FORTINET

WHITE PAPER

The Evolution of Network Access Control (NAC)

How IoT and Telework Have Changed NAC Solutions

Executive Summary

The proliferation of Internet of Things (IoT) and remote access issues due to the shift to telework have have both changed the shape of networks and subsequently how they must be protected. When it comes to protecting endpoints, network security strategies such as previous-generation network access control (NAC) solutions are outdated. They lack the comprehensive visibility, control, and automated responses necessary to ensure secure enterprise deployments of both IoT and remote devices. Beyond putting an organization's data, users, and regular business operations at risk, this defensive shortfall also exposes the enterprise to potential regulatory fines and other possible punitive damages.

From Mobile Endpoints to IoT Devices

Companies continue to struggle with securing mobile endpoints. Guests, contractors, service people, and other "outsiders" often require network access. While enterprise mobility management (EMM) technologies and firewalls can help, they don't have sufficient visibility into device and user status to determine whether they should have permission to connect to the network or the granular controls to set access limits.

At the same time, cybercriminals also frequently target IoT devices because they represent some of the weakest points on the network. For example, many IoT products are "headless"—unable to perform even simple patches and offering little to no built-in security.

While industry regulations for IoT devices are under development, IoT security is already an important consideration for maintaining compliance with existing standards and requirements. Most companies must comply with regulations that require strict network access control and data protection—such as the General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), U.S. Securities and Exchange Commission (SEC), Sarbanes-Oxley (SOX), and the Payment Card Industry Data Security Standard (PCI DSS). To maintain compliance, organizations must secure all endpoint devices or potentially face fines that can reach millions of dollars per violation.

With virtual/cloud services, switches, routers, and branch offices that are connected and sharing information throughout the globe, the task of identifying and securing endpoints can seem overwhelming. While individual security solutions can cover some attack vectors, they generally lack the integrated and comprehensive history tracking and forensic information that incident response and compliance teams require for breach prevention, detection, and remediation.

Furthermore, the pandemic has forced millions of workers to shift from office-based working to remotely connecting over virtual private network (VPN) tunnels from home. The need to identify and risk-profile the devices connecting over these VPN solutions grows over time, as the normal patching enforcement isn't available and employees are using personal gear to connect to the corporate network.

The key problem here is that outdated access controls are leaving networks exposed to attacks (e.g., contamination by malware-infected devices or unauthorized access via stolen credentials).

"IDC expects global IoT spending will return to double-digit growth rates in 2021 and achieve a compound annual growth rate (CAGR) of 11.3% over the 2020-2024 forecast period."[1]

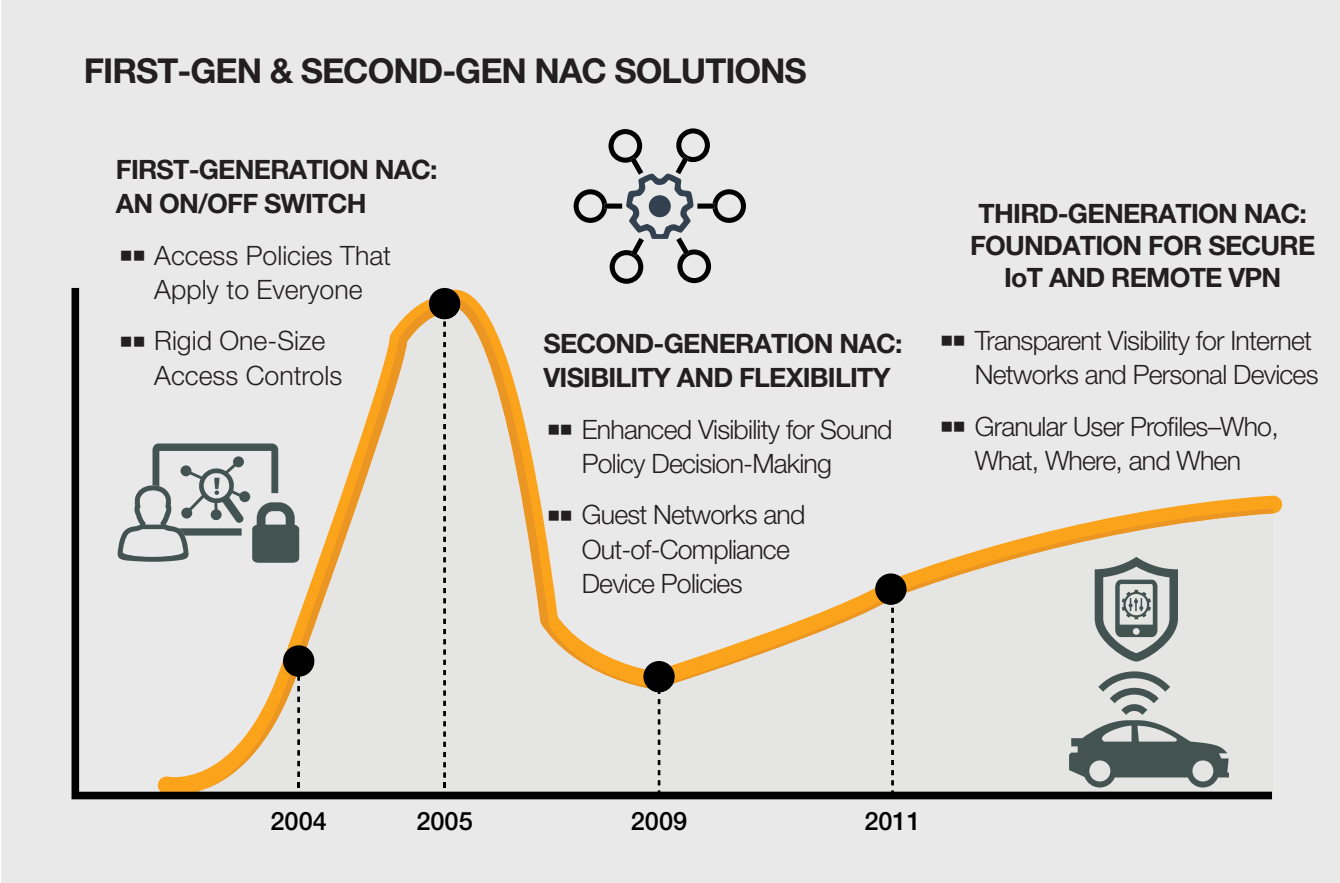
BYOD also continues to grow—the mobile worker population has exceeded 1.76 billion to account for approximately 59.4% of total global employment.[2]

According to one study, 63% of organizations are unable to monitor mobile devices when they leave the corporate network, and 53% reveal that malware-infected endpoints have increased in the last 12 months.[3]

First-generation NAC products functioned to authenticate and authorize endpoints (primarily managed PCs) using simple scan-and-block technology. The evolution to second-generation NAC solutions addressed the emerging demand for managing guest access to corporate networks. These second-generation access controls facilitated limited Internet access for external users such as visitors, contractors, and business partners.

But changes in both network infrastructure (digital transformation) and the evolving nature of sophisticated, targeted attacks have exposed several new network access vulnerabilities that must be addressed.

1. **Lack of Visibility and Awareness.** You can't protect what you can't see—the current lack of comprehensive and entralized device visibility (both BYOD and IoT products) leaves organizations vulnerable. Security teams must be able to see all network infrastructure gear across the many different locations, including the extreme edges of the network. Because endpoint security and network security typically operate in isolation from one another, they can't share much meaningful information in real time. If an individual device is being attacked, all other connected devices (and the rest of the network security architecture) should be instantly aware of the threat in order to mount a coordinated defense across the organization—something not possible with many traditional security approaches.



2. **Lack of Automated Threat Responses.** With thousands of security alerts per day, IT cannot manually intervene in every potential network threat. When the firewall, intrusion detection system (IDS), intrusion prevention system (IPS), or similar tool identifies a security breach at a particular IP address, the security architecture should automatically mitigate sophisticated threats with speed and efficiency, thus reducing risk exposure.
3. **Lack of Automated Workflows.** Many outdated processes, such as those for provisioning, require manual intervention from IT staff. This, in turn, can slow down on-boarding of new employees, introduce opportunities for human errors that increase risk exposure, expand IT workloads, and reduce overall security operations efficiency.

While these solutions provide control over traditionally managed devices, the unrelenting march to IoT and BYOD creates unique challenges. The most formidable issue is that there is virtually no device configuration standardization for BYOD or IoT. There are hundreds of permutations of device type, brand, operating system, and security health status—and most devices specifically lack

enterprise grade security. With the passage of time, the problem only becomes more complex as robots, heat monitors, insulin pumps, HVAC sensors, automated security access, and other IoT connections increase at a staggering pace.

Security Must Evolve To Control Access Exposures

With the proliferation of VPN remote access and IoT devices, endpoint security requirements have spread beyond the capabilities of previous-generation access controls. And as targeted zero-day exploits and advanced persistent threats continue to evolve and multiply, the need to close these defensive gaps becomes more urgent every day. Security architects must reevaluate network access controls to protect endpoints, users, and the broader organization from the potentially disastrous effects of a device-borne breach.

Experts estimate that we have approximately 9 billion IoT devices today, a number they expect to grow to more than 55 billion by 2025.[4]

[1] "Worldwide Spending on the Internet of Things Will Slow in 2020 Then Return to Double-Digit Growth, According to a New IDC Spending Guide," IDC, June 18, 2020.

[2] Nick Elia, "Mobile Worker Report Announcement," VDC Research, August 11, 2017.

[3] "The Cost of Insecure Endpoints," Ponemon Institute, June 2017.

4 Peter Newman, "IoT Report: How Internet of Things technology is now reaching mainstream companies and consumers," Business Insider, July 27, 2018.

December 5, 2020 7:24 AM

858990-0-0-EN

D:\Fortinet\White Paper\Purple White Paper\FortiNAC\wp-FA-the-evolution-of-network-access-control-1252020\wp-FA-the-evolution-of-network-access-control-1252020