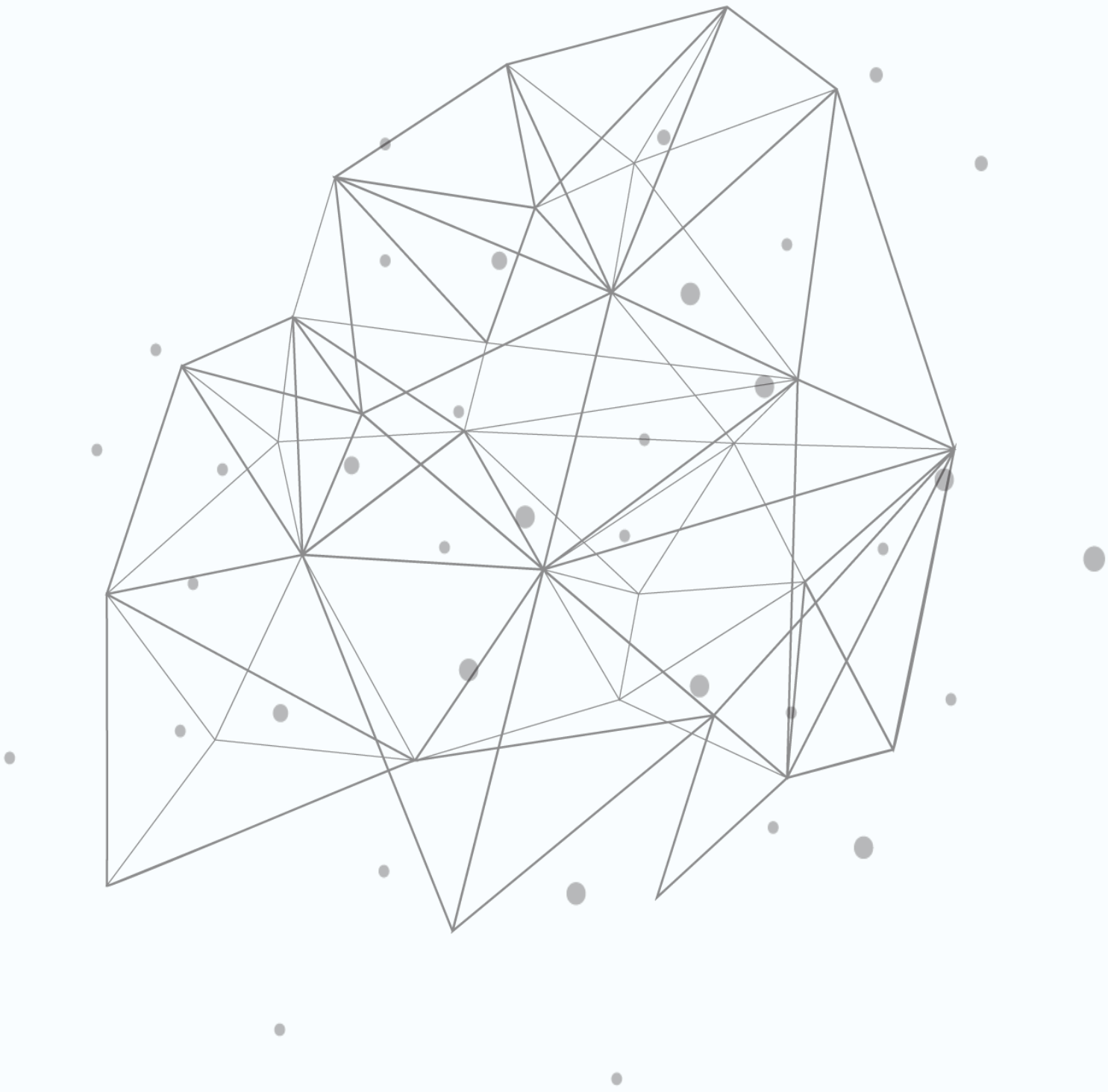
TCPWave DDI

DNS Security – Key Component of Zero Trust Model



Introduction

Historically, many organizations have adopted traditional perimeter-based network defenses, aka the castle-and-moat concept. The concept states that anything within the network perimeter is considered trusted. It proved to be ineffective with more high-tech targeting tactics.

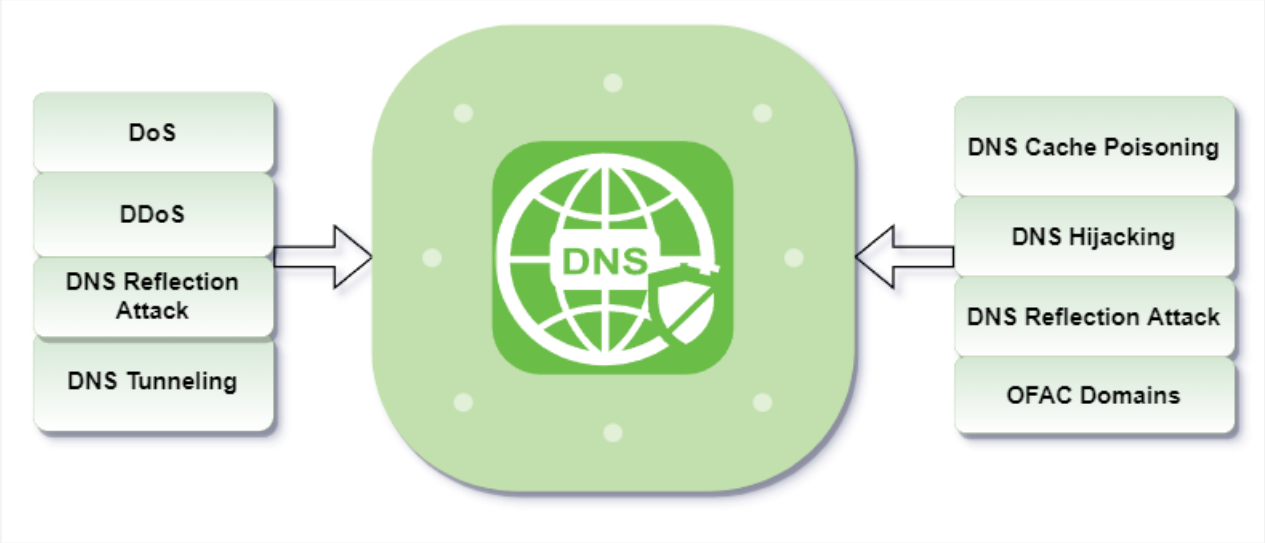
Cybersecurity has become a top concern for all organizations. While the saga of cyber-attacks continues, addressing such challenges has become a priority for many organizations in today's modern IT landscape. Hence to overcome the challenges of legacy security approaches and bolster the cybersecurity posture within the ecosystem, organizations require high-level security by implementing an end-to-end zero trust security model.

Zero Trust (ZT) Model

ZT model opposes the view of the conventional method of "perimeter-based" architecture of security. The underlying philosophy of the zero-trust model is simple – "Never Trust, Always Verify." - The mindset behind the model is to change from a network system perimeter build approach to an application-based and user-based security pattern.

DNS Security - Key Component of ZT

According to leading security reports, DNS is one of the most targeted services for application-layer attacks. Some of the most vulnerable DNS threats can compromise the integrity of the organization's DNS.



Hence DNS is one of the critical components that improve the overall defense of your network. With the TCPWave's advanced security features, the organization's business is always up and running, even during a DNS-based attack.

It can effectively detect the attacks using AI & ML logic DNS - TITAN, a threat intelligence algorithm - a fast and accurate detection by performing a smart analysis of the bi-directional DNS network traffic. Additionally, TCPWave's Reporting Management provides visibility across the organization's network and delivers quick insights that enable the network administrator to manage the network. With TCPWave's Advanced DDI Security platform, one can implement the key aspects of ZT model.

ADVANTAGES

The key benefits of the ZT model:

- Greater visibility of the organization's traffic
- Protection against internal and external threats
- Streamlined access
- Simplified logging and monitoring
- Easy detection of data breaches
- Optimizing end-user experience

Conclusion

Considering today's parade of mega breaches and where the organization's security perimeter is blurred, TCPWave's Advanced Security Solution fills the gap, elevates your organization's security at every level, and provides effective policies and procedures to implement proactive strategies for emerging cyber threats and secure your critical assets which in turn helps to implement the ZT model. Click here to know about TCPWave DDI Security.