AT&T Business Summit 2019: Securing the 5G World
November 22, 2019
By: Craig Robinson, Martha Vazquez, Christopher Kissel

IDC’s Quick Take
AT&T held its annual Business Summit November 4-7, 2019, in Dallas, Texas. While there were no major product or service announcements made during this time, the digital transformations that 5G will power were a hot topic overall for the conference. The long-promised rollout of the company’s 5G offering has the promise to create some unique use cases for the technology, while it also provides a test to see how well the integration of AT&T’s purchase of AlienVault into the new AT&T Cybersecurity division is able to provide the security umbrella over the expanded risk surface that these new 5G use cases will expose.

IDC recognizes that technology mergers and acquisitions are a common occurrence in the technology space that cybersecurity companies reside in. During the conference, AT&T was able to pacify industry analysts by showing that the combination of AT&T’s prior enterprise-focused cybersecurity business with AlienVault’s more midmarket focus has created a drama-free cybersecurity power player.

Event Highlights
In August 2018, when the AT&T acquisition of AlienVault was completed, the first set of reasons seemed clear enough. AT&T already had a presence as a managed security service provider (SP) and was an emerging leader in IoT. AlienVault had a core reputation as a services and appliance supplier for small and midsize businesses. (Importantly though, AlienVault was reducing emphasis on its AlienVault Unified Security Management [USM] all-in-one hardware appliance in favor of its cloud-based AlienVault USM Anywhere security-as-a-service approach). AlienVault hosted the Open Source SIEM project (aka AlienVault OSSIM) and the Open Threat Exchange (OTX), which has roughly 125,000 members and works in the best sense as a community repository of threat data and best practices. If AT&T only achieved what was on the surface, the acquisition made sense.

Ultimately, the acquisition of AlienVault was designed to bolster AT&T Cybersecurity. Perhaps underappreciated at the time of the acquisition was the union of AT&T’s threat data collection (including anonymized data from its USM global sensor network, which includes multicloud, mobile, and IoT, as well as anonymized data from AT&T’s security operation centers[SOCS]) with Alien Labs’ threat analysis engine and threat research team. The depth of threat analytics is impressive. One key statistic is that (now) AT&T Cybersecurity labs analyzes 370,000 unique malware samples per day.

ATT&CK in the MITRE ATT&CK framework stands for "adversarial tactics, techniques, and common knowledge." It might be instructive to turn the idea of ATT&CK around and figure out what a global SOC would need to be effective to support managed security SPs, MDR service, threat intelligence, and support for appliances. A first simple idea is that a global SOC would need to be able to dynamically group malware families to see patterns, newness (which determines the likelihood of targeted attacks), and what to do procedurally regarding mitigation/remediation. Second, a global SOC needs to have a comprehensive view of URL and IP addresses to help with whitelisting and blacklisting and to correlate destination with command-and-control servers. Third, the global SOC would need a combination of
human expertise and AI/ML to produce meaningful threat analytics and reduce noise in the network. Last, there would have to be some sort of way to analyze files and codes. AT&T Cybersecurity has built this type of back end and constantly refines it.

IDC's Point of View

New product or service offerings are often announced at events such as the one that IDC analysts witnessed at the AT&T Business Summit. Sometimes, the lack of any news is, in itself, newsworthy. Whether it was the discussions or demonstrations of its new 5G capabilities or a robust discussion of its ideas and philosophies on how businesses use its platforms and services to secure themselves, there was a feeling that AT&T Cybersecurity was showing gravitas on its offerings and did not need to make any big news. In discussions and product briefings that AT&T hosted, what stuck out was a feeling of business as usual, which is really quite remarkable given how its acquisition of AlienVault was just completed a short 15 months ago.

AT&T has combined its security consulting, managed security services, USM technology platform, and Alien Labs threat intelligence unit as a standalone division — AT&T Cybersecurity. AT&T, prior to the Alien Vault acquisition, had a threat platform called AT&T Threat Manager, which used advanced analytics to detect and respond to threats on customers' endpoints, data, and connectivity. With the integration, AT&T has rebranded AT&T Threat Manager as AT&T Managed Threat Detection and Response, with the USM service as the platform on which that service is delivered. What this means is that the platform can combine a multitude of security capabilities, providing better visibility across multiple IT environments such as on-premises, private, and public cloud networks. By doing so, AT&T has improved its detection, response, orchestration, and automation capabilities.

In addition, AT&T has vamped up its threat intelligence by leveraging Alien Labs, the USM global sensor network, and the Open Threat Exchange. The Alien Labs research team also has visibility into the AT&T IP network through its collaboration with the AT&T Chief Security Office (CSO). This combination alone has placed AT&T in a better position in the managed security SP market by offering MDR capabilities. In addition, the ability to target midsize businesses with a new offering that is simple to implement provides integration with other security tools, and better detection and response capabilities is a win-win for AT&T and the customer.

Philosophically, AT&T made some good points that strong players in the cybersecurity market can make and that buyers of these cybersecurity products and services should learn from. One of the points that IDC strongly agrees with is that cybersecurity teams need to transform from being the department of "no" to becoming the department of "yes" by providing strong security capabilities that allow businesses to confidently win new business bids by having a stronger security posture. AT&T needs to build upon it's historically strong ties in the IT and security departments of their clients to make the argument that a strong cybersecurity posture with the right platforms and services, teamed up with strong security-focused companies such as AT&T, can position their organizations to make confident business decisions. AT&T's challenge will be to make that argument not only in the technology-focused areas of the organization but also in other operational departments that are often used to fund technology-related investments. AT&T, like other telecommunication companies that have cybersecurity offerings, are not used to having much access to these other departments or corporate boards where, so often today, key financial investment decisions are made, but it will need to make inroads in this arena in order to grow its market share.
The large number of seminars, briefings, and use-case showcases highlighted what AT&T wanted its customers and industry analysts to pay attention to. What was especially fascinating was the topical areas that had high attendance numbers. The IoT use cases and seminars related to the dark web gathered high levels of attendance. IoT interest makes a lot of sense for AT&T to showcase, as the rollout of 5G opens up the potential risk surface of new use cases such as the smart car or smart cities. IDC survey data has also noted the recognition of CISOs' need for awareness into the dark web that threat intelligence services can provide. AT&T's leveraging of its Alien Labs threat intelligence research team can and will make a difference for its clients by proactively detecting and stopping the targeted attacks that cybercriminals are deploying today.

Just like AT&T made the corporate decision to have its global icon be that of a transparent globe when SBC merged with AT&T, AT&T's cybersecurity portfolio will allow businesses to move confidently in this new 5G transparently connected world by providing some of the more advanced products and services such as its Managed Threat Detection and Response service offering that it is heavily promoting. These more advanced capabilities that make up AT&T's portfolio would make the old Bell Labs engineers smile as they see their legacy being carried out today with AT&T Cybersecurity.

Subscriptions Covered:
Security Analytics, Intelligence, Response, and Orchestration, Security Services

Please contact the IDC Hotline at 800.343.4952, ext.7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC or Industry Insights service or for information on additional copies or Web rights. Visit us on the Web at www.idc.com. To view a list of IDC offices worldwide, visit www.idc.com/offices. Copyright 2019 IDC. Reproduction is forbidden unless authorized. All rights reserved.