BRADFORD NETWORKS

» WHITE PAPER

The Evolution of Network Access Control:

How NAC Solutions Have Evolved to Secure IoT and BYOD Devices

www.bradfordnetworks.com

Sizing-up the threat

Securing Bring Your Own Device (BYOD) & Internet of Things (IoT) devices are two of the most challenging areas of network security. BYOD has been a concern for several years, yet many companies are still struggling to secure these endpoint devices. It's important to note that BYOD is not all about mobile and it's not all about wireless. Guests, contractors, service people – all types of "outsiders" – may require access to your network. So simply focusing on mobile or wireless security is only half of the picture.

While EMM technologies can help (and so can firewalls), these technologies do not have the ability to determine whether individual devices should have permission to connect to the network, and then determine how much access to give each device. Most standalone solutions can't stop every attack, and since these solutions generally lack tight integration with other security solutions, they still leave the network vulnerable from BYOD endpoints.

Before many companies determined how to fully protect the enterprise network from BYOD, Internet of Things (IoT) enabled devices emerged. Built for autonomous machine-to-machine connection, IoT devices change how organizations collect data, automate services and structure inter-dependent systems. With functionality that ranges from simple tasks, such as tracking use and sending re-order alerts for a soda machine, to complex inter-connected devices like lights and HVAC sensors that can communicate and take action, IoT devices are becoming active participants in running a business and can be wired or wireless. With many of these devices designed to directly integrate into both the network of the company that purchases the device as well as the company that produced the device, IoT network integration is deeper and riskier than BYOD.

This is a concerning issue since IoT devices usually have very little security, and nothing close to enterprise grade defenses.

The first major IoT device attack shocked the industry in October of 2016 – before IoT devices were really in the enterprise space. A hacker launched an IoT DDoS attack on Dyn that used the Mirai virus to infect vulnerable IoT home security devices and turned them into attack bots focused on the Dyn enterprise network (for more information see our blog on this topic). This sent ripples of fear through organizations that realized attackers could soon leverage enterprise IoT devices to attack internal networks.

To counter the threat IoT devices introduce, organizations need to secure all endpoints. This white paper will explore endpoint security, and how the NAC solutions of yesterday have evolved into broader Security Automation and Orchestration (SA&O) solutions. Designed as a security integrator, SA&O coordinates all endpoint visibility, control and automated response, to ensure secure enterprise deployments of both IoT and BYOD devices.

» CONSIDER THIS

IoT network integration is deeper and riskier than BYOD.

Network Access Control Evolves to Meet BYOD & IoT Needs

As organizations rapidly add IoT and BYOD devices, it is critical to ensure this access does not compromise network security. In the past, enterprise networks were self-contained within a well-defined perimeter. A company could build strong defenses at the network edge and be fairly confident about keeping the bad guys out and the important data safe. As mobile access and IoT devices evolved, there is no longer a simple perimeter. Today, the network is accessed by a vast array of endpoints in varying locations. In addition, companies must now support multiple non-standard devices per user, as well as a host of IoT devices that must be secured. IDC predicts global IoT revenue will reach $7.065B by 2020, almost triple the $2.712B in 2015. BYOD also continues to grow, with IDC forecasting US mobile employees growing from 96.2 million in 2015 to 105.4 million mobile workers in 2020. This growth would mean more than 72 percent of the total workforce qualifies as a mobile worker. Clearly, mobile and IoT devices are here to stay, with increasing use becoming the norm, rather than the exception for enterprise organizations.

The Evolution of Network Access Control

IoT and BYOD devices are not the only endpoints that need to be controlled. As enterprise organizations continue to connect with partner networks or outsourced service agencies, these connections must also be secured. IoT security is also the subject of scrutiny, and discussions are under way about when and how much IoT regulations will be necessary. "The growing dependency on network-connected technologies is outpacing the means to secure them," Jeh Johnson, U.S. Secretary of Homeland Security said. "Securing the Internet of Things has become a matter of homeland security." IoT security will also be important to ensure compliance with existing regulatory requirements. With more companies facing regulatory requirements such as HIPAA, SEC/SOX, PCI DSS, etc. that require strict network access control and data protection, companies must secure all endpoint devices or potentially face fines that can reach millions of dollars per violation.

With virtual servers/cloud services, switches, routers and offices that are connected and sharing information throughout the globe, the task of identifying and securing these endpoints can seem overwhelming. To manage these trends about half the market has turned (or are turning to) to network access control (NAC) technology. The network access control market size was $681.3 million in 2015 and is estimated to reach roughly $2.65 billion by 2020.

> **» A MATTER FOR HOMELAND SECURITY**
>
> "The growing dependency on network-connected technologies is outpacing the means to secure them. Securing the Internet of Things has become a matter of homeland security."
>
> *— Jeh Johnson, U.S. Secretary of Homeland Security*

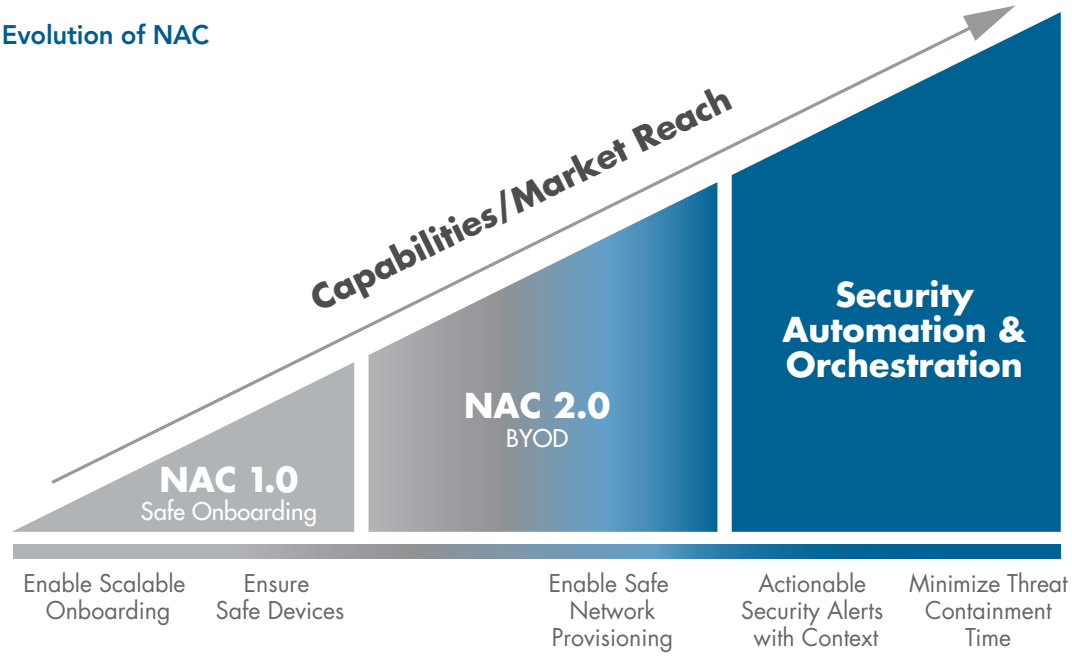
NAC solutions enable administrators to precisely define and control how devices and users gain access to network resources. Interestingly, *at the end of 2016, only about half the market has adopted network access control technology.* With the advent of IoT and endpoint risks, the market evolved so quickly that the

best NAC solutions are now the foundation of a more sophisticated Security Automation and Orchestration Solution (SA&O) before network access control even fully penetrated the market.

Many organizations have already realized that vendors who ***only*** offer NAC solutions for visibility, without the benefits of multiple data stream integration and automation, are severely behind the market. Savvy companies are leap-frogging past network access control and moving directly to the more sophisticated and successful SA&O solutions. SA&O solutions not only control access, but also provide complete visibility, automate threat response, and record and deliver all contextual information with each security alert, to speed the time to threat remediation. Let's review how and why the best network access control technology has evolved into a more sophisticated SA&O solution.

From the Basics to Advanced Control

Figure 3: Evolution of NAC



The early versions of network access control functioned as a way to authenticate and authorize endpoints, primarily managed PCs, using simple scan-and-block technology. NAC solutions then evolved to address the emerging demand for managing guest access to corporate networks. Network access control was used to facilitate limited Internet access for external users such as visitors, contractors and business partners.

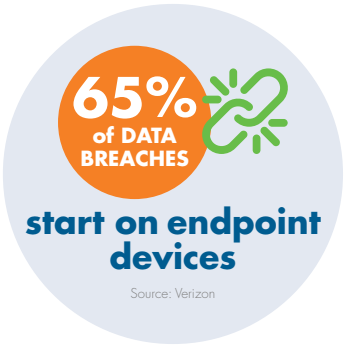
While these early NAC solutions provided control over traditionally managed endpoints, the unrelenting march to IoT and BYOD created unique challenges. The most formidable challenge is that there is virtually no device configuration standardization for BYOD or IoT. There are hundreds of permutations of device type, brand, operating system and security health status, most without any enterprise grade security, and it's getting more complex as time goes on. From robots, heat monitors, and insulin pumps, to HVAC sensors and automated security access, the number of IoT devices that are connecting to networks is increasing at a staggering pace.

Enterprise organizations also face the need to secure IoT devices in two different ways. First, many companies are now selling, or planning to sell, IoT enabled products that connect back to their networks to provide valuable information on product use and maintenance needs. Companies are rolling out IoT-enabled products for almost everything, from large wind powered turbines and trains, to office printers and security cameras.

The second IoT challenge is that more enterprises are buying and incorporating IoT enabled devices from other vendors, such as IoT enabled printers, copiers and cameras, into the enterprise network environment. While these devices save time and simplify operations (for example, they can email you when you are low on toner or automatically re-order), they also offer another avenue for hackers to access enterprise networks. To be successful, NAC solutions had to evolve into SA&O to fully secure these endpoints. You have to be able to see where each device is, what it is doing, how it is connected to other devices as well as the entire network topology. Organizations also need to integrate with other best-of-breed security solutions to get comprehensive security, but require an orchestration level, that aggregates all the security data, automatically quarantines and triages threats, and enables organizations to see it through one pane of glass for rapid resolution.

Endpoints are the Weakest Spot in the Enterprise Network

Mobile and IoT endpoints expand the network attack surface and pose a serious threat to security. Cyber criminals recognize this threat and frequently target their efforts at endpoints, which represent one of the weakest points on the network. In fact, as much as 65% of data breaches start on endpoint devices.



Many users don't recognize the security risks that individual actions (or inactions), as well as individual devices represent. Many users don't even enable the basic security features that come with their smartphones and tablets. What's more, they see little harm in downloading dozens of mobile apps from dubious sources. Even legitimate app stores such as those hosted by Apple and Google are known to offer applications riddled with malware. In fact, the Aranx 2016 State of Application Security Report revealed that 90% of the apps tested were vulnerable to at least 2 of the OWASP mobile top 10 risks.

While individual wireless mobile or wired device solutions can control some of these issues for BYOD, they generally lack the integrated and comprehensive historic tracking and forensic information necessary that incident response and compliance teams require – and IoT devices are still in their infancy when it comes to security.

Network Segmentation, offered by progressive NAC suppliers, is a key step in securing BYOD & IoT devices. If properly implemented and automated network segmentation helps to significantly shrink the threat landscape. By implementing "micro segments" on the network (that can be isolated, creates a deeper security layer.

Another rising threat is internal actors. It is important that organizations control the level of access for authorized users and devices, that sometimes get access to restricted areas or data, by either inadvertent or deliberate actions. For instance, an employee might gain access to a protected cardholder network in violation of PCI, or a hospital worker might gain access to records for patients not assigned to his/her care, which violates HIPAA. Although these employees and devices may be legitimate users on the network, they have gained inappropriate access to specific resources, posing an unnecessary risk. On occasion, disgruntled employees can pose a massive security risk. Securing endpoints and controlling access are critical steps in closing these security gaps. Evolved NAC solutions allow seamless and automatic access control policies to be implemented based on level of trust.

TRUSTED DEVICES

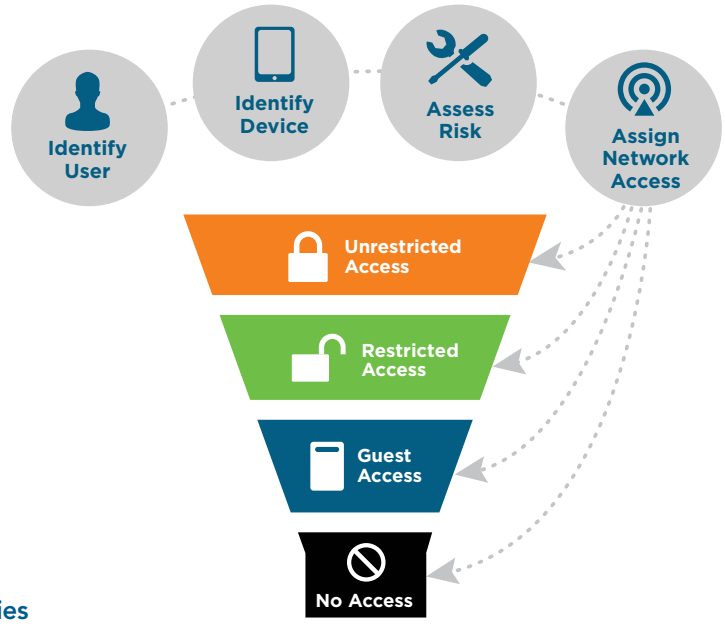


Figure 6: Trust-based policies

Security Automation & Orchestration: How to Put IoT and BYOD to Work with Confidence

Moving beyond the NAC capabilities of the past, Security Automation and Orchestration control technology is ideally suited to the challenges of BYOD & IoT. It delivers major advances to secure a much more dynamic environment and specifically addresses the challenges of complete endpoint visibility and access control. With the vast amount of data being collected, an automated and centralized security program that can aggregate data from numerous security programs and automatically respond to incidents is critical. Organizations gain complete endpoint visibility, access control and automated threat response that secure the network, but still enable the productivity-boosting use of IoT and BYOD devices. SA&O offers clear advantages.

- Network Edge Visibility – The old adage "You can't control what you can't see" is more appropriate today than ever. Lack of visibility makes an organization vulnerable, organizations need to see all network infrastructure gear across the many different locations and to the extreme edges of the network, including a clear view of all internal devices on the network (PCs, smartphones, laptops, servers, IoT devices, medical devices, POS terminals, etc.) as well as any other IP-based device through one integrated network topology view.
  - Visibility needs to include both the device type, as well as the software configuration (including whether anti-virus and malware protection is up to date); who the user is and what devices he/she has registered with the network; and even the location and time of day of the connection request.
  - Organizations should be able to automatically discover and interrogate all potential users associated with their devices before they are granted access to the network. This ability to identify devices and apply network access control policies before the connection takes place should be a prerequisite for connecting BYOD and IoT enabled devices to any enterprise network. Why? Consider this. Researchers at Purdue University analyzed how quickly malware can spread and found that malicious software can propagate to roughly 500,000

devices in just 100 seconds. Another recent test found that an IoT security camera was compromised within 98 seconds of plugging it in. While results will vary by incident, these figures are a reminder of how dangerous post-connect network access control can be. Just one infected device can become an epidemic in minutes. The visibility and granular access policies offered by SA&O are critical to controlling IoT & BYOD endpoints.

- Automated Provisioning & Network Access Control – A good SA&O solution supporting a BYOD environment must make on-boarding a seamless, simple interactive process that is simple for end users and does not require manual intervention from IT. Automated provisioning is critical for large-scale organizations (or even large-scale events such as conferences) to maintain scalability, minimize manual processes, and eliminate (or minimize) IT involvement. Automating Network access control and provisioning minimizes overall support and operating costs. A good SA&O solution should include automated self-provisioning that enables users to register themselves and their device. The SA&O solution can then do its risk assessment based on the Who, What, When and Where attributes of both the user and device. Based on the current circumstances and policies, it can then provision the right level of network access. With granular and flexible policies, users and their devices can be directed to pre-determined network segments such as Internet-only for guest users and unsupported devices, or full network access for authorized users. The best SA&O solutions should also enable organizations to allow unlimited access for some, such as the CEO, but restrict bandwidth and the number of device connections for others. By restricting access by time of day, by location, by job role or other criteria, a good solution can monitor usage, identify and restrict resource hogs and automatically ensure users have the right level of access. This automation decreases the burden on IT support staff while giving workers efficient access to the network.
- Automated Threat Response – BYOD & IoT devices increase the attack surface as well as the number of potential threats exponentially. With thousands of security alerts per day, IT cannot manually intervene in every potential network threat. When the firewall, IDS/IPS or other threat detection tool detects a security breach at a particular IP address, the SA&O solution must be able to automatically identify the compromised device, isolate or move it to a safe guest network, and send an alert to the user and administrator. Depending on the type of threat and established security policies, it should direct the user to take other actions to remediate the issue. With IoT devices, there is no user to self-remediate, so automated detection and quarantine is even more critical. A good SA&O solution should automatically detect threats, identify and quarantine the offending IoT device. The best SA&O devices also have the ability to automatically integrate information from different best-of-breed technologies, and take action according to security policies. Furthermore, it must provide open APIs to work with common and popular security solutions, such as those provided by Cyphort, Fortinet, Palo Alto Networks and Tenable; with mobility applications from companies like AirWatch and MobileIron; and with network infrastructure vendors, from Aerohive to Xirrus, to name a few.
- Analytics – By analyzing and visualizing large volumes of network access data over time, a SA&O solution should generate detailed reports that provide organizations with the long-term visibility and answers they need to make better business decisions; for example, to plan wireless network capacity, to manage software licenses, to provide better mobile device support, and to meet compliance requirements such as HIPAA, PCI DSS, etc. A great SA&O solution also enables organizations to assign business value to threats, so analytics can also be used to provide data-driven decisions on financial resource planning.

The best Security Automation and Orchestration solutions combine the visibility and granular, flexible policy-based network access control, with automated threat response and triage. This enables IoT and BYOD devices efficient and cost-effective access, while optimizing network security and performance.

Comprehensive Network Security: A Checklist

The most important feature of an SA&O solution is that it should enable an organization to see all endpoints and integrate information from multiple security sources into a single, comprehensive view using just one instance of the solution. Network segmentation strategy and implementation,likewise, is not a "set and forget" undertaking. Network access policies are constantly changing to cater to new business requirements. A topology-aware NAC solution is needed to maintain segmentation policies, and bring comprehensive visibility – automatically.

» THE KEY FEATURE

The most important feature of an SA&O solution is that it should enable an organization to see all endpoints and integrate information from multiple security sources into a single, comprehensive view using just one instance of the solution.

To accomplish this, the solution needs to communicate and exchange information with all network devices, rather than requiring an access control solution for each network segment. Companies should start by looking for a vendor-agnostic solution that supports all best-of-breed technologies, is proven, scalable and offers multiple deployment options for physical devices, virtual appliances, and cloud services. A good SA&O solution should also meet the following criteria:

- Flexible connectivity support – The solution must be vendor-agnostic and support all wired and wireless connectivity sources across the entire network.
- Broad range of device support – New generations of IoT, mobile and gaming devices enter the market every few months, and companies in every industry are quickly adopting IoT enabled devices such as printers, security systems, HVAC and medical devices. To secure these devices, companies will need an array of security solutions that work together seamlessly to protect every endpoint and network device.
- High level of automation – IT security professionals are stretched thin in most organizations. Any security device that's brought in must support a high level of automation so that it does not drain already limited IT resource. An endpoint security solution should support user self-provisioning, so little to no intervention is needed to give users the appropriate level of access. Automation should also include basic self-remediation measures if a device does not meet minimum security standards. For example, if a device requires an important security patch or has an outdated operating system, that user can be re-directed to a self-remediation page to correct the issue without requiring any IT intervention.
- Real-time threat response – For endpoints that could pose a potential threat, organizations need automated, real-time threat response that quarantines suspect devices immediately before an attacker can cause damage or access information. Companies should look for a solution that gathers and reviews contextual information, then forwards it along with the quarantine alert to a security analyst for resolution.
- Granular policies – Endpoint security solutions must support very specific levels of policies tied to both the user and the device. For instance, it may be fine for a doctor to use his tablet to access patient records while on the hospital ward but not from the hospital cafeteria. A high school student can be denied access to her school network at 3 a.m. because she really has no business being at school at that hour. The endpoint security solution must be able to determine such conditions – all of them – and make a judgment as to what level of access to provide for that specific request.

- **Integration with other security solutions –** When looking for an endpoint security solution, many companies adopt a SA&O solution because it does more than just co-exist with other complementary security solutions. The best solutions seamlessly integrate with other best-of-breed solutions and leverage the data in order to form a much stronger, secure enterprise network infrastructure. With SA&O IT groups can deploy best-of-breed vendor technologies without creating information silos and does not require a forklift replacement of existing solutions to upgrade one component.
- **Scalable to support rapid growth –** Building operational processes (for example, automating mobile device registration) is key to scaling an IoT or BYOD project. An enterprise SA&O solution must provide a scalable architecture that can support multiple locations across the enterprise, and virtually unlimited devices so that the organization can on-board additional devices as needed without costly upgrades or the need to deploy multiple instances of the security solution.

Network Access Control Moves Into the Future

Network access control has changed dramatically in just a few years. With the proliferation of BYOD & IoT devices, the network perimeter is now an amorphous grouping of endpoints and partner integrations that must be secured. With zero-day exploits and advanced persistent threats, no one can anticipate every incursion. Attackers are targeting the weakest links: the endpoint. As the number of IoT and BYOD devices connect to a company's network, the attack surface grows broader. Security administrators need to secure endpoints in both pre-connect and post-connect scenarios, as well as automate threat response, to reduce risk. The best SA&O products are designed with this precise scenario in mind. For any organization that allows BYOD or IoT, SA&O is a must-have security solution and an important piece of an overall security infrastructure that enables worker productivity while securing endpoints and the network from threats.

BRADFORD NETWORKS

374 Congress Street, Suite 502, Boston, MA 02210, USA
Toll Free +1 866.990.3799 | Phone +1 603.228.5300
Email info@bradfordnetworks.com
Web vwww.bradfordnetworks.com

Bradford Networks is leading the transformation of network security by providing visibility, control and response to minimize the risk and impact of cyber threats. The company's patented Network Sentry solution continuously assesses the risk of every user and endpoint, and automatically contains compromised devices that act as backdoors for cyber criminals. Through its SmartEdge Platform, Network Sentry seamlessly integrates with firewall, threat detection and endpoint security solutions to enhance fidelity of security events with contextual awareness. This unique triaging process bridges the gap between the SOC and the NOC by replacing error-prone manual interventions with automated threat to reduce containment time.