BLOG

AUGUST 27, 2018 BY ATCHISON FRAZER

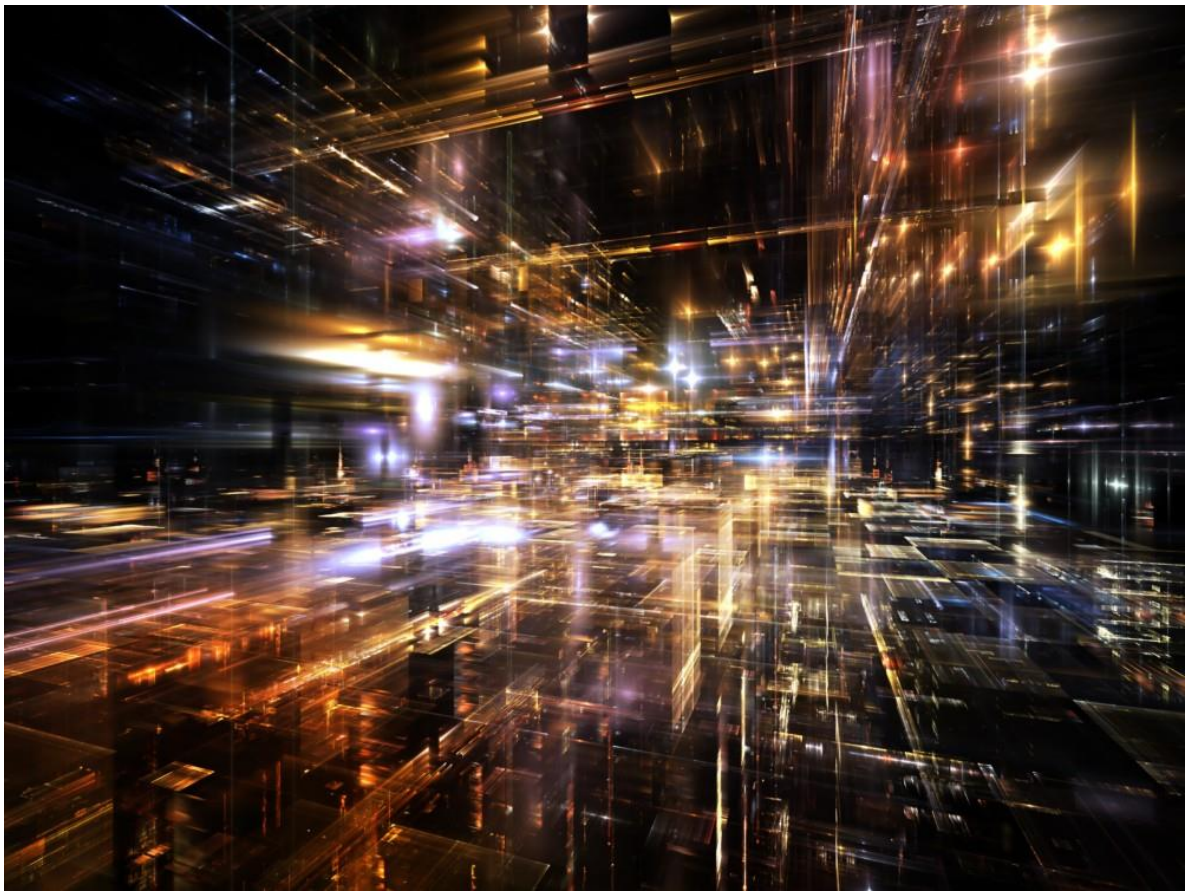
SECURE SD-WAN HELPS MANUFACTURERS DELIVER THE GOODS

Every manufacturer is concerned about the potential risks associated with cyber-crimes. If their data are stolen, it can lead to financial losses in sales, fines and monetary judgments against them; not to mention, the loss of customers and brand loyalty.

In 2017, there were over 53,000 security incidents and 2,216 confirmed data breaches. This is according to the 2018 Data Breach Investigations Report (DBIR) by Verizon. The report goes on to state, the most common access among all security breaches (73 percent of breaches) are those perpetrated from outside the organizations through the wide area network (WAN).

Enterprise WANs, with multiple ISP links and even private leased lines like MPLS, represent cracks in the surface for hacking, malware, phishing, ransomware, and Denial of Service (DoS) attacks. Simply put, you can't have a reliable WAN without a secure WAN. One without the other puts manufacturers at great risk.

WANs are a primary means for cyber-criminals to surreptitiously reach into a manufacturer's treasury. Manufacturers have endured many compromising attacks, from individual hackers to state-affiliated criminal espionage. Last year there were 536 security incidents, and 73 with confirmed data disclosures that compromised personal data, corporate secrets and user credentials.



Long before someone in an organization discovers it, cyber-criminals can steal a manufacturer's product and technology plans, research and development information, and other vital secrets. According to the Verizon DBIR, this type of cyber-espionage accounts for 31 percent of all breaches, that can lower a manufacturer's earnings potential and undo a potential competitive advantage. Not only are manufacturers at risk, they can also be the source by which cyber-criminals gain access to customers and business partners, using botnets to infect devices with malware that captures login credentials.

When Verizon examined targeted versus opportunistic attacks, they found that, in manufacturing, 86 percent of breaches were targeted. With the clear majority of cyberattacks in other industries being opportunistic, this discovery underscores the fact that criminals go after certain manufacturers with very specific purposes in mind.

Based on the growing attacks perpetrated through the WAN on seemingly ineffective security infrastructure, siloed security and networking infrastructures have proven to be ineffective. When we separate security infrastructure from network infrastructure, we create opportunities for cyber- criminals to find and exploit architectural weaknesses.

Versa offers a single multi-tenant branch VNF where different organizations can still configure and monitor their own services or establish SLAs with MSPs. This branch VNF is centrally managed by a multi-tenant Versa Director and multi-tenant Versa Analytics instance.

For example, consider the composite enterprise use case of a global auto and truck manufacturer: the primary service provider maintained one corporate tenant but was able to segment main department functions by sub-tenant, such as HR, Engineering and Sales, and regulate traffic flows, performance and security policies by the SLAs established for each department. In the case of Engineering, tenants subordinate to the Engineering tenant, were broken out for software development, R&D and manufacturing, with even more tailored policies for virtualized networking and security.

Networking and Security Requires a New Model

The types of security breaches documented by Verizon's DBIR require a paradigm shift to a modern software-defined enterprise infrastructure. One that consists of multiple inter-dependencies, relationships and key structural network and security functions that are inherently integrated into a single, cohesive network-wide, and cloud-native platform.

SD-WAN with full-featured security that is automated and programmable at every edge location, enables incident data to be centrally managed and responded to in real-time, sophisticated algorithms that benefit from the contextual visibility to fully integrated networking and security protocols.
When architecting a secure SD-WAN, it is vitally important to implement uniform corporate security policies for every node at the network edge. In doing so, manufacturers will have protected audit trails for traffic going in and out of the company network.

Even if a manufacturer has established infrastructure operations with multiple levels of security, that includes strictly enforced policies, and regularly scheduled audits, they are susceptible to many potential cyber threats that at minimum, can bring down their network; let alone, compromise personal data, corporate secrets, and user credentials.