IDG
INTERNATIONAL DATA GROUP

White Paper

Staying Ahead of the IoT Security Curve With Reimaged Network Access Control

The dramatic influx of IoT and other network-connected devices requires a radical new approach to management and security.

International Data Corp. forecasts that approximately 80 billion devices will be connected to the internet by 2020, up from 11 billion today. This flood of internet of things (IoT) is expected to transform the corporate IT landscape at an unprecedented scope and scale, potentially crippling legacy IT infrastructure management systems.

Security concerns—the top issue voiced by IoT developers according to a 2016 IEEE survey—could dampen IoT's potential. IT organizations must rethink their approach to securing the network perimeter, pushing intelligence to the edge of the network with a focus on managing devices at a much higher level of granularity—without imposing access controls that penalize the business.

Defining the problem

The days of exercising strict control over which devices attach to the corporate network are over. The influx of IoT devices—not to mention the bring-your-own-device (BYOD) phenomenon—has dramatized the many benefits of flexible network access. Customers, suppliers, and partners increasingly expect to tie into corporate networks, whether through access points, APIs, or microservices. As a result, enterprise networks must be flexible enough to accommodate occasionally connected devices while also being robust enough to quickly detect and block malicious activity.

Endpoint devices that lack the latest software and firmware updates and security patches are one of the most pervasive security risks in today's networks. Endpoint management systems can now automate many software update procedures, but today's systems are largely unprepared for the barrage of new devices that don't conform to legacy standard definitions of PCs and servers.

Even with automation, large-scale software and firmware updates are extremely difficult to coordinate. Lack of knowledge about the latest security updates, combined with overwhelming workloads and shorthanded administrative staff, can result in mayhem, with many patches and security upgrades being applied haphazardly or not at all.

The problem is about to get worse too. Makers of IoT devices like sensors, cameras, and thermostats all have their own approaches to distributing and applying updates.

Bankruptcies and acquisitions may leave some devices marooned with no updates at all, while older devices may go unsupported simply because maintenance isn't worth the effort. This issue is important enough that the Federal Trade Commission has urged device makers to take these issues into account when designing products and subscription plans.

PRESENTED BY

Genians

Wanted: A new breed of network access control

Network access control (NAC) systems protect network perimeters by restricting the availability of network resources to endpoint devices that comply with defined policies. Most NACs do a good job of maintaining an asset inventory, authenticating devices, and keeping anti-virus and anti-malware software up to date. However, most are incapable of managing the more complex network environments of the future.

Traditional NAC solutions are complex, slow, costly, and limited in the range of devices they support. They can manage end-user productivity devices like PCs and wireless access points, but they aren't designed to accommodate the new breed of IP-connected sensors, cameras, and controllers.

Next-generation solutions need to combine technology information with business context to understand where vulnerabilities may exist. This demands not only a more comprehensive view of the devices themselves, but also better understanding of risk indicators.

Here are some of the advanced features that the next generation of NAC will need:

- **Comprehensive visibility** into all devices on the network, including contextual information about function, connectivity, application dependencies, EOL/EOS status, and vendor viability and commitment
- **Integration with the bigger context** of how devices are used
- **Integration with authentication and identity management platforms** to extend controls to individual devices
- **Automatic update** capabilities
- **A constantly updated master database** of vulnerabilities and the status of patches and fixes for all devices
- **Policy-based node group management** that permits microsegmentation so that devices and users can be organized dynamically
- **Tracking and monitoring** of network-attached and network-enabled devices from installation through decommissioning
- **Remote blocking and isolation**
- **Full reporting** with drill-down capabilities

A cloud-based approach

Today's network environments evolve too rapidly for on-premises NAC solutions to keep pace, which is why future solutions are cloud-bound. They allow for constant refreshes with the latest information about patches, upgrades, threats, and vulnerabilities. They deliver superior functionality, security, and availability to on-premises approaches. They also shift costs from capital to operating budgets, enabling IT organizations to forecast more accurately and free up capital reserves. Updates can be delivered immediately without the need for installation, and the solution is inherently protected against obsolescence.

Get started

A recent survey reveals that more than half of industrial IoT leaders believe IoT will have a major impact on their industry within three years, but barely 2% have a clear vision for adoption or large-scale implementation. The same study finds that executives see significant benefits from IoT in product and service differentiation and customer engagement.

This suggests that early movers have an opportunity for long-term competitive advantage through IoT-driven innovation. Those organizations that put the infrastructure in place today to capture that value will be the winners. It all starts with the network.

The Genians Difference

Genians reimagines network access control by using device platform intelligence to monitor the entire lifecycle of all devices connected to the network to ensure the highest levels of security and IT operational efficiency.

Device platform intelligence incorporates technology information with business context to expand visibility holistically and ascertain any vulnerabilities accurately. Genian NAC powered by this intelligence can detect platform information precisely about most connected devices without the need for an agent and present actionable information through personalized dashboards.

The Genian NAC performs ongoing compliance checks efficiently to ensure that all connected devices are continually identified and authorized, given policy-based access control, and constantly referenced against vendor/manufacturer information to determine any need for updates, patches, or retirement. The solution can be delivered via cloud or on premises at a fraction of the cost of a traditional NAC.

For more information, visit **genians.com/editions.**

Genians