Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Securing BYOD With Network Access Control, a Case Study

This Case Study highlights how an organization utilized NAC and mobile device management solutions to establish policies for enabling a bring-your-own-device environment with an acceptable level of risk.

Copyright SANS Institute
Author Retains Full Rights

AD

LICENSED FOR DISTRIBUTION

Gartner

Research
G00226207

29 August 2012

Securing BYOD With Network Access Control, a Case Study

Lawrence Orans

This Case Study highlights how an organization utilized NAC and mobile device management solutions to establish policies for enabling a bring-your-own-device environment with an acceptable level of risk.

© 2013 SANS Institute. Author retains full rights.

Key Findings

- The knowledge and experience gained in establishing and enforcing network access control (NAC) policies for corporate-owned Windows laptops can be extended to apply policies for personally owned devices.
- Strong operational processes are needed to maintain an exception list of devices that are exempt from NAC policies. An automated solution for discovering and profiling all endpoints, including exception devices, is the preferred approach.
- Supporting a large NAC implementation is not a labor-intensive effort. In this example, only one full-time equivalent (FTE; a senior-level engineer) is dedicated to supporting approximately 100,000 endpoints (1,000 are personally owned devices, the rest are corporate-owned).

Recommendations

- Combine NAC and mobile device management (MDM) to enforce policies in a BYOD environment. Personally owned devices that are not managed by MDM agents should be limited to Internet access only, or placed in a limited access zone where they can access a subset of applications and network resources as per user/group role.
- BYOD policies should be broad-based and protect the wired and wireless networks. Use cases should address smartphones and tablets that need wireless access and laptops (Mac and Windows) that need wired access.

What You Need to Know

A combination of NAC and MDM can enable a flexible BYOD environment with an acceptable level of risk for many organizations. NAC can be used to check for the presence of an MDM agent. Endpoints that do not have the agent can be blocked or granted limited access (for example, Internet access only). NAC can ensure that employees must comply with MDM policies if they wish to gain access to

the corporate network. Building operational processes (for example, automating mobile device registration) is key to scaling a BYOD project.

Case Study

Introduction

Security-conscious organizations need to proactively develop solutions to mitigate the inherent risks in the BYOD phenomenon. IT departments must respond to pressure from employees and business units to support a BYOD environment, and security professionals do not have the luxury of saying "no" to this unstoppable trend. Organizations can establish policies that create a common ground, where employees are allowed to use personally owned devices in the workplace, and the organization maintains an appropriate degree of control over the device. NAC policies can be used as key components of an overall solution to successfully create this type of environment. Organizations can create BYOD policies that reflect their security postures, and can use the network to allow, deny or grant limited access to devices, based on their compliance with these policies. Here, we analyze how an organization with a mature NAC solution successfully extended its network access policies to enable a secure BYOD environment.

The Challenge

In 2010, a large financial services company realized that it needed a strategy for supporting personally owned devices in the workplace. The company has more than 100,000 endpoint devices distributed over 200 locations worldwide, and it anticipated that it would soon need to support approximately 10,000 employee-owned smartphones, tablets and personally owned laptops.

Approach

The company's risk and compliance management team led the project and was responsible for establishing the BYOD policies. The project team consisted of four key individuals — the company's lead for the compliance team, a company network engineer, the NAC vendor's system engineer and the NAC vendor's on-site service engineer.

As a risk-averse organization, the company already had stronger-than-average security controls in place. It had successfully implemented an NAC solution to enforce configuration policies for its corporate-owned and managed Windows devices, and it decided to extend its NAC policies to include personally owned devices. The NAC implementation was based on a solution from ForeScout. It was originally deployed in 2008, and it had grown to support over 100,000 PCs worldwide. The company's network infrastructure (mostly Cisco switches and wireless controllers) enforced the policies, based on commands that it received from the ForeScout NAC appliances.

The company identified three BYOD use cases. In each scenario, employees were required to register their devices via a Web portal, and a sponsor (typically the employee's manager) needed to approve the request

© 2013 SANS Institute. Author retains full rights.

before the device would be granted network access. The company developed a Web registration portal to automate the process.

Use Case 1 — Employee-Owned Tablet/Smartphone

Policies:

- An MDM agent is required for the device to gain access to a wireless BYOD network. Fiberlink's MaaS360 was selected as the MDM solution because of its integration with ForeScout. The Fiberlink solution provides device configuration and status information to the ForeScout management console.
- Employees can use any device that supports the Fiberlink agent, including Apple, Android, Windows and BlackBerry.

Actions:

- If the MDM agent is detected, the device is granted access to a separate wireless BYOD network. Citrix Systems' Receiver agent is used to grant access to a subset of applications on the corporate network, based on the user's profile, thereby creating a limited-access zone.
- If the MDM agent is not detected, the device is positioned on the guest network and is limited to Internet access only. (The user must register at the guest Web portal to gain Internet access).
- Jailbroken iOS devices and rootkitted Android and Windows devices are denied access to the network, including the guest network. The MDM agent determines if the device has been jailbroken or rootkitted.

Use Case 2 — Employee Brings Own Windows Laptop

Policies:

- Up-to-date patches are required.
- Up-to-date antivirus signatures are required (employees can select from an approved list of solutions at the company's expense, per corporate licensing agreements).
- Disk encryption is required (employees can select from an approved list).
- Specific ports must be blocked via a personal firewall (such as Telnet/SSH).
- ForeScout SecureConnector agent must be enabled (checks configuration status of endpoint).
- Vontu's data loss prevention (DLP) agent is required.

Actions:

- If the Windows laptop is compliant with all six of the policy criteria, it is granted full access to the corporate network.
- If the Windows laptop is noncompliant with one or more of the policies, it is positioned on the guest network and is limited to Internet access only. (The user must first register at the guest Web portal.)

© 2013 SANS Institute. Author retains full rights.

Use Case 3 — Employee Brings Own MacBook Laptop

Policies:

- It must be running OS 10.5 or later.
- ForeScout SecureConnector agent must be enabled.
- Vontu DLP agent is required.

Actions:

- If the MacBook is compliant with all three of the policy criteria, it is granted full access to the corporate network.
- If the MacBook is noncompliant with one or more of the policies, it is positioned on the guest network and is limited to Internet access only. (The user must first register at the guest Web portal.)

All three of the use cases also apply to contractors.

The company has embarked on a three-phase project:

- Phase 1 — A pilot project, in which 200 IT staffers brought personally owned devices to work. This phase lasted for six months, during which time the project team refined the Web registration portal and addressed early minor product integration issues with ForeScout and Fiberlink.
- Phase 2 — The project team broadened the program with the goal of supporting 1,000 employee-owned devices. Employees in the information risk management, and the risk and compliance departments were chosen to be part of this phase. The primary focus of Phase 2 was to assess the end-user experience and the overall performance of the solution. A secondary goal was to define and monitor role-based access.
- Phase 3 — The goal of Phase 3 is to open the project to all employees and contractors in the company. At the time of this writing, the company had just launched Phase 3. By year-end 2014, the company expects that the project will grow to over 10,000 personally owned devices.

Results

- Of those employees that use personally owned devices at work, approximately 80% have chosen to comply with corporate policies and install the required MDM agent and other software on their mobile devices. Those users that choose not to comply with the policy must register their devices at the guest portal on a daily basis, and are only allowed Internet access.
- At the time of this writing, approximately 1,000 employee-owned devices are present on the corporate network on a regular basis. Contractor-owned and personally owned Windows laptops are the largest category, representing about 85% of the noncorporate devices on the network. Smartphones and tablets represent about 10% of the noncorporate devices, and MacBooks represent about 5% of the noncorporate devices.
- The company did not add FTEs to support the BYOD initiative. One FTE (a ForeScout professional services consultant) is on-site and supports the broader NAC project. Using the ForeScout consultant minimizes the

© 2013 SANS Institute, Author retains full rights.

project's impact on internal FTEs and helps to shorten implementation cycles. The BYOD initiative has only resulted in additional endpoint growth of approximately 1%, so it is not surprising that the company did not need to add resources to support an already mature NAC implementation.

- Policy enforcement has gone relatively smoothly. For example, five employees reported that they lost their personally owned devices. According to the company policy, these devices were immediately wiped clean (the entire device; the company has not implemented containerization). The employees had signed waivers agreeing to the remote wipe policy. Because the policy was communicated clearly, the employees (grudgingly) accepted the fact that they lost personal content.

Critical Success Factors

- A mature NAC program contributed greatly to the success of the BYOD initiative. The knowledge and experience gained in establishing and enforcing NAC policies for corporate-owned Windows laptops enabled the company to extend network access policies to personally owned devices. Key factors that contributed to the success of the initial NAC project include:
  - A monitoring-only period of eight months, in which no policies were enforced. At the beginning of this period, approximately 11% of the Windows devices were noncompliant with corporate policy. By the end of the eight months, the IT department brought the number of noncompliant Windows devices down to 1%, and was able to enable policy enforcement (quarantining of noncompliant endpoints).
  - A two-year project rollout, which included three FTEs. The company believes that it could have implemented NAC more quickly, if it had been able to dedicate more FTEs to the project.
- Automating the classification of headless devices (such as printers and IP phones) was essential to scaling the initial NAC project to support 100,000 devices. All endpoints are automatically profiled when granted network access, and NAC policies are applied based on device type. The profiling function also helps with network visibility (such as the number of iPads, Android devices, etc. on the network).
- A BYOD council meets monthly to review requests for exceptions to the policies. The council consists of approximately 25 IT staffers across several disciplines (for example, compliance, risk management, networking, security, change management and others). When an application developer required periodic vulnerability assessments on its application, the council approved the request for an external auditor to scan the application servers, but required that firewall policies prevent the auditor from reaching other network devices.

© 2013 SANS Institute. Author retains full rights

Lessons Learned

- Effective communications are critical in the early stages of the BYOD implementation. The company was late in publicizing the BYOD initiative, and it began testing in a production environment before communicating the BYOD plan to its employees. The help desk became inundated with calls from employees with questions about policies and device registration. The company quickly realized that it should have informed its employees about the details of the program before it began production testing, and IT executives responded by implementing a communications and training program to update employees about the BYOD program. The company also made these changes to it processes:
  - The BYOD policy is outlined as part of the onboarding process for new employees.

  - The BYOD policy has been incorporated as part of the annual recertification process, in which all employees certify that they will abide by corporate IT policies.

- Requiring managers to sponsor employees' participation in the BYOD program helps to communicate the company's position that using personally owned devices at work is a privilege, and employees must comply with corporate policies. Initially, employees could register their devices and gain network access without needing approval from a sponsor. By requiring managers to sponsor an employee's participation in the BYOD program, the company was better able to manage and communicate BYOD policy changes. Managers sponsor employees via the registration portal, in response to an email alert.

- As a large organization, the company was able to influence its NAC vendor (ForeScout) to integrate with its chosen MDM vendor (Fiberlink). Not all organizations will have this luxury. For example, choosing an NAC vendor first will limit MDM options, if the goal is to integrate NAC and MDM. Choosing the MDM vendor first will limit NAC options. Enterprises should drive vendors toward broader NAC and MDM integration partnerships.

© 2012 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. The information contained in this publication has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information and shall have no liability for errors, omissions or inadequacies in such information. This publication consists of the opinions of Gartner's research organization and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice. Although Gartner research may include a discussion of related legal issues, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner is a public company, and its shareholders may include firms and funds that have financial interests in entities covered in Gartner research. Gartner's Board of Directors may include senior managers of these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see "Guiding Principles on Independence and Objectivity" on its website, http://www.gartner.com/technology/about/ombudsman/omb_guide2.jsp.

© 2013 SANS Institute, Author retains full rights

Last Updated: September 4th, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
Security Leadership Summit & Training	Dallas, TXUS	Dec 03, 2015 - Dec 10, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced