SEPIO

Merger and Acquisition

USE CASE

Background

In 2018, when exposed that unauthorized cybercriminals had been accessing millions of Starwood's guests' data since 2014, Marriott had to bear the brunt of the breach. Why? Marriott acquired Starwood back in 2016, and while this meant inheriting more hotels, it also meant inheriting Starwood's cyber risks.

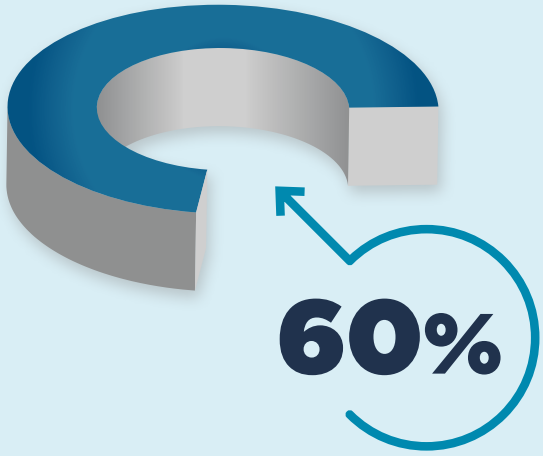
So, despite the attack being initiated two years before the acquisition, it was Marriott's responsibility to accurately assess Starwood's cyber posture prior to integration. Failure to do so means that any cyber incident that occurs post-acquisition falls on the acquiring company. This incident is one of many that demonstrate the cybersecurity blind spot of the Mergers and Acquisitions (M&A) process.

COVID-19 has had a financial impact on almost all organizations. While this has caused an overall decline in M&A, many companies were forced to merge with, or be acquired by, another enterprise to remain in business. Hence, the cybersecurity risks of M&A remain prevalent and are only going to increase as the world recovers (financially, physically, mentally, you name it) from COVID and begins to engage in more M&A.

Attack Study – Merger and Acquisition Cybersecurity Risks

A report on the cybersecurity risks of M&A by Forescout showed that 62% of organizations agree that they face significant cybersecurity risks when acquiring new companies and that cyber risk is the greatest concern following the acquisition. For the former, cyber risks increase during the process as data and money are being transferred, which puts them in a more vulnerable position to be stolen by malicious cyber actors. More than half of acquiring companies experience a critical cybersecurity issue or incident during the M&A process. As for the latter, any cybersecurity risk associated with the target enterprise (the one being acquired) becomes the responsibility of the acquiring company. Enterprises need to know what they are acquiring – it is not only the company and its products/services but a myriad of other aspects, including cyber risks. Hence, the acquiring company must perform a comprehensive cyber assessment on the target company before integration to account for any cyber risks and to take the necessary actions to mitigate such risks. However, enterprises struggle with a lack of device visibility meaning that both parties struggle to gather the necessary information for an accurate and comprehensive cyber assessment.

Cybersecurity posture considered a critical factor in the due diligence process by 2022



Cybersecurity is Critical to the M&A Due Diligence Process, Gartner, April 2018

The importance of cybersecurity during M&A deals is increasing. According to Gartner, by 2022 60% of organizations will consider cybersecurity posture a critical factor in their due diligence process. Additionally, Forescout's report highlighted that the second most significant factor when performing due diligence on M&A targets is the history of their cybersecurity incidents. However, eight in ten organizations discover a previously unknown or undisclosed cyber-related issue following integration, with a lack of asset visibility often being the cause of the former. Those which do get detected may be inaccurately assessed based on incomplete information due to a lack of asset visibility. For example, a data breach could be incorrectly attributed to a phishing email when it was in fact caused by a Rogue Device that went under the radar of security tools. If you do not know it is there, how would you know it caused an attack?

Additionally, Forescout's research found that many cyber assessments were conducted as a point-in-time exercise rather than a continuous process, which such an assessment needs to be. Furthermore, according to IBM's assessment of cyber risks in M&A, almost 60% of organizations performed a comprehensive cybersecurity assessment after the due diligence process. In other words, the assessment was performed during the transaction execution and integration processes, which is at much too late a stage. As a company's assets can become vulnerable at any point during the M&A process, there needs to be constant, real-time monitoring from beginning to end.

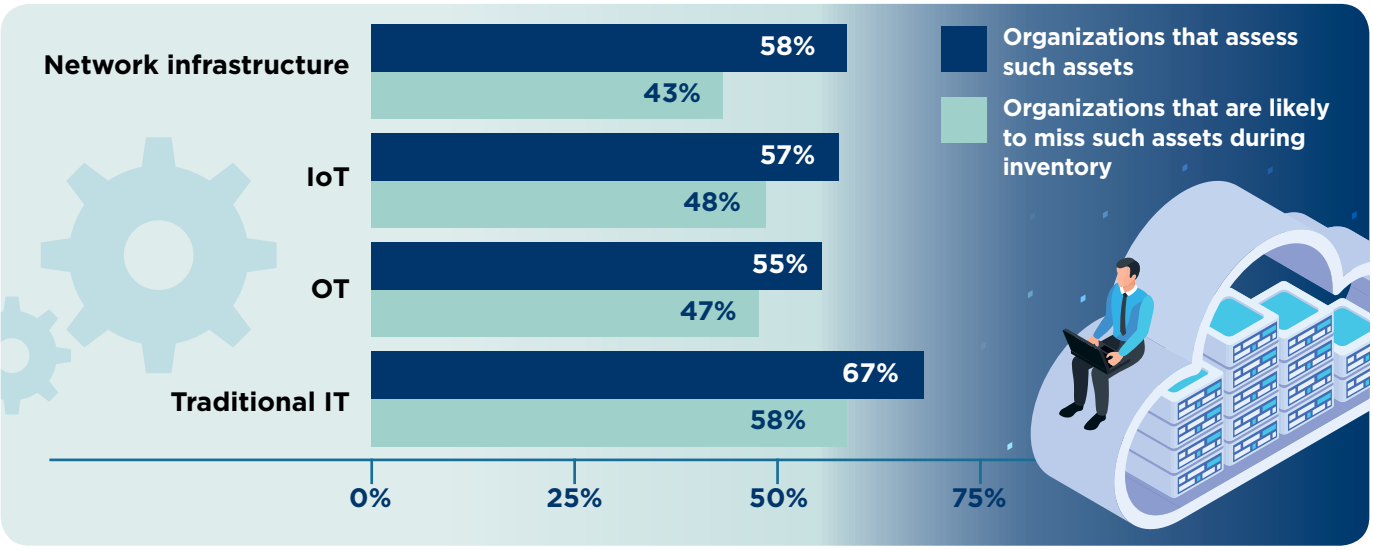
The Risks of Connected Devices

For 50% of organizations, connected devices are deemed the greatest risk during the technology integration process

The Role of Cybersecurity in Mergers and Acquisitions Diligence, Forescout, 2019

For half of organizations, connected devices put them most at risk during the technology integration process. The more connected devices there are, the greater the risk. Hence, asset inventory is an essential component of the M&A process. However, just as the target organizations face asset visibility challenges, so do the acquiring organizations. The efficacy of a cyber assessment is extremely limited if the acquiring organization struggles to comprehensively identify and track every connected device.

Without complete visibility, the enterprise does not know what it is inheriting – whether that be an asset already carrying a cyber risk or a vulnerable device that can present a risk to the company in the future. The chart below highlights organizations' gaps in asset assessment and inventory during new acquisition evaluation.



Tools used

While these stats might seem average, when it comes to a comprehensive cyber assessment, average does not cut it. With such worrisome numbers, it is unsurprising that 53% of organizations discovered unaccounted for devices after completing the integration of a new acquisition, and Forbes reports that 40% of acquiring organizations found a cybersecurity issue following integration. Ineffective due diligence means that the company does not really know what it is acquiring; it cannot protect itself against something that it does not know exists. However, device visibility challenges go deeper than those that were simply not assessed or missed during inventory.

Not only are organizations struggling to account for every hardware asset, but attackers are turning to hardware attack tools which operate on both USB and network interfaces. Such devices are covert by nature and operate on the Physical Layer, going under the radar of existing security solutions such as NAC and IDS.

Rogue Devices operating on the USB interface have spoofing capabilities, allowing them to impersonate legitimate HIDs which raises no security alarms. So, if the IT department cannot detect the presence of a Rogue Device, nor can the security tools in place, the acquiring organization is unable to make an accurate cyber assessment. Similarly, as mentioned, the acquired organization faces the same challenge and might be unable to accurately report its cyber incident history. As a result, the acquiring company will likely inherit far more cyber risks than it thinks.

As hardware-based attacks require the perpetrator to gain physical access to the organization, the M&A process is an ideal method of infiltration in a similar way the supply chain is often used. By targeting the acquired organization, attackers can infiltrate the acquiring company once the two entities integrate.

However, in other cases, the acquired company itself might be the target of many cybercriminals and, by procuring it, the acquiring company has inadvertently made itself a target. Retailers, for example, have been hard-hit by COVID and many have had to be acquired by larger enterprises in order to remain open. Retail, however, is one of the most targeted industries for cyberattacks, with 72% of retailers being hit. Hence, the acquiring company now takes on that risk. And without complete asset visibility, the enterprise has no way of knowing the full extent of the risks it is inheriting.

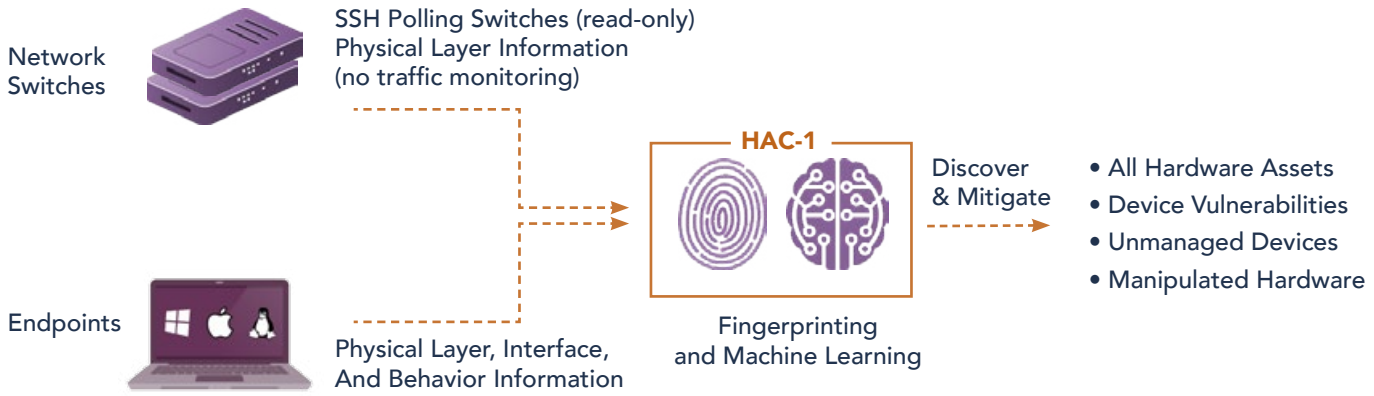
HAC-1 SOLUTION

Sepio's Hardware Access Control solution (HAC-1) provides a panacea to the gap in device visibility. As the leader in Rogue Device Mitigation, Sepio's solution identifies, detects, and handles all peripherals; no device goes unmanaged. This allows for a complete asset inventory of all IT, OT and IoT devices operating on both USB and network interfaces.

There is no longer the risk of certain assets going unassessed or missed during inventory. Furthermore, HAC-1 uses Physical Layer fingerprinting technology and Machine Learning to calculate a digital fingerprint from the electrical characteristics of all devices and compares them against known-to-be-vulnerable devices through its extensive built-in threat intelligence database. In doing so, HAC-1 not only detects all managed, unmanaged, and hidden devices operating within the enterprise's infrastructure, but also reveals devices' true identity. As such, HAC-1 automates a thorough cyber assessment that continues throughout the entire M&A process.

Moreover, the comprehensive policy enforcement mechanism recommends best practice policy and allows the administrator to define a strict, or more granular, set of rules for the system to enforce. When a device breaches the pre-set policy, HAC-1 automatically instigates a mitigation process that instantly blocks unapproved or Rogue hardware. So, whether the device is present prior to the M&A process, or it is inserted during it, HAC-1 provides organizations with constant, real-time protection that does not just stop post-acquisition. We will be there as long as you will have us; and we are confident you will want us long after the M&A process is over.

How It Works



HAC-1 - Visibility & Security of Hardware Assets

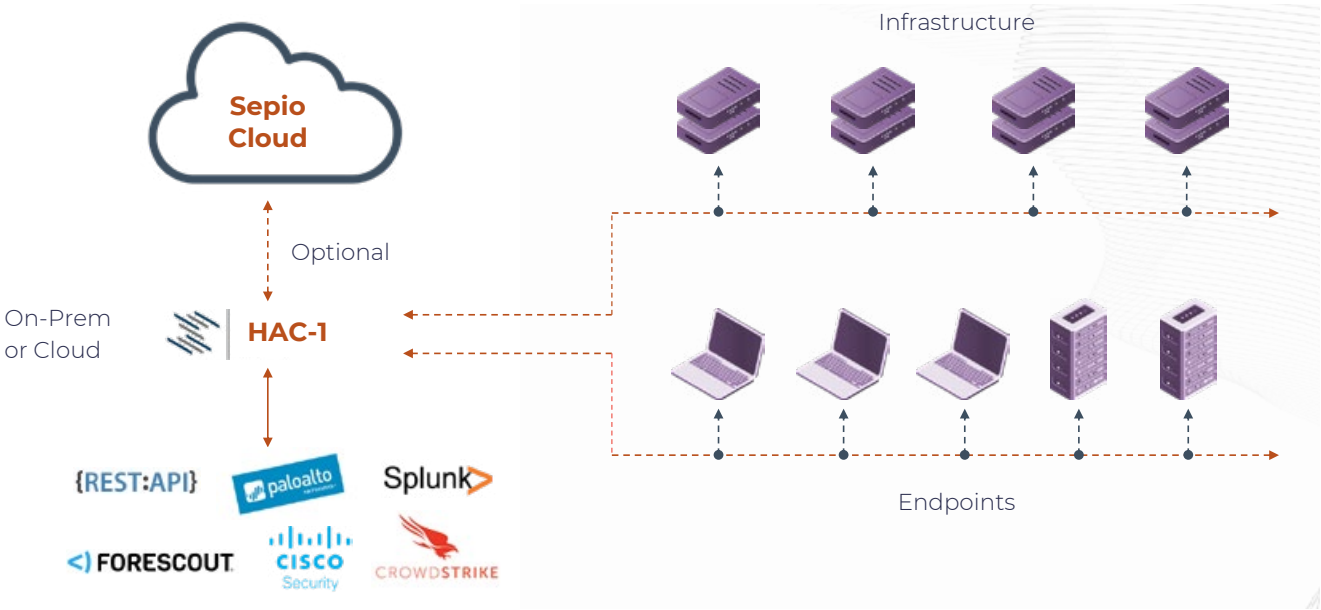
Main Benefits

Complete Visibility of all Hardware Assets: With all devices and anomalies detected, enterprises benefit from a greater overall cybersecurity posture. Gaining full visibility of all hardware devices from endpoint peripherals to connected devices (IT/OT/IoT), Sepio uses unique physical layer hardware fingerprinting technology and data augmentation from endpoints and networks.

Full Control through Predefined Policies: Enterprise-wide policies enable compliance, regulation and best practices. With predefined templates and no baselining or whitelisting, and no requirement for a clean environment start, Sepio provides a fast and easy setup.

Rogue Device Mitigation (RDM): Threat mitigation upon discovery of rogue or threatening devices. Integrations with existing security platforms such as NACs and SOARs for mitigation and remediation enhancements.

System Architecture



About Sepio

Sepio delivers a Hardware Access Control (HAC) platform that reduces the risk of unapproved and Rogue Devices by providing complete visibility, control, and mitigation of all hardware assets. Sepio's hardware fingerprinting, augmented by machine learning, discovers all managed, unmanaged, and hidden devices that are invisible to all other security tools. Sepio's HAC-1 solution enhances Zero Trust, insider threat, BYOD, IT, OT and IoT security programs.

LEARN MORE


access denied