NEHEMIAH SECURITY

CASE STUDY

Mid-Sized Bank

At a Glance

Industry
Financial Services

Geography
Northeast United States

Mission
Extraordinary community banking

Challenges
- Reducing security risk by enforcing configuration compliance and ensuring consistency throughout the IT environment.
- Extensive manual auditing required by previous methods, which is labor intensive and lacking in precise answers about standards compliance.

Solution
Deploying AtomicEye ASM to quickly identify which endpoints in the environment are complying with standards and which are not—***even endpoints not connected to the network***.

Results
- Control gained over expanding environment without increasing IT staff
- Savings in time, labor and cost by eliminating manual audit processes.
- Improved security posture by establishing configuration standards throughout the organization.

Dramatically streamline security audits and empower policy compliance with AtomicEye ASM

Client Profile
With branch offices spanning the Jersey Shore, this mid-size East Coast bank prides itself on extraordinary community banking. Families and local businesses in central and southern New Jersey are the company's bread and butter. These bankers are active in their communities, volunteering for local causes and non-profits. In 1996, they launched a foundation, which has committed millions of dollars to over 600 charities and non-profit organizations in the communities the bank serves.

The Challenge: Inconsistent Configuration Settings Pose Security Threat
Like many growing organizations, the bank faced the challenge of gaining control over security standards for its endpoint devices. Not only was there a need to reduce vulnerabilities in the attack surface but also to demonstrate compliance. One specific area of concern was adherence to the Security Configuration Authentication Protocol (SCAP)– establishing secure configurations of systems to prevent unauthorized access. One familiar example (among hundreds of types of configuration settings) is having standards for password character length, complexity and frequency of change. Too often, organizations fall back on out-of-the-box default settings, which are not optimal when highly-sensitive data is at stake.

In the past, attempts to confirm configuration security required extensive manual auditing. The audit team selected systems at random,

looked at security policy configuration settings and compared them to a written list. “The audit process was taking too much time and labor,” recalls the Senior VP IT.. “And it did not really give us a complete picture of configuration security throughout our environment. We knew we needed to do better.”

The Solution: AtomicEye ASM and Security Expertise from Nehemiah Security

When launching an initiative to gain tighter control of its network endpoints, the bank engaged Nehemiah Security to consult on the project. Nehemiah’s AtomicEye ASM (Attack Surface Manager) gives organizations the ability to scan all network endpoints and uncover configuration anomalies—without the need for human intervention. These hard-to-detect aberrations can include a missing patch on a server, an unauthorized application, or inappropriate admin privileges. They can also involve an unusual open port or an unrecognized IP address—all indicators of a potential security vulnerability.

Nehemiah audited the bank’s implementation against the United States Government Configuration Baseline (USGCB), an extremely secure standard for Microsoft® Windows-based computers developed by the National Institute of Standards and Technology (NIST). USGCB settings are so secure, in fact, that they often interfere with applications and processing. As a result, these exacting settings must be tested extensively before they can be properly implemented. A key objective of Nehemiah’s audit was to confirm which of these settings were required for the bank’s security and compliance policies.

The bank rolled out approved USGCB settings across its organization based on group policies and rules. The key challenge was determining whether those rules had been properly implemented and were continuing to be adhered to. Prior to engaging Nehemiah, this process required an exhaustive, machine-by-machine search.

Enter AtomicEye ASM. The solution was used to evaluate each rule against the population of endpoints throughout the organization. This automated process ensured that a Windows-specific rule would not apply to a Linux-based or Apple computer. For endpoints affected by a given rule,

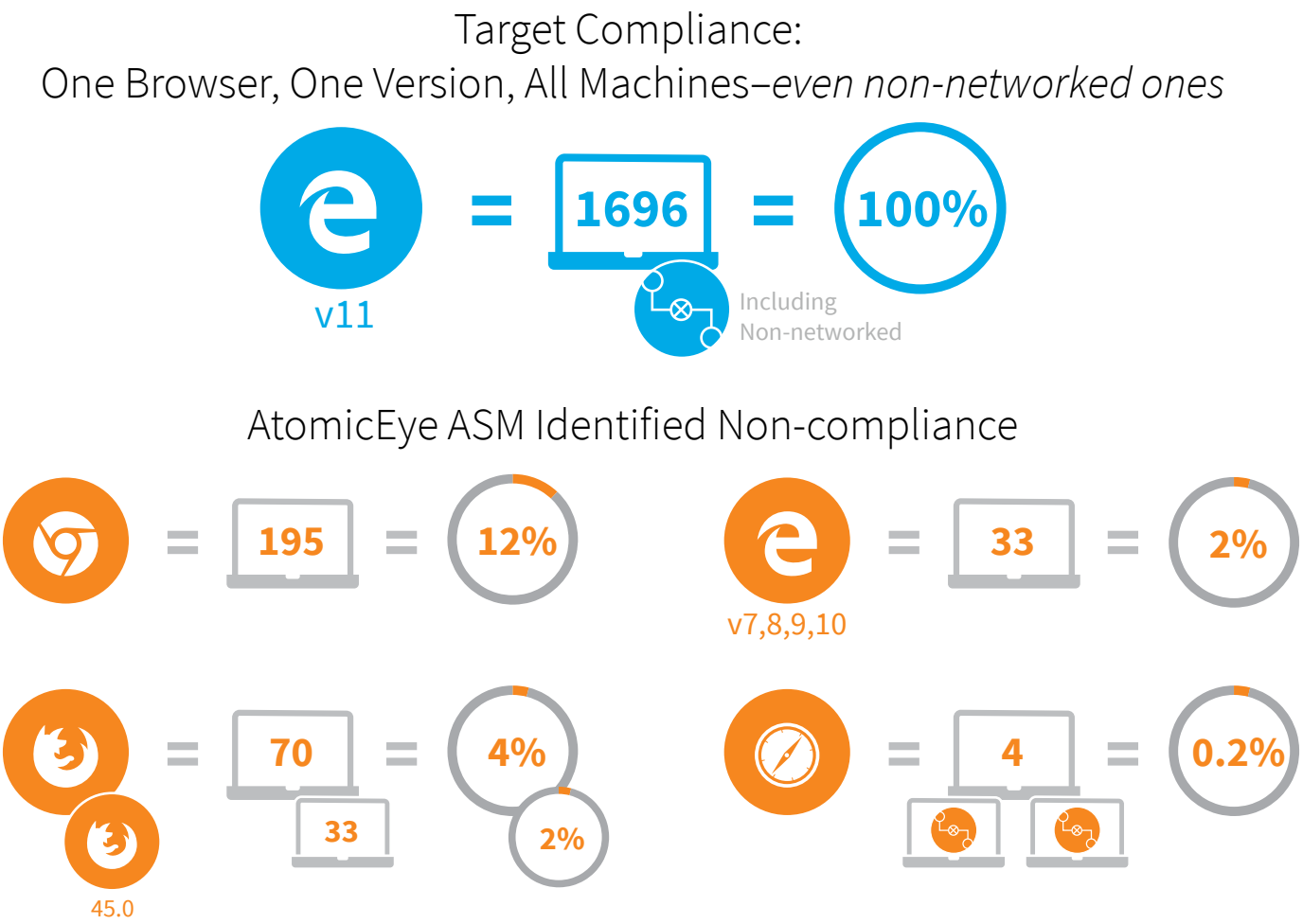
> *“AtomicEye ASM has saved us an* **incredible amount of time and effort** *in implementing configuration standards and auditing for compliance throughout our environment. It has given us a level of visibility that we simply did not have before.”*
>
> — Senior VP IT,
> Mid-size East Coast Bank

AtomicEye ASM ascertained which were compliant and which were not. As an example, for one particular rule the solution determined that 803 of 914 affected machines (88%) were compliant, while 111 were not. Armed with this knowledge, the IT team could focus on correcting the non-compliant cases rather than using their time manually searching for them. Multiplied by a set of around 180 rules, the time and labor savings turned out to be enormous.

The Results: A More Secure Environment through Greater Compliance and Simplified Audits

“We utilize AtomicEye ASM in two different ways,” the Senior VP IT explains. “One is to hunt down machines that are not compliant and convert them to regulatory requirements. The second is in our auditing. Not only are we better able to ensure that required standards are being implemented, but we can also verify ongoing compliance.”

Every week, the IT team receives a spreadsheet showing which machines are affected by each configuration rule,



Today's task: Making sure all machines are running Internet Explorer 11. How long would that take you to do? For AtomicEye, it can be a 10-minute automated task and includes endpoints that are not currently connected to the network.

which are compliant and which are not. It's all summed up with a compliance "score" representing the percentage of compliant machines.

Smoother post- acquisition transitions

This weekly compliance audit is critical to the bank's continued growth through acquisitions. The IT team can use AtomicEye ASM post-acquisition to quickly determine what is needed to transition the acquired systems to the bank's standards – avoiding a huge integration headache.

"At one point, we wanted to get everybody up on the current version of Internet Explorer," the Senior VP IT recounts. "AtomicEye ASM was able to generate reports showing all the different browsers and different version numbers of IE running in the environment. So it was easy to bring everyone up to the standard."

Not only can AtomicEye establish the browser and version for every machine in the system, it can do it for machines that aren't turned or or are otherwise disconnected from the network when the scan is conducted. AtomicEye evaluates rules against its master list of all endpoints. When it finds a machine that's not accessible, it pulls in data from the machine's most recent scan. This ensures the most complete results possible to maximize IT staff's efforts.

Above all, AtomicEye ASM verifies that hundreds of network endpoints – all potential attack surfaces – are no

longer vulnerable due to improper configurations.

"AtomicEye ASM has saved us an incredible amount of time and effort in implementing configuration standards and auditing for compliance throughout our environment," says the Senior VP IT. "It has given us a level of visibility that we simply did not have before."

More and more enterprises are utilizing AtomicEye ASM to gain control of their IT environment. It gives them greater visibility into their IT asset management practices. This strengthens their security posture and cuts the time and expense associated with security auditing. AtomicEye ASM enables organizations to quickly go from "soft" security to hardened systems with little effort. Based on this bank's experience, the system can be up and running within a month.

Not only can AtomicEye establish the browser and version for every machine in the system, it can do it for machines that are turned off or are otherwise disconnected from the network when the scan is conducted.

CONTACT

To discuss your security issues and find out how AtomicEye can solve them, contact 571-321-5350, option 1.