CISO MAG

beyond cybersecurity

Volume 3 | Issue 10 | November 2019

INSIDE ▸

REPORT ON

**Summit & Awards – Middle East**

PG 125

ENDPOINT SECURITY

# POWER LIST

SHOWCASING THE POWERHOUSES IN CYBERSECURITY

# INDEX

Volume 3 | Issue 10

# EDITOR'S NOTE

Endpoint security is not new to enterprises. With the proliferation of devices (official and personal) on enterprise networks, securing the endpoints became a priority for organizations years ago. And now, there is a huge demand for endpoint security solutions. Mordor Intelligence estimates the endpoint detection and response (EDR) market will grow to US$ 3,443.64 million by 2024, growing at a CAGR of 22.97 percent, between 2019 and 2024.

To understand how companies are consuming endpoint protection solutions, *CISO MAG* conducted a multiple-choice survey in October 2019. The results of this global survey form the basis of our research and conclusions on the state of endpoint security.

Some key findings, as you will read in our cover story: half of all companies (53.19%) that participated in this survey are using both EPP (Endpoint Protection Platform) and EDR solutions. An integrated solution that offers the best of both worlds is the preferred choice. Two-thirds (62.55%) said their endpoint solution included Managed Endpoint Detection Services. So, many are opting for specialized cloud-based services to monitor and manage endpoints with advanced threat protection.

In this issue, you will also find our Power List of market-leading endpoint security solutions. The Power List is put together by the *CISO MAG* editorial team.

*CISO MAG* also acknowledges institutions and individuals for their achievements and contributions to cybersecurity. We've included a section with a report of the *CISO MAG* Summit & Awards – Middle East. The event was conducted on 21 October, 2019 in Dubai.

Tell us what you think of this issue. If you have any suggestions, comments or queries, please reach us at editorial@cisomag.com.

**Jay Bavisi**
Editor-in-Chief

CISO MAG
beyond cybersecurity

Volume 3 | Issue 10
November 2019

Editorial
International Editor
**Amber Pedroncelli**
amber.pedroncelli@eccouncil.org

Principal Editor
**Brian Pereira**
brian.p@eccouncil.org

Senior Feature Writer
**Augustin Kurian**
augustin.k@eccouncil.org

Feature Writer
**Rudra Srinivas**
rudra.s@eccouncil.org

Technical Writer
**Mihir Bagwe**
mihir.b@eccouncil.org

Media and Design
Media Director
**Saba Mohammad**
saba.mohammad@eccouncil.org

Sr. Graphics Designer
**Sameer Surve**
sameer.s@eccouncil.org

UI/UX Designer
**Rajashakher Intha**
rajashakher.i@eccouncil.org

Management
Executive Director
**Apoorba Kumar***
apoorba@eccouncil.org

Senior Director,
Compliance & Governance
**Cherylann Vanderhide**
cherylann@eccouncil.org

Deputy Business Head
**Jyoti Punjabi**
jyoti.punjabi@eccouncil.org

Marketing and Business Development Officer
**Riddhi Chandra**
riddhi.c@eccouncil.org

Digital Marketing Manager
**Jiten Waghela**
jiten.w@eccouncil.org

Publishing Sales Manager
**Taruna Bose**
taruna.b@eccouncil.org

Technology
Director of Technology
**Raj Kumar Vishwakarma**
rajkumar@eccouncil.org

* Responsible for selection of news under PRB Act. Printed & Published by Apoorba Kumar, E-Commerce Consultants Pvt. Ltd., Editor: Rahul Arora.

CISO MAG

beyond cybersecurity

# POWER LIST

SHOWCASING THE POWERHOUSES IN CYBERSECURITY

FOR MORE DETAILS:

## JYOTI PUNJABI

Deputy Business Head - CISO MAG
☎ +91 9963654422
✉ jyoti.punjabi@ecccouncil.org

## TARUNA BOSE

Publishing Sales Manager - CISO MAG
☎ +91 7838483171
✉ taruna.b@eccouncil.org

Volume 3 Issue 10

Volume 3 Issue 10

# THE NEED FOR LAYER 8:

## Why the OSI Model Isn’t Enough for Application Security

John Adams,
Chief Executive Officer of Waratek

For the modern business, application security is an essential concern. Every company uses a variety of web, software, and mobile applications in order to serve customers and execute internal functions. Unfortunately, far too many of these applications are subject to critical vulnerabilities as a result of insecure coding practices, flaws in third-party libraries, and changes in the cybersecurity threat landscape.

The effects of web application vulnerabilities have been tumultuous and widespread. We've seen huge global corporations fall victim to a single vulnerability with disastrous results. Equifax remains the poster child for application security awareness. The original September 2017 breach occurred when a vulnerability in the Apache Struts tool (used by numerous corporations and government organizations) was compromised by hackers. By the time the breach was discovered, the personal data of 143 million Equifax customers was accessed. A settlement with state and federal investigations could ultimately cost the company as much as $700 million dollars. Meanwhile, more than 200,000 people have already signed a petition against the deal demanding Equifax face stronger accountability.

> Equifax is not the only company to fall victim to a web application vulnerability. The list of victims crosses a wide array of industries including tech, financial and education, among others, with names like Facebook, Capital One and Georgia Tech making headlines for large-scale breaches.

If incidents like this can happen at this level, all businesses should be aware that they too could become victims of an application breach. The warning signs are all there. Research shows that 71 percent of applications in product contain at least one high-severity application flaw, with the average number of high-severity flaws in production applications being five. With numerous glaring vulnerabilities, it's no wonder that web applications remain the primary target for attackers.

So what can be done to protect businesses from falling victim to web application breaches? Perhaps a new path forward is needed. Current solutions for keeping applications secure have been developed by the network engineering community, not the application engineering community itself. In fact, far too many companies have little or no application security at all—opting instead to deploy network security controls around the application—essentially perimeter protection.

This may be due, in part, because many vendors and companies design their security posture around the Open Standard Interconnection model (OSI) model. Popularized in the mid-80's by the International Standards Organization (ISO), OSI is conceptual model to promote interoperability between computing systems. This model sets out a construct of standard network protocols divided into seven layers that still govern how all internal and external networks communicate and function, including how they are secured.

## The OSI Networking Model

The OSI (Open Systems Interconnection) networking model describes how applications exchange information over a network by separating these communications into seven different "layers." While each layer is independently developed, the OSI model anticipates that each layer only communicates with the layer above and below it as information passes through the layers.

According to the OSI model, the seven layers of networking are:

**APPLICATION** This layer specifies how users interact with the data on the network through the form of interfaces and protocols.

**PRESENTATION** This layer translates data between the application and the network, performing functions such as encryption, compression, and string conversion.

This layer manages the connection between different systems (known as a session).

**TRANSPORT** This layer defines the protocols and port numbers that hosts on the network use to communicate.

**NETWORK** This layer moves data throughout the network by selecting the appropriate route and forwarding the data.

**DATA LINK** This layer handles the encoding, decoding, and logical organization of bits into data packets.

**PHYSICAL** This layer deals with the transmission of electrical signals across different physical devices.