



# Trends in CyberSecurity

Madalin Vasile

Manager Systems Engineering, Fortinet

# Network Security Leader

Fortinet is #1 in Security Appliance Shipments for 6 Consecutive Years and it is #2 in Firewall, UTM and VPN Revenue (according to IDC,2019).

Its broad portfolio of solutions spans Network, Infrastructure, Cloud, and IoT Security.



**\$13B Mkt Cap**



**~\$1.8B - 2018**  
(revenue)



**400,000+**  
Customers



**4.6M+ Appliances**  
**Shipments Worldwide**  
(+30% units WW)

# 70% of F100 Are Fortinet Customers

4 of 4



Telco

9 of 10



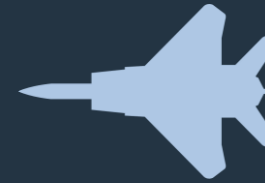
Financials/  
Banking

11 of  
13



Retail

4 of 5



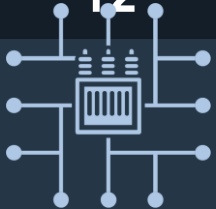
Aerospace/  
Defense

3 of 5



Energy

10 of  
12



Technology

12 of  
15



Healthcare

3 of 5



Transportation

9 of 11



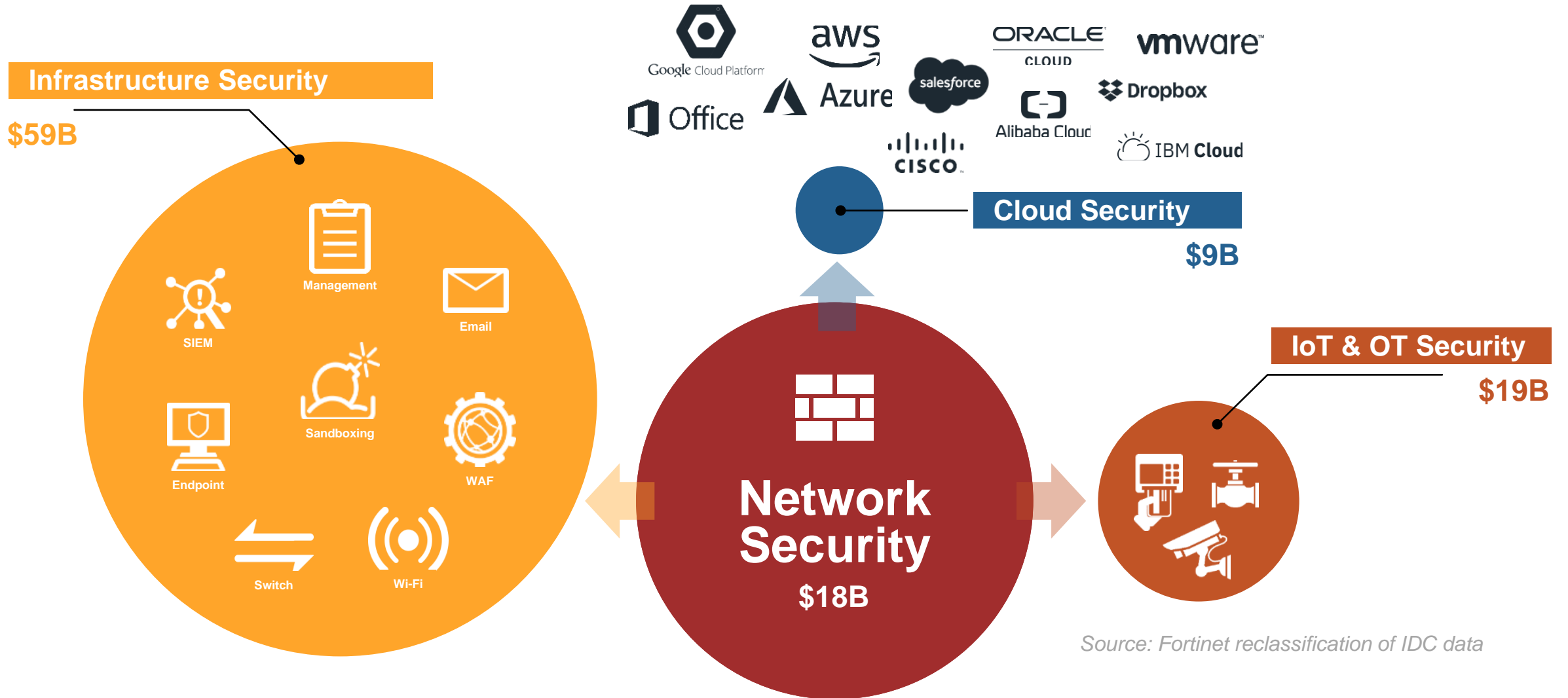
Financials/Ins

3 of 5



Food/Bev

# Fortinet Focus on 4 Security Markets



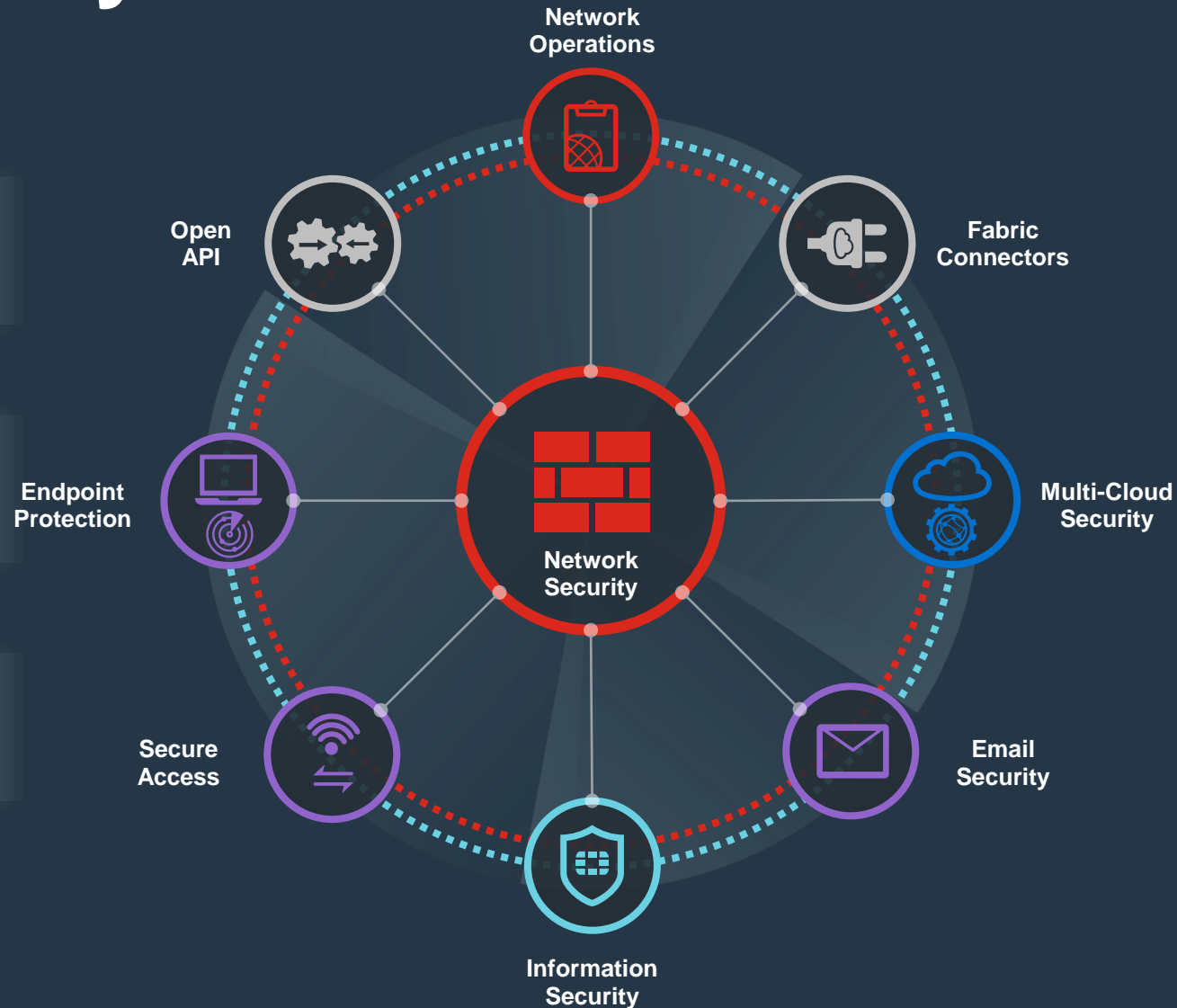
# Fortinet Security Fabric

- Network Security
- Multi-Cloud Security
- Infrastructure Security
- Ecosystem
- Information Security

**BROAD** visibility of the entire digital attack surface

**INTEGRATED** Protection across all devices, networks and applications

**AUTOMATED** Operations and continuous trusted assessment



# EXPAND



## Cloud

## SDN

## CASB

## SD-WAN

## UEBA

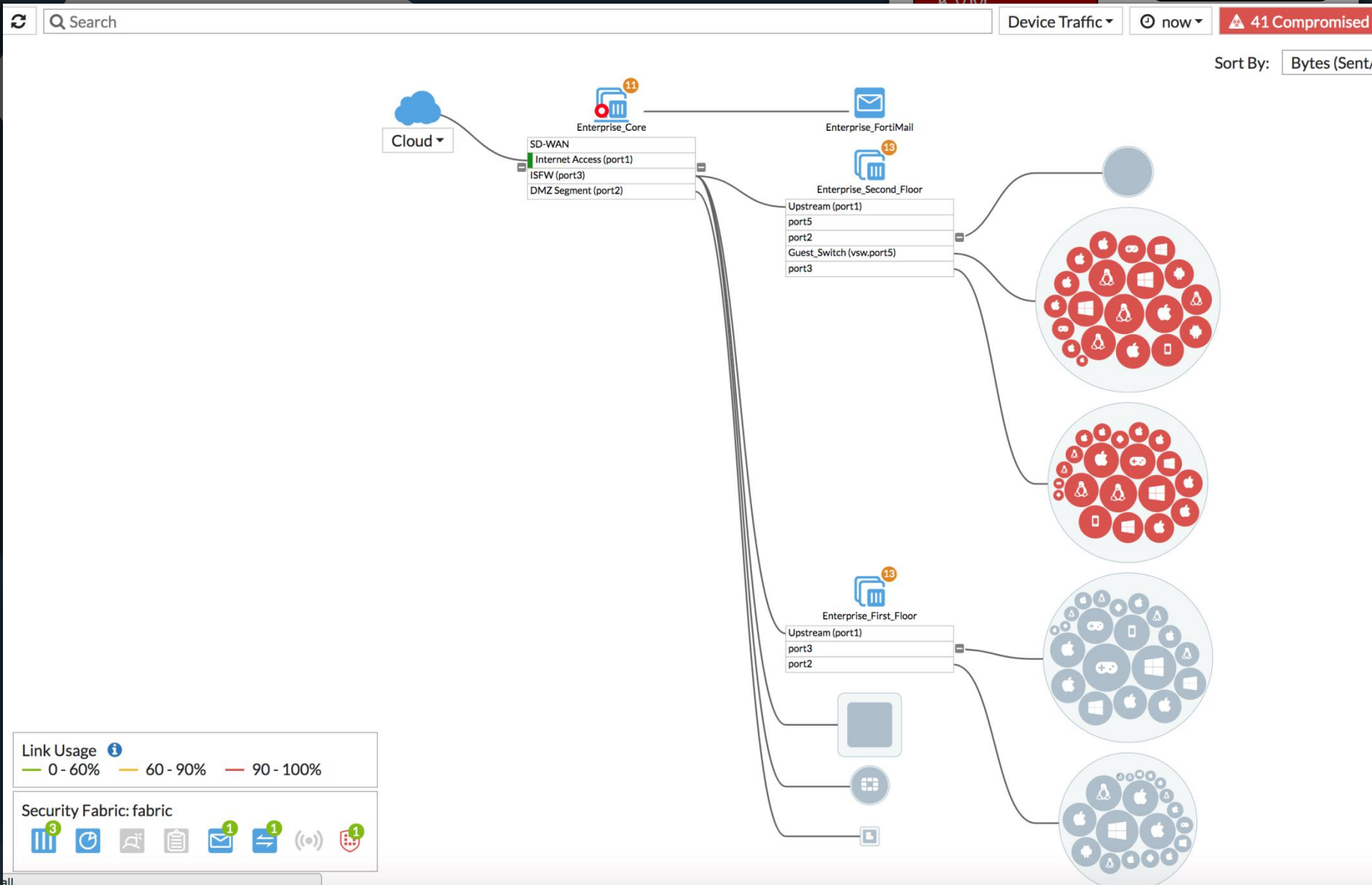
## Single Pane

FORTINET

AWS  
Azure  
Google  
Oracle  
VMWare  
KVM

Acceleration

Dynamic  
Policies



# MEASURE



## Integrated Measurement

## Fabric-wide Reporting

## Multi-product

## Industry, Region & Size Comparison

## How Secure Am I?



Map

Firmware and Subscriptions

# DETECT



APT

IOC

3<sup>rd</sup> Party

Vulnerability

UEBA

Weakness

The screenshot displays the Fortinet Security Fabric interface. At the top, there is a search bar and navigation tabs for 'Access Device', 'No Access Device', and 'Device Traffic'. The main area shows a network topology with nodes for 'Cloud', 'Enterprise\_Core', 'Enterprise\_Second\_Floor', and 'S108DWWA9XDVG54'. A central pop-up window provides details for user 'jlauer' (10.100.94.100), including their email, phone number, device 'Jake-PC', status 'Registered', vulnerabilities (5, 3, 7), MAC address, interface 'port2', OS 'Linux Ubuntu / 16.04', and topology path. To the right, a panel titled '41 Compromised Hosts' lists MAC addresses and 'Compromised' status for several hosts, with a 'Quarantine' button for each. The bottom of the interface shows a 'Security Fabric: fabric' status bar with various icons.



# FortiClient Automatic Quarantine (FOS 6.0.0)

- Based on IOC level (medium/high)
- Automatic FortiClient quarantine via EMS

The screenshot displays the 'New Automation Stitch' configuration interface in the FortiGate EMS. The left sidebar shows the navigation menu with 'Automation' selected. The main content area is divided into several sections:

- Name:** A text input field.
- Status:** Radio buttons for 'Enabled' (selected) and 'Disabled'.
- FortiGate:** A dropdown menu showing 'All FortiGates'.
- Trigger:** A row of eight circular icons representing different triggers: Compromised Host (highlighted with a green checkmark), Event Log, Reboot, Conserve Mode, High CPU, License Expiry, HA Failover, and Configuration Change.
- IOC level threshold:** Radio buttons for 'Medium' and 'High' (selected).
- Action:** A row of seven circular icons representing different actions: Email, FortiExplorer Notification, Access Layer Quarantine, Quarantine FortiClient via EMS (highlighted with a green checkmark), IP Ban, AWS Lambda, and Webhook.
- Minimum interval (seconds):** A text input field with the value '0'.

# AntiMalware Protection

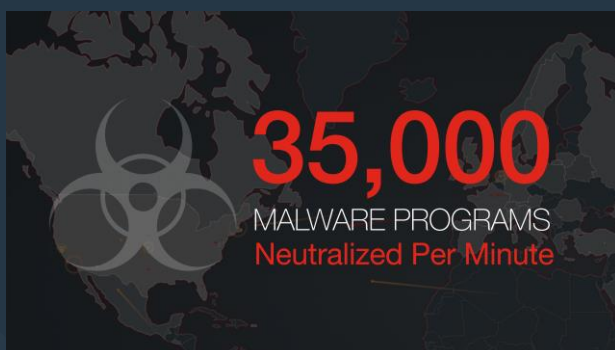
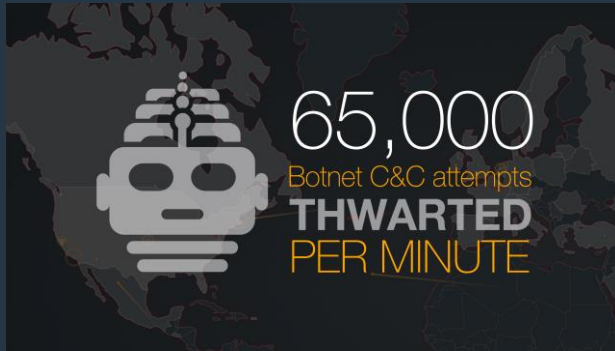
- New GUI for Windows, Mac and Linux
- Anti-Virus Protection
- Anti-Exploit GUI
- Sandbox Detection
- Removable Media Access Analysis
- Vulnerability Detection

The screenshot displays the FortiClient interface for Anti-Virus Protection. The top window shows the user profile 'Kunal Marwah' and the 'Anti-Virus Protection' toggle switch. The main window displays the 'Scan Complete' results. A large red shield icon indicates a 'Critical' severity level. Below the shield, a bar chart shows the distribution of vulnerabilities: 5 Critical, 3 High, 2 Medium, and 1 Low. The scan duration is 01:30:45. The total vulnerabilities found are 68, and the critical vulnerabilities found are 0.

Severity	Count
Critical	5
High	3
Medium	2
Low	1

Duration: 01:30:45  
Total Vulnerabilities Found: 68  
Critical Vulnerabilities Found: 0

# FortiGuard by the numbers Q4 2018



**FORTINET**<sup>®</sup>