Securing today's enterprise from targeted attacks using Promisec Endpoint Manager, Portnox™ and HP ArcSight™

Control Access and Detect Cyber Incidents Without Deploying Agents

Today's Enterprise is under constant attack; whether from nation states or hacker groups, targeted threats are on the rise and they have their sights set on destroying your brand and stealing your customer's private data

The challenge: To find these advanced threats before they do damage

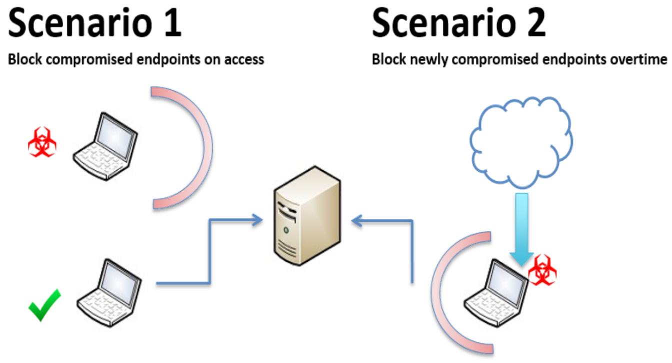
The problem: Advanced threats take advantage of one of the weakest links in layered security in that many security products do not communicate or operate together effectively to stop these threats from doing damage. The old adage "Security is a team sport" while true, goes completely out the window when the first time you hear your defenses have been breached is when MasterCard calls you to report fraudulent activity on a set of cards that all had transactions just prior at your business.

You do not need to look any further than what happened at Target Stores in late 2013 for an example of this. It has been widely reported that Target used an advanced threat detection product but that it wasn't tied into the rest of the infrastructure or the security operations to be effective at stopping the attackers from making off with millions of Credit cards. Furthermore, another aspect of this example that double underscores the importance of having a security solution stack that operates together is timing of the breach vs when it became known. Various sources have indicated that the hackers were inside Target's networks for months and started their nefarious actions right at the height of the Christmas shopping season where even just a few days' worth of transactions could net the hackers many, many millions of stolen accounts. Unfortunately this was the case, many completely innocent victims had their Credit Card information stolen and had to have their cards replaced.

How do you lower the risk of a targeted attack from happening in your environment?

Let's start with two scenarios that happen in nearly every customer environment:

1. Block compromised endpoints on access to a network resource
2. Detecting when an already authenticated client is compromised to block further access


Scenario 1
Block compromised endpoints on access
Scenario 2
Block newly compromised endpoints overtime

In a perfect world, you would stop all compromised systems from gaining access to network resources or connecting out of the network to exfiltrate data or post authentication detect they were compromised and remove their access to secured resource. Unfortunately if your endpoint security is not working tightly with your network security and access controls, these very universal scenarios are hard to detect and control.

The Promisec, Portnox and HP solution

To address these fundamental scenarios takes utilizing products that you likely already have in your environment (such as a NAC solution like Portnox and SIEM such as HP ArcSight) working with an advanced threat detection and remediation solution from Promisec.

The following scenarios highlight the key interactions of this solution:

Customer Success Stories

ZIM GLOBAL REACH LOCAL TOUCH Integrated Shipping Services Ltd

amdocs

Scenario 1: Block compromised endpoints on access

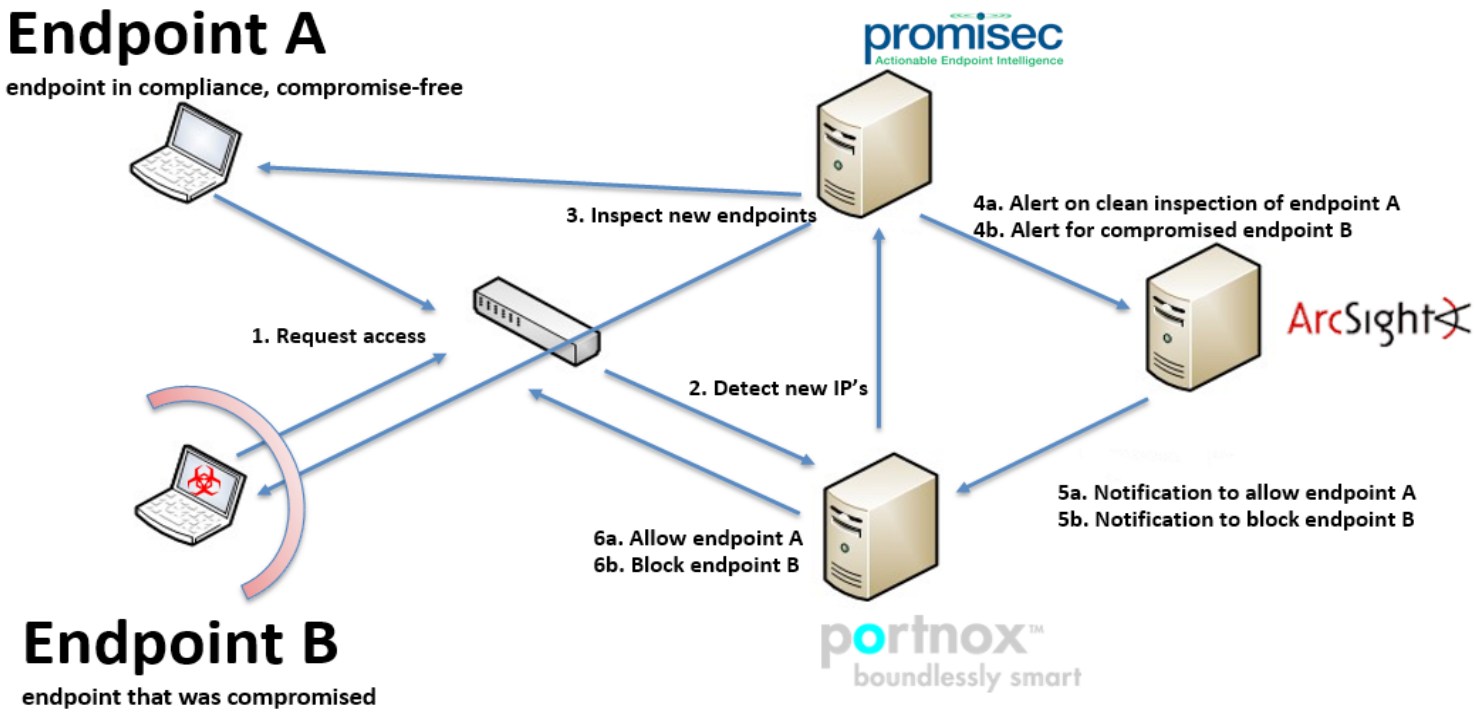
Imagine two endpoints accessing a network resource: one that is completely clean and compliant, the other is compromised. The combined solution of Promisec, Portnox and HP Arcsight will detect and handle this scenario every time.

Endpoint A: Clean endpoint

1. Endpoint A requests access to a network resource
2. Portnox detects access request and pushes IP to Promisec to scan the incoming system
3. Promisec determines that client 1 is clean and compliant with corporate security controls and notifies HP ArcSight
4. HP Arcsight notifies Portnox to allow access to resource
5. Portnox allows access to Endpoint A

Endpoint B: Compromised endpoint

1. Endpoint B requests access to a network resource
2. Portnox detects access request and pushes IP to Promisec to scan the incoming system
3. Promisec determines that client 2 has an issue with compliance or that it has a known malware onboard and notifies HP ArcSight
4. HP Arcsight notifies Portnox to NOT allow access to resource
5. Portnox blocks access to Endpoint B

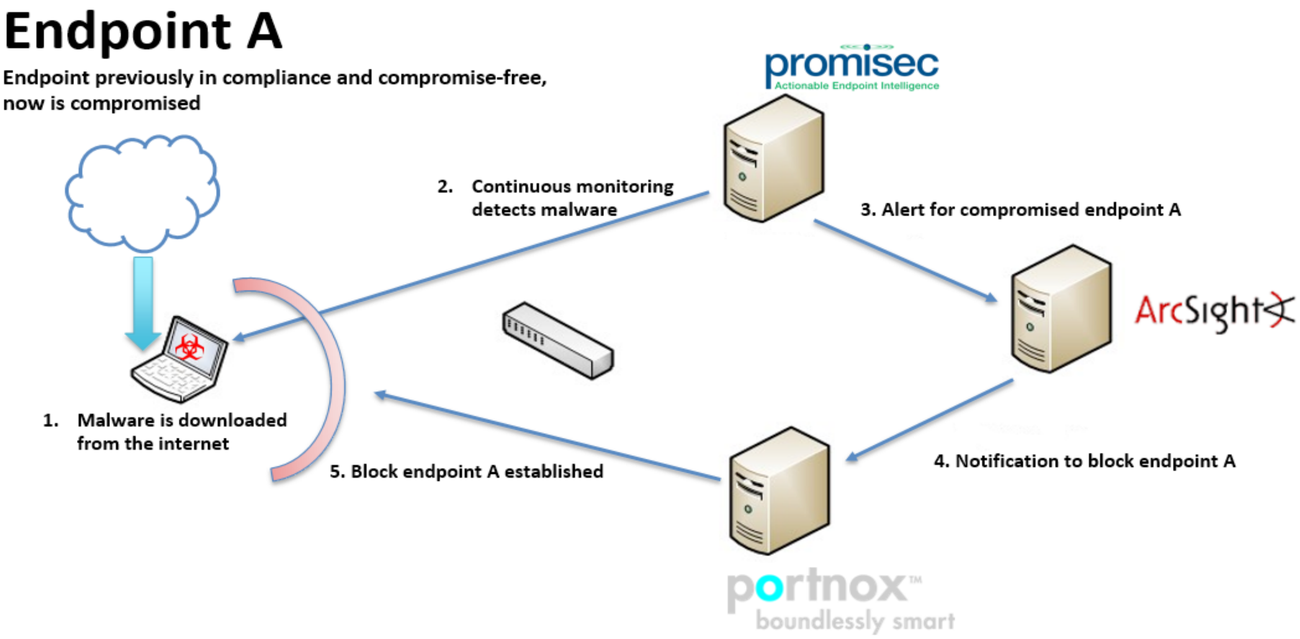

Endpoint A
endpoint in compliance, compromise-free
promisec
Actionable Endpoint Intelligence
3. Inspect new endpoints
4a. Alert on clean inspection of endpoint A
4b. Alert for compromised endpoint B
1. Request access
ArcSight
2. Detect new IP's
5a. Notification to allow endpoint A
5b. Notification to block endpoint B
6a. Allow endpoint A
6b. Block endpoint B
portnox
boundlessly smart
Endpoint B
endpoint that was compromised

Scenario 2: Block newly compromised endpoints after access was granted

Imagine a client that was previously granted access to a network resource but has become compromised. The joint solution will determine this scenario, shutdown access to the network resources and put the client on a private network to allow the Security Operations Center to further investigate.

Endpoint A: Once Clean Endpoint, Gets Comprimsed, Is Then Blocked

1. Endpoint A which was previously authenticated becomes infected with some new malware via a client side email attack or a drive by attack from their internet browser; the malware turns off the local AV service to prevent from being discovered and persists itself to survive a reboot.
2. Promisec, via continuous monitoring detects both the AV was turned off and a change in the file system from this malware and futher classifies this malware as a high alert item.
3. Promisec alerts HP Arcsight of the issue on Endpoint A in that there is a compromise by malware
4. HP Arcsight has a rule defined that indicates that it should remove (quarantine) this client from the network and notify the SOC team to investigate further.
5. Portnox receives this alert from HP Arcsight and removes this client from the network and access to the resources are terminated. It puts this client on a private network VLan that ensures that the client is accessible but only to the SOC team to investigate further.


Endpoint A
Endpoint previously in compliance and compromise-free, now is compromised
promisec
Actionable Endpoint Intelligence
2. Continuous monitoring detects malware
3. Alert for compromised endpoint A
ArcSight
1. Malware is downloaded from the internet
5. Block endpoint A established
4. Notification to block endpoint A
portnox™
boundlessly smart

Next Steps

Since these two scenarios are fundamentally about detecting and blocking when a bad actor in the form of a compromised endpoint might be trying to gain access to your network you can easily utilize them as building blocks for completing your security solution picture for both preventative measures and detective measures and in the process enable you to better handle advanced threats at the earliest possible time.

Contact Promisec to better understand what Amdocs, ZIM and other global blands are enjoying about this joint solution.

» Contact us:

Promisec USA
75 Second Ave, suite 140 | Needham, MA 02494 | 855.891.5854
sales@promisec.com | www.promisec.com

About Promisec

Promisec is a pioneer in endpoint visibility and remediation, empowering organizations to avoid threats and disarm attacks that can lead to unwanted headlines and penalties. Promisec's technology assures users that their endpoints are secure, audits are clean, regulations are met and vulnerabilities are addressed proactively to ensure the integrity of enterprise IT. More than 450 globally recognized companies trust in Promisec to stay secure and operationally efficient.