Work from home risk mitigation

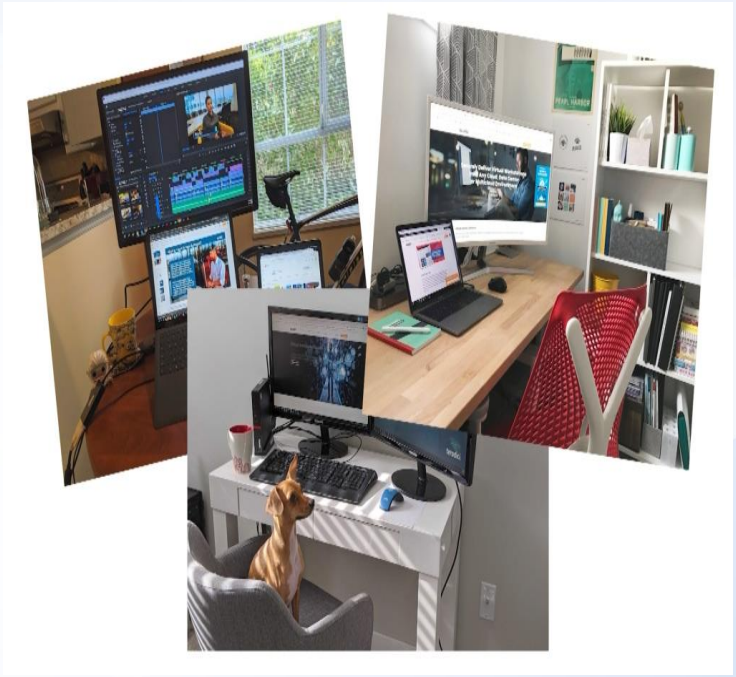
FireEye WFH Platform

Ahmed Tharwat

Senior Sales Engineer – MEA

Work form home Risks

- Uncontrolled access on the Internet
- No visibility on malicious activity on the remote endpoint
- VPN not connected 24/7
- Infiltration of threat actors through VPN
- Longer IR process and forensics investigation
- Physical isolation of the infected endpoint
- No visibility to the employee's productivity
- Novel of Coronavirus and the elevation of threat actors' activities



Required Capabilities

Protection from new threats in a timely manner

Detect threats across all remote endpoints regardless VPN is on or off .

Respond to threats remotely and in an efficient way

Remote isolation of infected machines

Secure user Internet access from any location, on any device, with and without VPN

FireEye Innovates to Combat Cyber Threats

0-Day Web Protection

Content Filtering & Policy Enforcement

Network Flow Generation & Tracking

Machine Learning

Indicators of Compromise

Agent Modules

Our **real-time knowledge** of the threat landscape ensures that FireEye solutions are built to **directly address** today's threats and the techniques employed.

FireEye WFH Platform at a Glance

How We Do It

Protect

- Malware Protection
- MalwareGuard
- ExploitGuard
- 0-Day Web Protection
- Intrusion Detection & Prevention

Detect

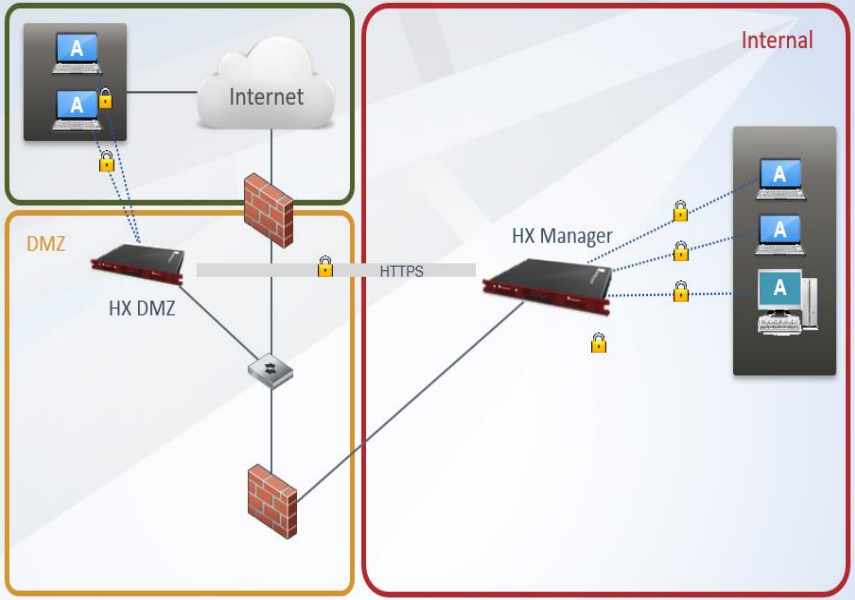
- Indicators of Compromise
- Enterprise Search
- Investigative Data Acquisition

Respond

- Auto Containment
- Remote network response
- Respond at scale

Endpoint Security Simple, Flexible and rapid deployment

- Pre-built virtual machines plug and play
- HX DMZ to manage all remote endpoints without the need of VPN
- A Cloud manager option is available if no restrictions
- The solution will be fully operational in maximum 5 business days from placing the PO



Cloud platform iBoss + FireEye Simple, Flexible and rapid deployment

- Cloud Instance plug and play
- Agent ready to be installed on Windows, MAC, iOS, and Android
- Web filtering, application control, double Intrusion Prevention System, Bandwidth Optimization, Data Loss Prevention policies and more.
- The solution will be fully operational in maximum 5 business days from placing the PO

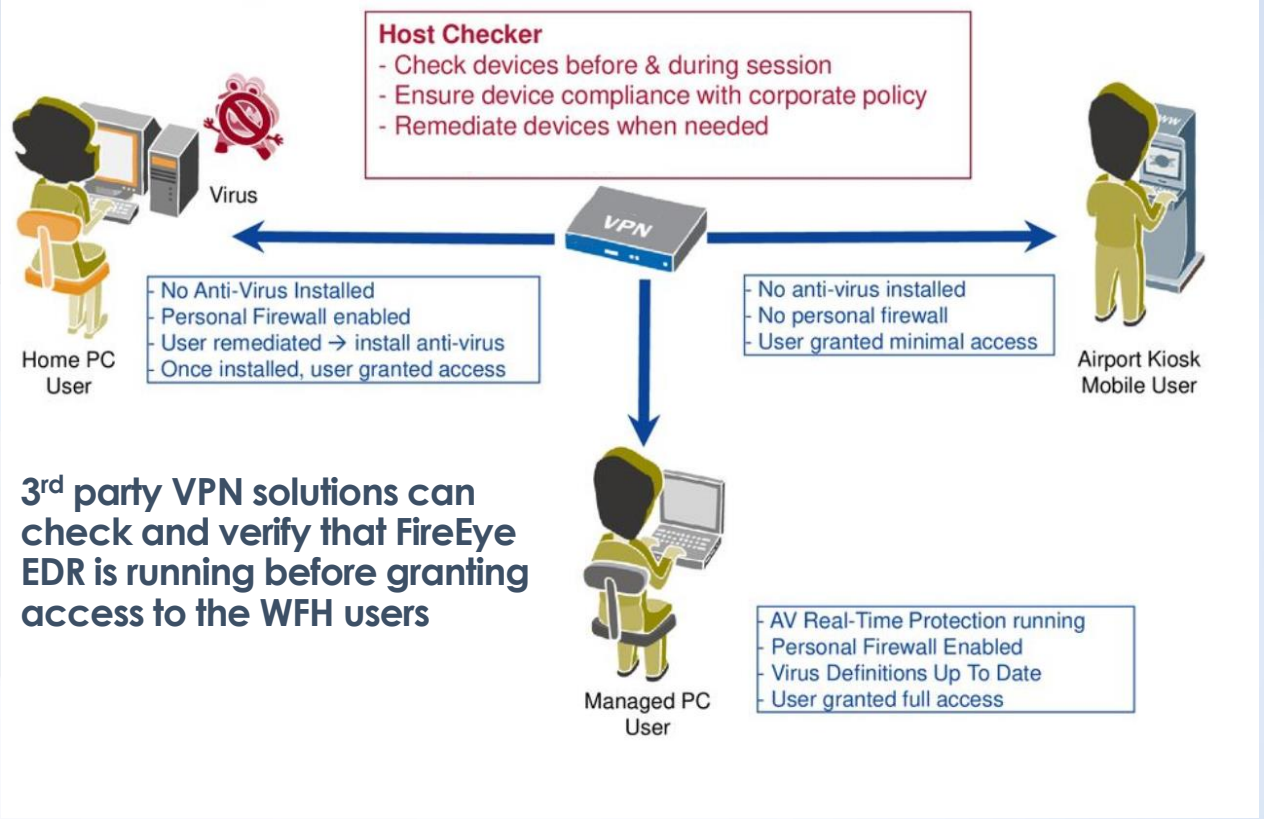
Host checking before granting VPN access with FireEye Endpoint Security

FireEye endpoint

Access granted

No FireEye endpoint

Access Restricted



Cloud Gateway

Features Delivered

- Malware Prevention
- Malware Breach Detection
- Intrusion Detection & Prevention
- Content Filtering & Policy Enforcement
- Data Exfiltration Containment
- EOL Browser Protection & Management
- EOL OS Protection & Management
- Network Flow Generation & Tracking
- Advanced Cloud Controls
- High-Risk Device Locking
- CASB & Application Controls
- SSL MITM Decryption
- Auto-Depositing Malware into Sandbox
- Device Tracking including machine names
- User Tracking including usernames
- Integration with Directory Services/AD
- Proxy

Core Capabilities

- Scan data for malware, breaches and data loss
- Cache web content
- Reassemble data streams and prevent unwanted cloud data transfers

Advantages

- Cache and analyze files for malware and data loss prevention, including: PDF, Outlook data files, and zip files.
- Full visibility across the entire data stream to detect and block the evasive malware that causes data breaches.
- The ability to monitor across all protocols to ensure that applications such as TOR and Torrent aren't being used as conduits for evasive malware.
- Can dynamically detect highly evasive applications that circumvent and evade your security.
- Monitors across all traffic to detect anomalies, alert IT and automatically contain data exfiltration before loss occurs.

Cloud Reporting

Features Delivered

- Drill-Down Reports
- Real-time Dashboards
- Report Schedules
- Anonymization of PII in logs, if needed
- Incident Response Center
- Detailed Event Logs
- Bandwidth Consumption Reports
- Risk Reports
- Encrypted Cloud Backup
- SIEM Integration - Splunk, QRadar, Syslog

Core Capabilities

- Store security log events, generate drill-down reports and provide permanent data storage

Advantages

- Live Bandwidth Dashboard and Dynamic Plotter gives you granular visibility and control over bandwidth consumption with exclusive features such as geotagging, reverse-geomapping of IP address to organization and user, and map overview.
- Live Threat Dashboard provides immediate insight into threats, suspicious events, and liability risks that can result in AUP or regulatory violations, data loss or costly litigation.
- Stream Logs to Any SIEM directly from the cloud without the need for virtual appliances as required by alternative cloud platforms.
- Web Security Reporting and Log Management tools go beyond standard static reporting, to deliver proactive indexing and archiving that enable instant drill-down access to user activity, threats and bandwidth consumption.

FireEye Endpoint Security with Managed Defense

FireEye Endpoint

FireEye Managed Defense

- Analyst-driven detection and response
- Systematic, proactive hunting
- Proprietary investigative techniques
- Detailed investigation reports with recommendations
- Visibility to emerging threats
- Threat assessment managers provide insight on risks

FireEye Endpoint Security with Expertise on Demand

FireEye Endpoint

Expertise on Demand

- Access to proven skills and threat insight
- Increases situational awareness
- Training and consulting services
- A single, trusted partner with unrivaled breadth and depth of cyber security tools and techniques

FireEye to address the WFH risks

Outcomes

- Detects all threats on remote endpoints
- Control all the web traffic
- Advanced remote IR capability
- Embedded threat intelligence that can detects Threat actors IOC's/TTP's
- Efficient remote hunting and investigation
- Remote isolation of infected machines
- Integration with the current VPN solution
- A quick and simple deployment
- Monitor the endpoints while VPN is off
- Monitor your employee's productivity

FIREEYE™

Thank you

Ahmed Tharwat
Senior Sales Engineer – MEA