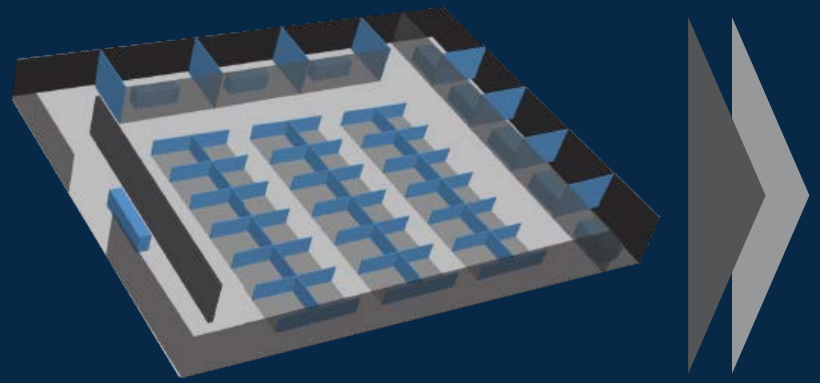
Black Hat Web Series
BleedingBit and IOT devices

Ron Chestang
Senior Print Security Advisor

Future Workplace

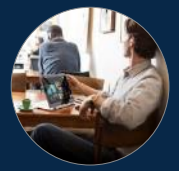
Driven by changes in how people are working – and what they need from the office environment

Traditional office

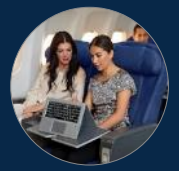


Work outside the traditional office increasing

Home

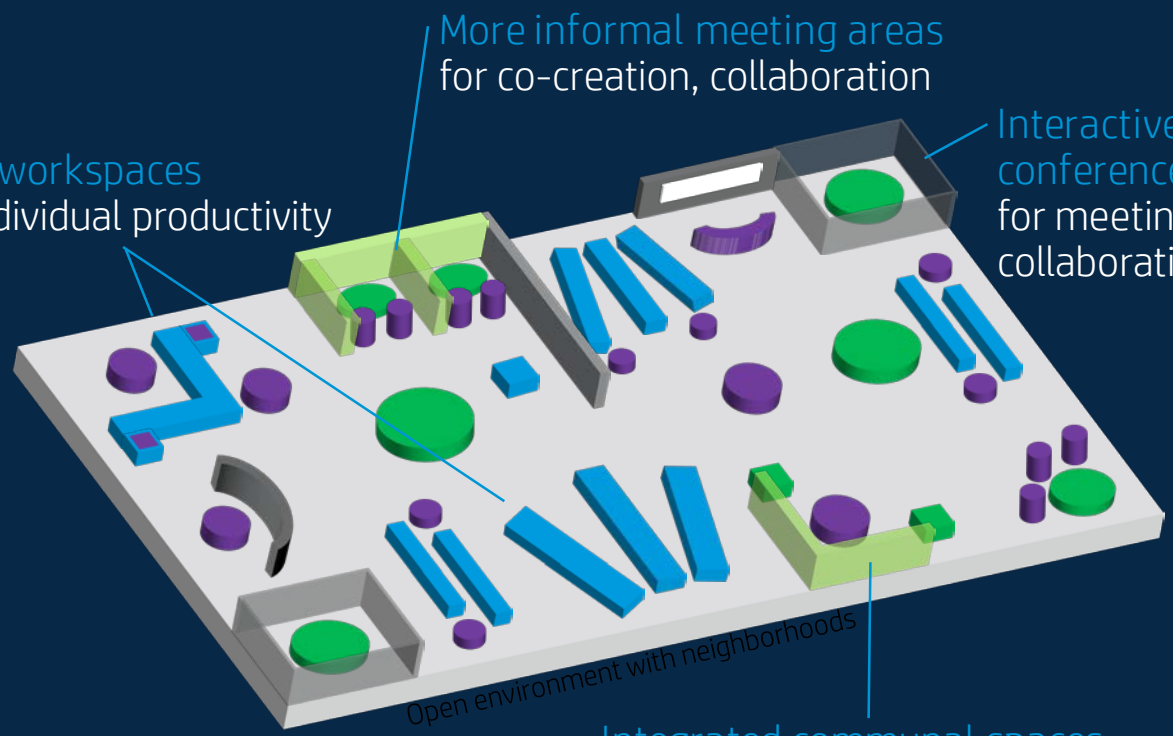


Cafe/public space



Airplane

Emerging office



Today's Meeting Room Technology

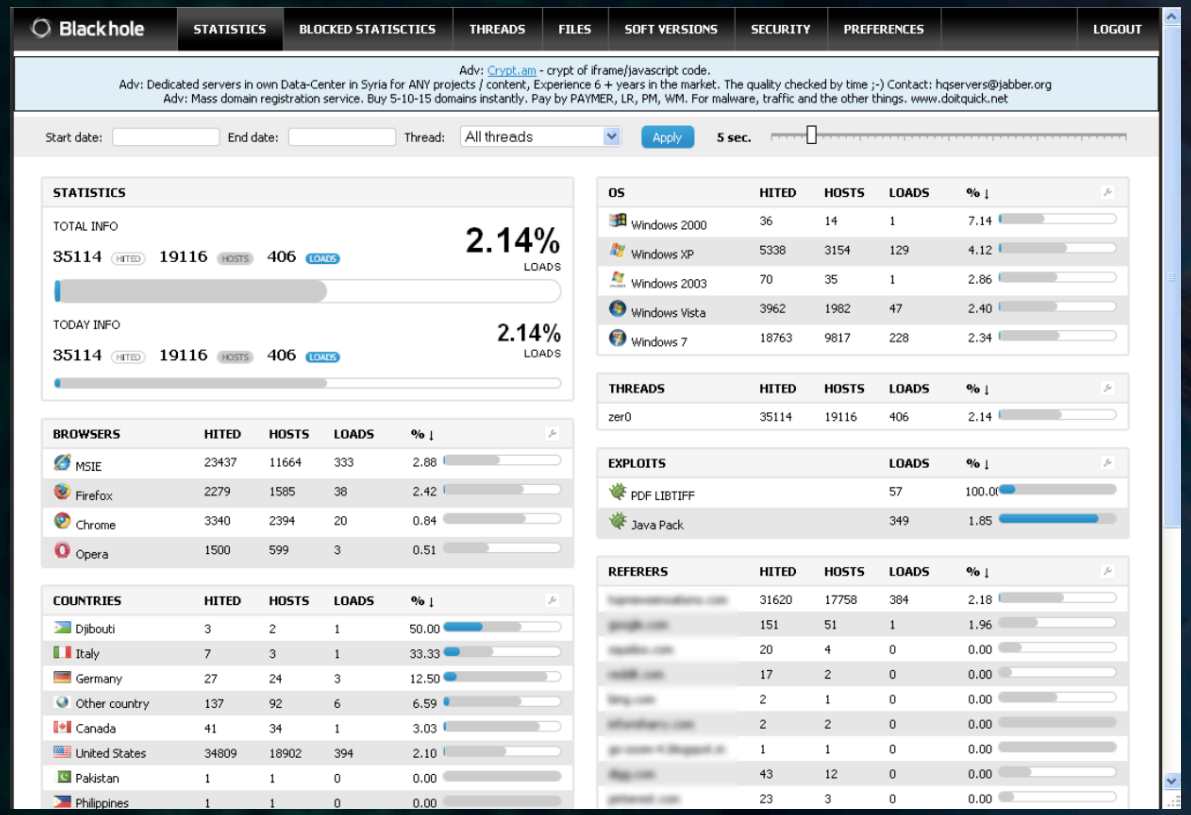
The market is busy innovating, and technology options are multiplying

Simplified Projection ⟷ Team collaboration devices

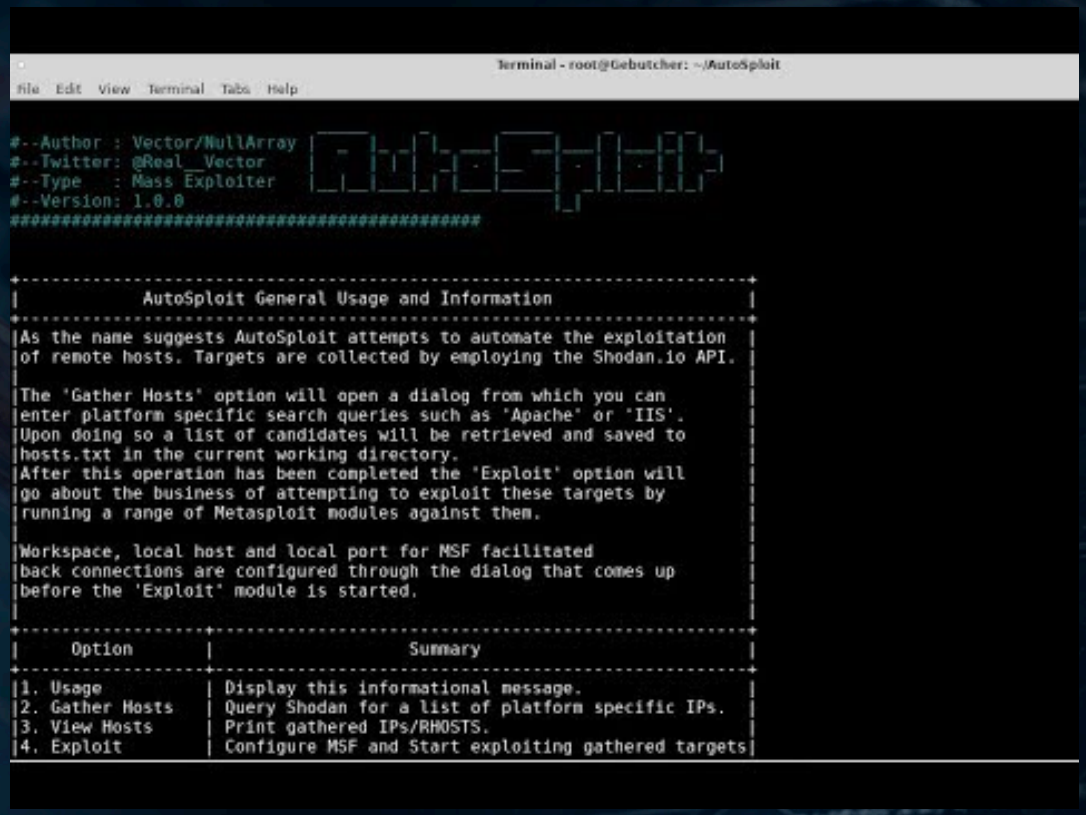
 Barco Clickshare, Intel Unite, SmartBoard, Cisco Spark, MSFT Surface Hub

The Changing Threat Landscape

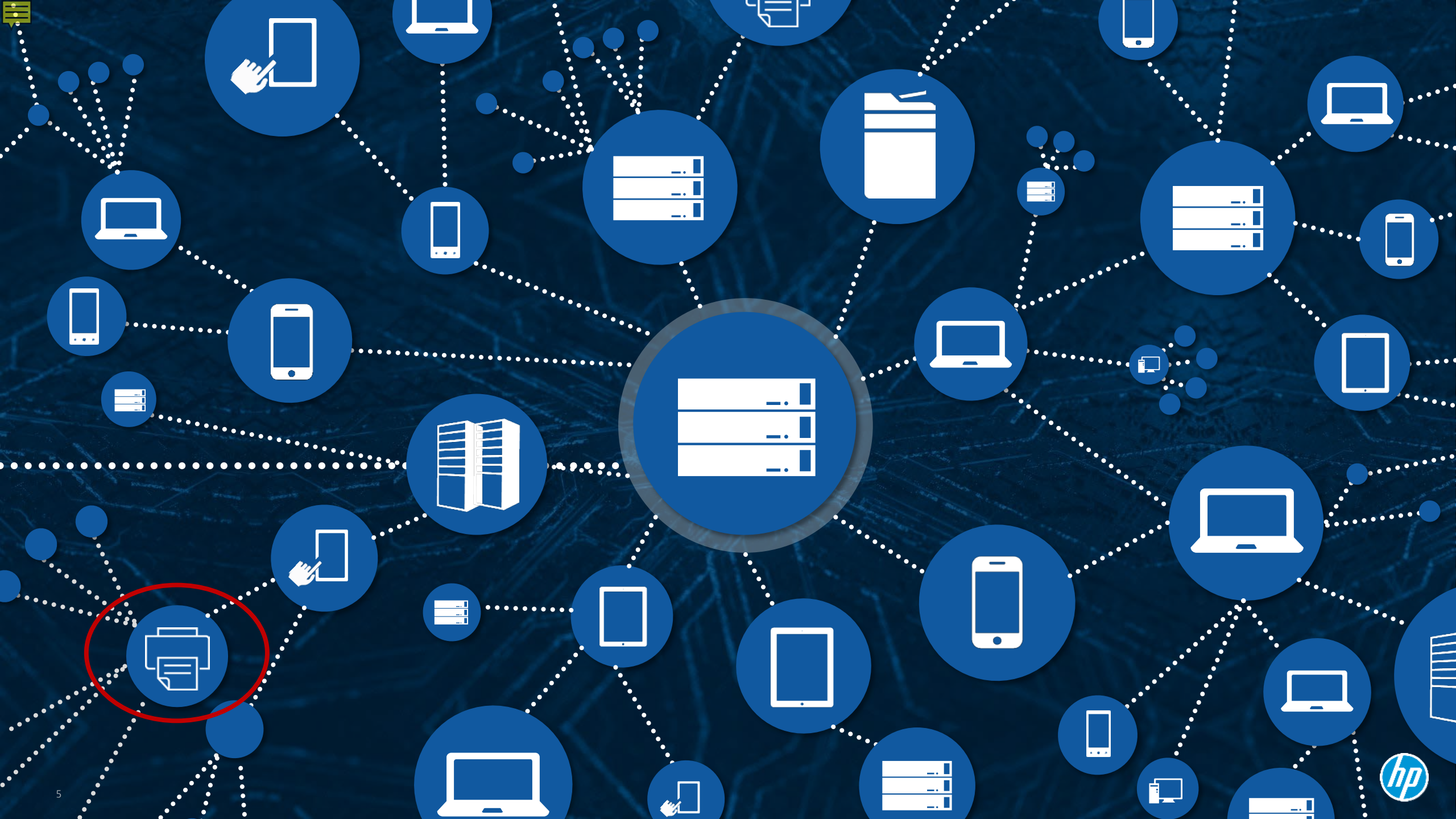
Commercialization of attack software



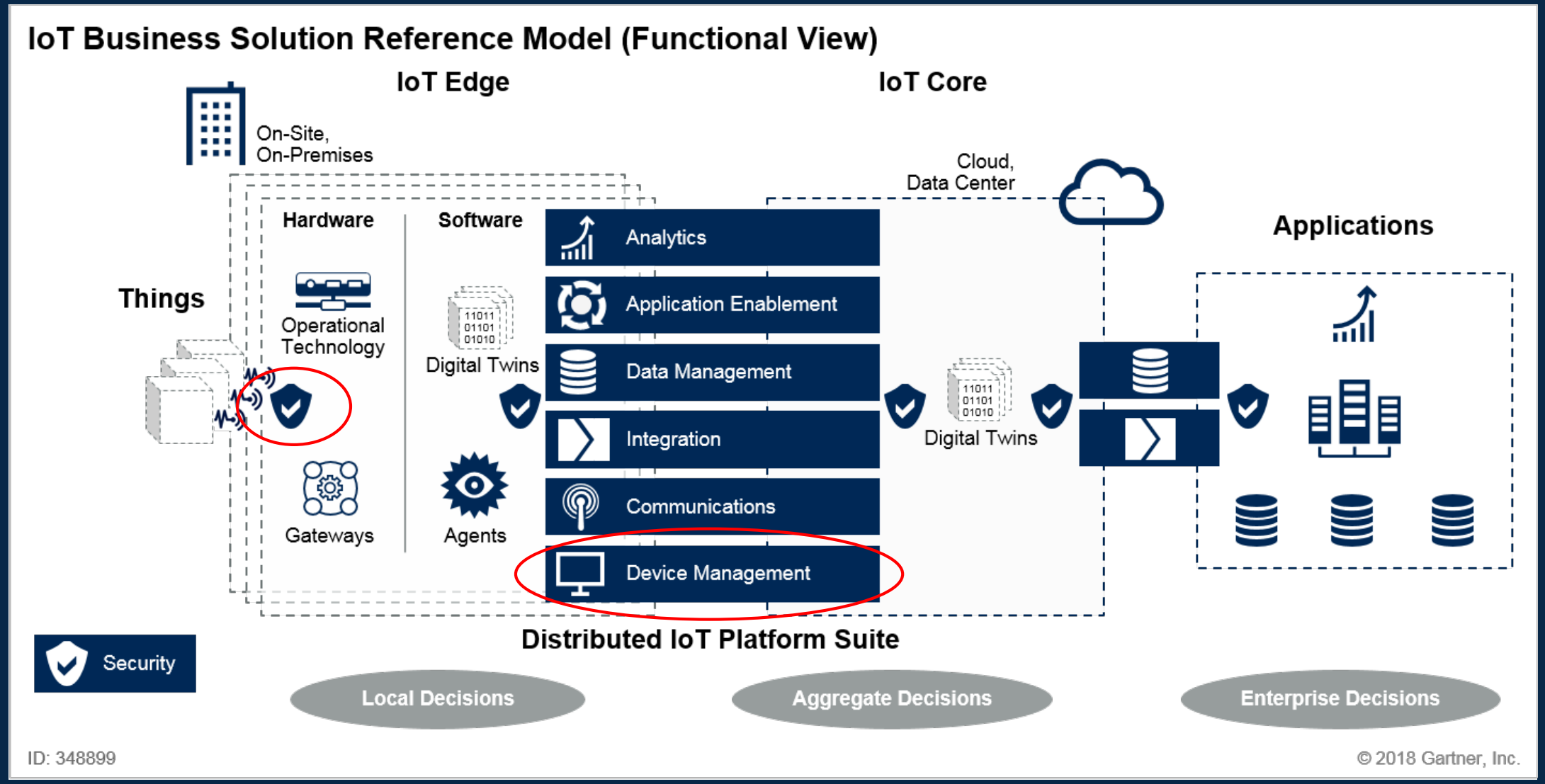
Black-hole Exploit Service Command Console



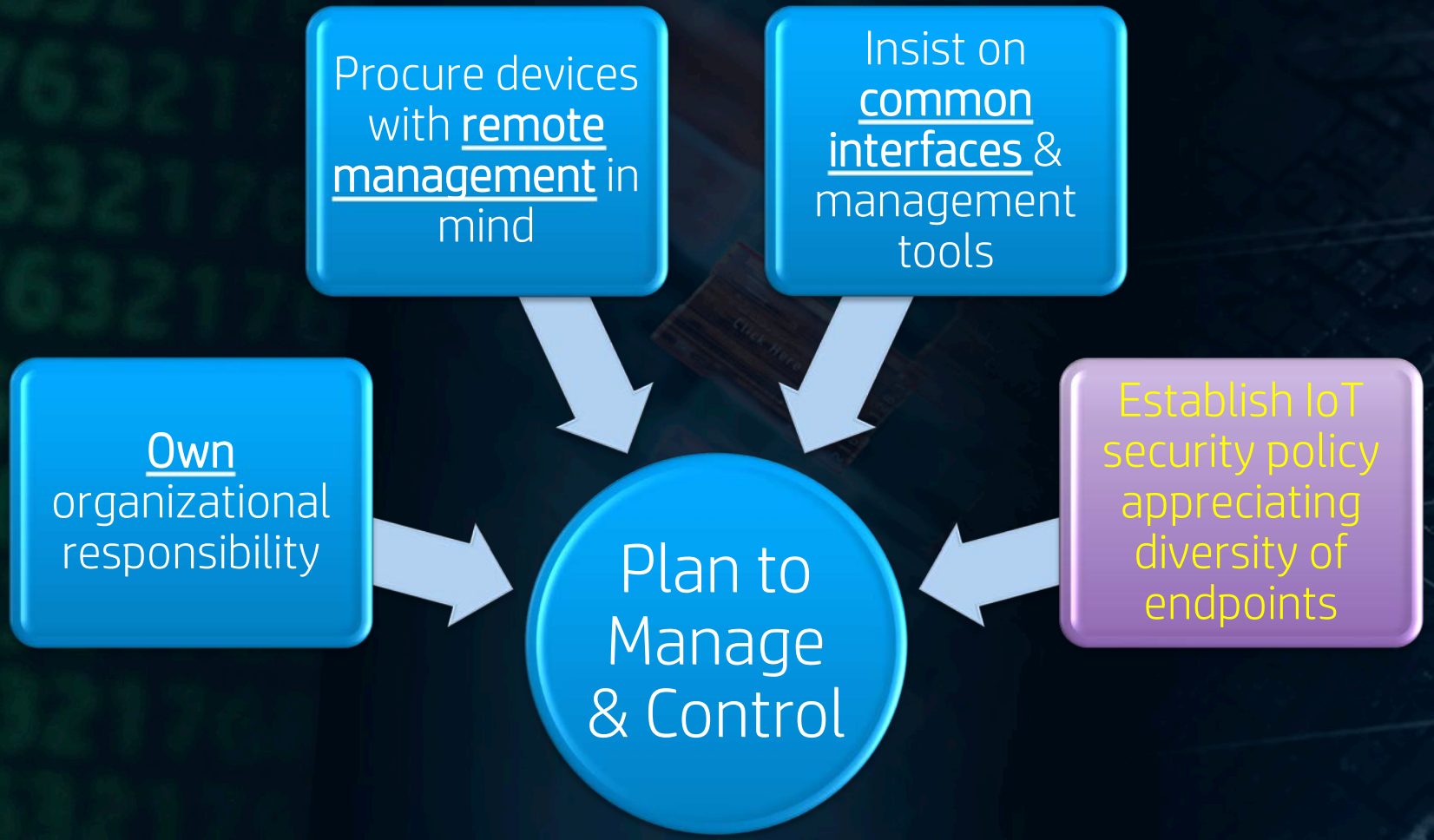
Autosploit loader



Context setting: Gartner IoT Reference Model



Required Next Steps

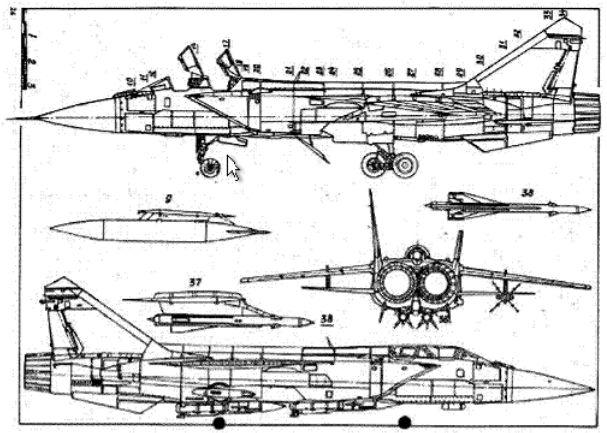


Print jobs on network

Network Access

Filter: tcp.port==9100 && ip.addr==192.168.0.51

Confidential Information:



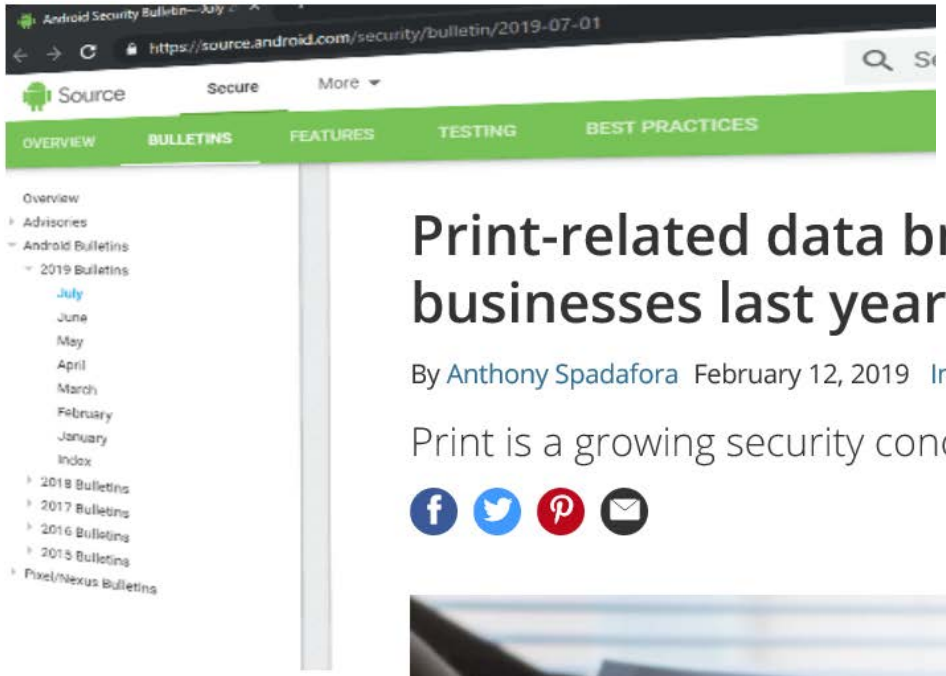
Payroll information:
John Doe $32,000

Destination
92.168.0.51
92.168.0.51
92.168.0.109
92.168.0.51
92.168.0.51
92.168.0.51

WIRESHARK

Android July 2019 Security Update Patches 33 New Vulne

July 02, 2019 Swati Khandelwal



https://thehackernews.com/2019/07/a
update.html?utm_source=feedburner&
+Cyber+Security+Blog%29&_m=3n.00

Amazon Admits Alexa Voice Recordings Saved Indefinitely

mazon-admits-alexa-voice-reco lings ave nde tel 4622

Print-related data breaches affected 60% of businesses last year

By Anthony Spadafora February 12, 2019 Internet

Print is a growing security concern

https://www.techradar.com/news/print-related-data-breaches-affected-60-of-businesses-last-year

NSA Presentation at RSA 2018

- 93% of 2017 incidents preventable with best practices
- In 2018, NSA stated 90% of cyber incidents due to human error

GOOD CYBER HYGIENE

United Kingdom National Audit Office

- 80% of cyber attacks preventable with basic cyber hygiene

BASIC CYBER HYGIENE

Key Takeaways

1. Every purchase decision is a SECURITY decision
2. CIO & CISO must get involved early in all endpoint procurement to ensure and drive security requirements into the endpoint procurement decisions
3. On-going assessment and monitoring of endpoint risks
4. Increase data controls for endpoint devices
5. Data breach monitoring and reporting for all endpoints
6. On-going evaluation and monitoring of endpoint protections deployed
7. Treat endpoint devices as the first line of defense
8. Include all endpoint devices in your policies and security action plans

Thank you

Ronald.Chestang@hp.com

www.hp.com/thewolf
www.hp.com/reinventsecurity