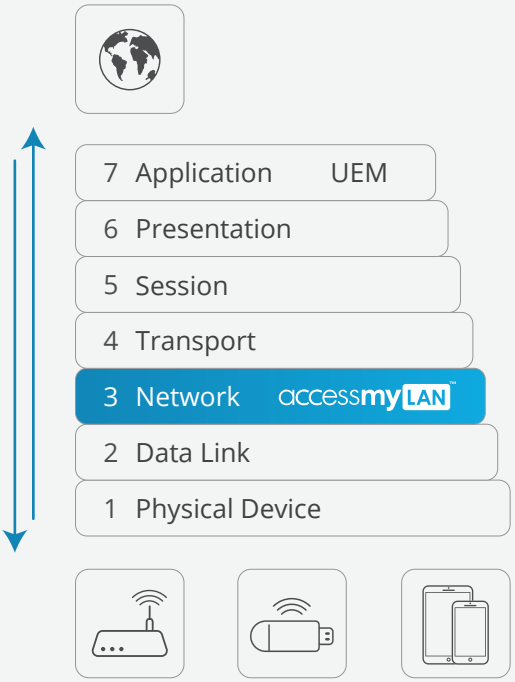
AccessMyLAN

Protecting the Mobile Enterprise against Cyber Threats through Private Connectivity

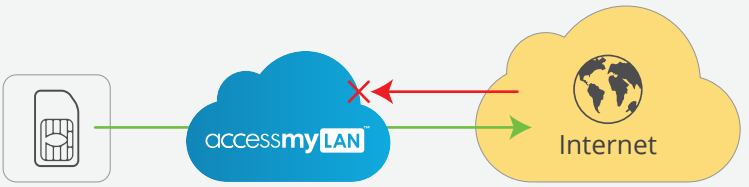
Cyber-crime is growing every day with an increasingly vast variety of attack vectors used by criminals including malware, phishing, botnets, and spyware.

Industry Leading Facts

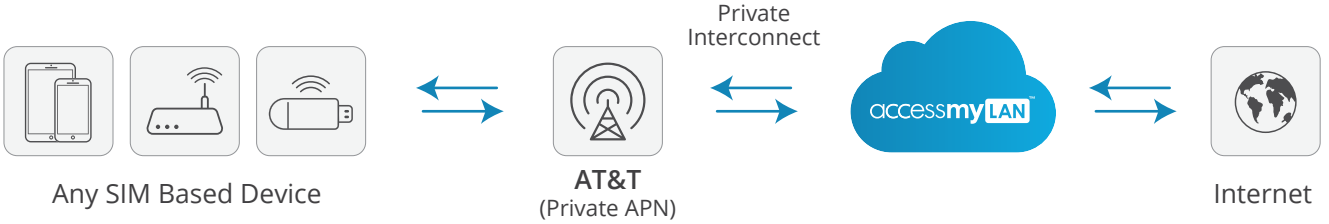
- *The global average cost of a data breach is up 6.4 percent over the previous year to $3.86 million. The average cost for each lost or stolen record containing sensitive and confidential information also increased by 4.8 percent year over year to $148.* IBM
- *Global ransomware damage costs are predicted to grow from $5 billion in 2017 to $11.5 billion by 2019.* Cybersecurity Ventures
- *By the end of 2018, more than 50 percent of companies affected by the GDPR will not be in full compliance with its requirements.* Gartner



Ecosystem



Architecture



AccessMyLAN Overview

Security Features

- Real Time Alerting for Admins & End Users on data usage
- Domestic & International Control for any device with a SIM
- All Anonymizers/Malicious/Unknown Sources blocked
- Private Network Transport over AT&T Network
- Content Filtering/Custom Policies of the entire world wide web & applications
- WIFI protection to protect against man in the middle attacks
- Over the Air deployment; no end user interaction needed when paired with a UEM*
- Private Static IP and Routing
- Manage & Protect Devices from Tor Traffic

Technical Capability

- Radius Authentication directly from the AT&T LTE Network
- Access Control Lists (ACL)
- Layer 3 of the OSI model (Complement to UEMs)

AML analyzes billions of URLs and ad impressions daily by combining static analysis, behavioral analysis, 3rd party industry feeds, and human-supervised machine learning to deliver the most extensive malicious website detection such as:

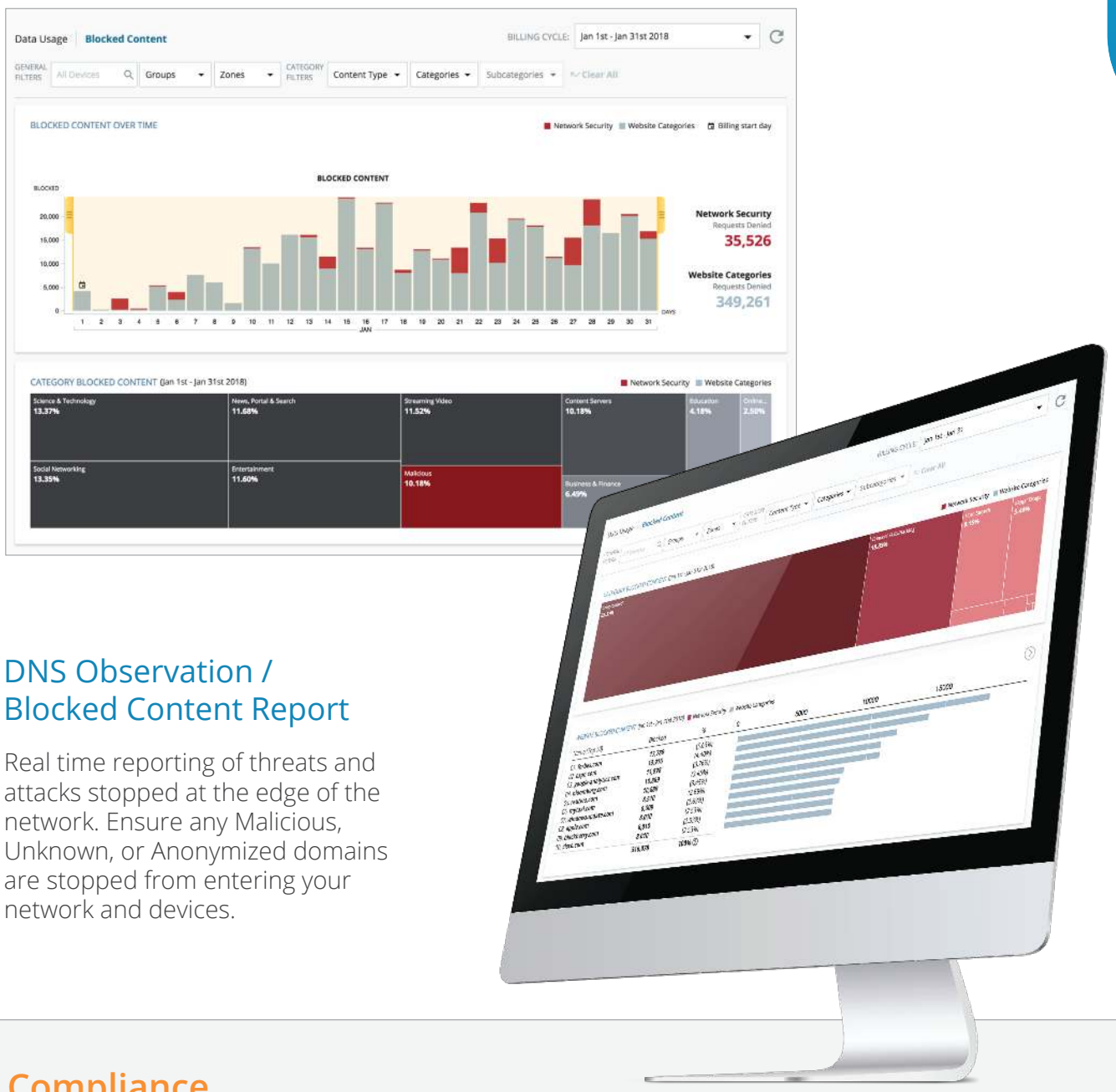
Category	Description
Phishing	Web pages that impersonate other web pages usually with the intent of stealing passwords, credit card numbers, or other information. Also includes web pages that are part of scams such as a "419" scam where a person is convinced to hand over money with the expectation of a big payback that never comes. Examples con, hoax, scam etc.
Spyware & Questionable Software	Software that reports information back to a central server such as spyware or keystroke loggers. Also includes software that may have legitimate purposes, but some people may object to having on their system.
Compromised & Links to Malware	Compromised web pages are pages that appear to be legitimate, but house malicious code or link to malicious websites hosting malware. These sites have been compromised by someone other than the site owner. If Firefox blocks a site as malicious, use this category. Examples are defaced, hacked by etc.
Malware Distribution Point	Web pages that host viruses, exploits, and other malware are considered Malware Distribution Points. Web Analysts may use this category if their anti-virus program triggers on a particular website.
Cryptocurrency Mining	Websites that use cryptocurrency mining ("cryptojacking") technology without seeking the user's permission.
Malware Call-home	When viruses and spyware report information back to a particular URL or check a URL for updates, this is considered a malware call-home address.
Command & Control Centers	Internet servers used to send commands to infected machines called bots.
Spam URL	URLs that frequently occur in spam messages.

AccessMyLAN Portal

Data Usage Reports

360 degree real time visibility into all mobiles devices with deep network level insights into any website or application accessed domestically or internationally. Granular reporting allows for deeper network level insights with advanced filtering technology to provide the best in class reporting.

AccessMyLAN Portal



DNS Observation / Blocked Content Report

Real time reporting of threats and attacks stopped at the edge of the network. Ensure any Malicious, Unknown, or Anonymized domains are stopped from entering your network and devices.

Compliance

We take protecting data seriously. We have implemented the strictest industry security best practices to ensure our services are built to meet the most rigorous standards.

FIPS 140-2 Compliance

CJIS Compliance

FirstNet Certified

ISO 27001