in an interconnected system. Considering the intimacy of data that IoT devices have access to, it's important to understand their security risk and react accordingly. Finding a software security partner, who understands the IoT ecosystem, how to uncover vulnerabilities, and manage potential privacy issues and risks, is key.

The right security partner

HPE continues to invest significant effort in the IoT; we understand its value and the security implications it presents. That's precisely why HPE Fortify on Demand team members are **OWASP Internet of Things Top 10 Project leaders** and why our research team continues to test and report on IoT systems. Moreover, Fortify is a Gartner Magic Quadrant AST leader[3] and has the application security testing assessment expertise needed to help secure your Internet of Things solutions: Web, cloud, and mobile applications across network, client, and server surfaces. Fortify on Demand leverages our dynamic and static security testing technologies through a global infrastructure that's augmented by an experienced team of researchers, testers, and software engineers.

The testing process

Our team of security testers can thoroughly assess your complete IoT solution before going to market (using the Internet of Things Top 10 vulnerability categories) or we can test according to your needs—it's your choice.

[1] "The Internet of Things report: How the market will grow across the home, enterprise, and government sectors", John Greenough, BI Intelligence, 2015

[2] "Security is a must for the Internet of Things", Terrell McSweeny from FTC, Re/code, January 2015

[3] HPE Security Fortify: A leader in 2015 Gartner Magic Quadrant for Application Security Testing.

We perform application security testing to assess the entire ecosystem to prevent weak links—not only within the device, but also on the Web, mobile, cloud, and network components. As we do with our full mobile stack testing, we can leverage each component to test the others.

As part of the Fortify IoT security testing service, our team can:

- Conduct an automated and manual security test, covering device, network, Web app, mobile app, and cloud components
- Provide results in a consolidated report noting critical findings
- Work with you to prioritize remediation tasks
- Perform the necessary remediation scans to validate fixes

For more information
To learn more about HPE Security Fortify on Demand managed security services, contact your HPE representative or email **fodsales@hpe.com**.

Sign up for updates

★ Rate this document

⚠ 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: **owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project#tab=OWASP_Internet_of_Things_Top_10_for_2014**

Figure 1: OWASP Top 10 for Internet of Things

Testing details

For IoT devices, HPE Security Fortify performs the following activities:

- Conduct static analysis on the IoT application
- Perform dynamic analysis on IoT devices and application based on the categories in the OWASP Top 10
- Remove all vulnerabilities that can be validated as being false positives
- For mobile applications, HPE Security Fortify performs the following mobile security testing activities:
- Conduct static analysis on the mobile application
- Perform dynamic analysis on the mobile application
- Remove all vulnerabilities that can be validated as being false positives

For Web server applications, HPE Security Fortify performs the following security testing activities:

- Perform static analysis on the Web application
- Identify URL and credentials of Web application to be assessed
- Perform an automated dynamic assessment of the Web application. If an automated assessment cannot be performed, a manual dynamic assessment should be executed against the entire application
- Test the site manually using a combination of open source tools and custom scripts to identify False-Negatives that may have been missed in the dynamic test
- Remove all vulnerabilities that can be validated as being false positives

Benefits

Build security into your smart devices and patch up all the loopholes before release.

- Comprehensive security testing across device, network, Web app, mobile app, and cloud
- Time to market—without risking security
- Fully managed service—no security experts to hire, train, and retain—and it need not be done in-house

Learn more at
hpe.com/software/fod

Hewlett Packard
Enterprise