DON'T LET SMART DEVICES OUTSMART IT

Delivering a Security Framework Built on Adaptive Trust Defense

Mobile computing and the Internet of Things (IoT) have changed everything— especially how devices, data, identities and applications are secured. It's time for a security framework built on an adaptive trust defense.

The New Reality: Everything is connected to everything else

Endpoint growth is massive and diverse, due to the twin drivers of mobility and IoT

9 billion connected IoT devices in 2016

2.4 billion smart connected devices (notebooks, tablets, smartphones) will be shipped in 2018

New, ground breaking use cases
Smart workplaces, Connected healthcare, Omni-channel retailing

This new IT landscape comes with greater risk

Endpoint proliferation and diversification increases risk for IT and security professionals.
- Unmanaged endpoints
- Rogue applications
- Shadow IT
- Unfamiliar IoT devices
- More points of entry into the network - and beyond

THE RESULT...

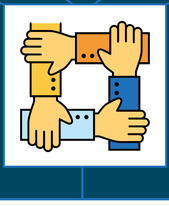
1 Billion+ data breaches in 2016; a new record

By 2018, **66%** of networks will have an IoT security breach

31% of stolen smartphones were not blocked by operators

Building an Adaptive Trust Framework You can't protect something if you don't know what it is, whether it's connected to the network, who has access to it or what it's connected to. **An adaptive Trust Framework is built on four key principles:**

- **Discovery & Profile**
- **Authentication & Authorization**
- **Monitoring & Alerting**
- **Decision - Making & Action**



Traditional security products and processes are insufficient for the new endpoint security realities:
- Carefully designed and targeted attacks
- Lack of security skills, especially for new mobility and IoT threats

Real-world solutions in the new era of Adaptive Trust

An Adaptive Trust solution delivers greater functionality, automation, scalability and flexibility than traditional security point products. The combination of Aruba ClearPass and Niara User and Entity Behavior Analytics (UEBA) is optimized for the new worlds of BYOD, IoT and unlimited connectivity.

- Endpoint visibility that identifies all forms of endpoints on wired and wireless networks
- Aruba ClearPass Policy Manager for real-time enforcement, BYOD onboarding, guest access and reporting
- Niara UEBA for detecting attacks into the network and big data forensics to accelerate investigations and remediation
- Integration with firewalls, SIEM and other security solutions to respond to possible attacks and threats
- Extended and deeper capabilities of legacy security approaches such as SIEM, firewalls and endpoint detection

For more information on how to build the ideal Adaptive Trust security framework, please go to www.arubanetworks.com

iStock Credits: Enis Aksoy, stevanovicigor, vasabii
Infographic Design: Sophia Tamura/TechTarget

aruba
a Hewlett Packard Enterprise company

TechTarget Custom Media