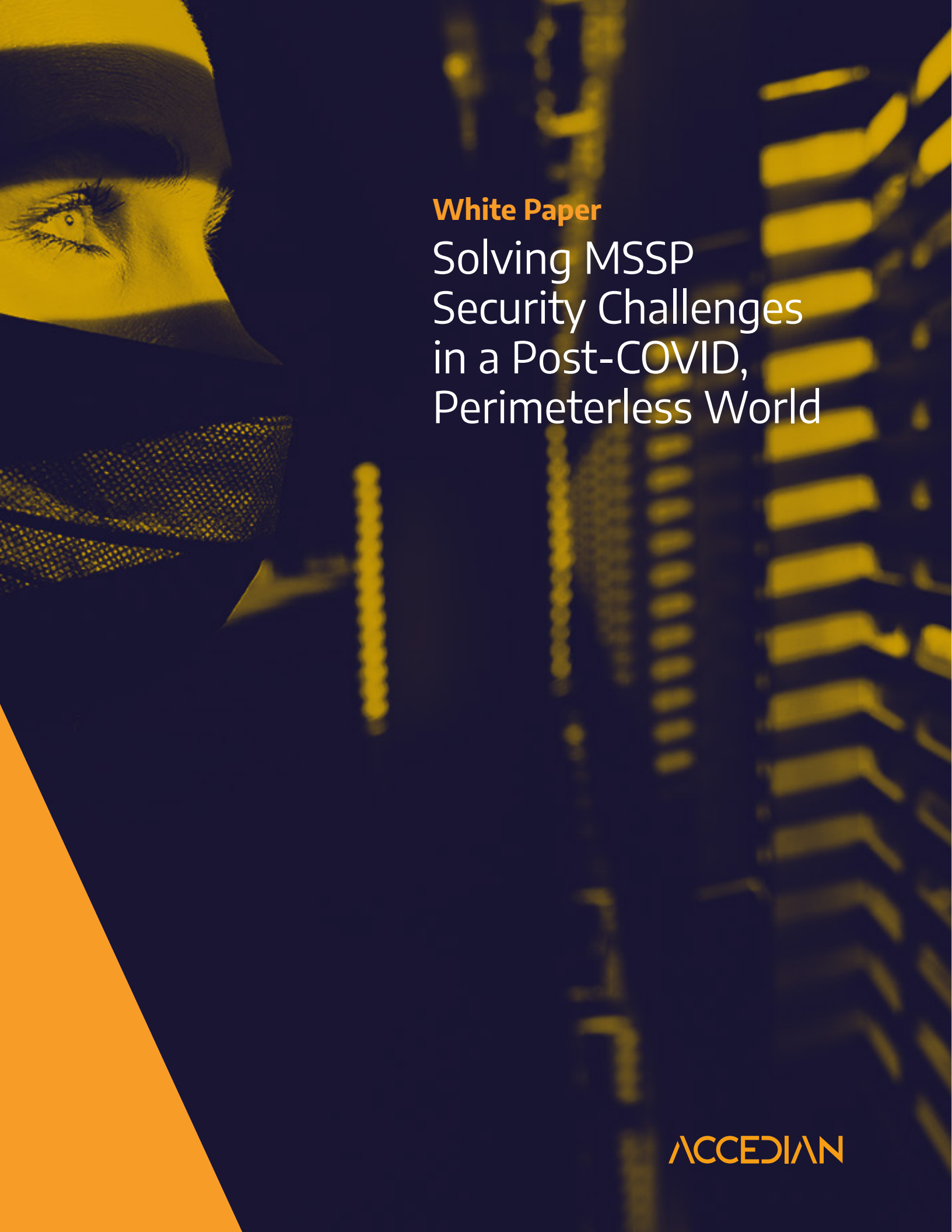

White Paper

Solving MSSP Security Challenges in a Post-COVID, Perimeterless World

ACCEDIAN

Introduction

After more than 25 years of innovation in cybersecurity, organizations still find themselves on the back foot. In many ways, that's because the attackers are doing a better job of innovating. Backed by an underground economy estimated to be worth $1.5 trillion annually, they've been highly successful in forcing CISOs and security vendors into a continuous reactive mode.[1]

Ransomware attacks soared by 365% year-on-year in the second quarter of 2019, as cyber-criminals targeted businesses with phishing lures, software exploits and attacks on RDP infrastructure.[2] The average ransom payment is now said to exceed $111,000, although this figure is a reflection of the large number of attacks on SMEs which lead to lower overall ransom charges on average.[3] Attacks on large multinationals can easily cost tens of millions.[4] At the same time, over 100 million attacks on IoT endpoints were detected in the first half of 2019 alone, as factory default log-ins and firmware vulnerabilities exposed a growing number of organizations.[5] With 5G promising a new wave of IoT deployments, this malicious activity is likely to be just the tip of the iceberg.

Data breaches at big-name brands remain an ever-present feature of news headlines, although many more smaller companies are also impacted.

Some 8.4 billion records were exposed in Q1 of 2020 – a 273% year-on-year increase, and the largest figure since records began.[6]

It's not just end-customers that are being targeted either. Increasingly, MSSPs themselves are under attack for the data they hold and as a conduit for malware distribution to customers.[7]

The challenge of mitigating the financial, reputational and compliance risks that result from such threats is made harder still by the continued push for digital transformation. Migrating apps and infrastructure to the cloud is too often a strategic initiative without input from the security department, leading to problems later on. This only serves to expand the corporate attack surface, inviting security breaches which ironically can end-up derailing further digital investments.

In this new cloud-first, perimeter-less environment, organizations have struggled to find the right tools to provide the visibility and control they need to preserve innovation-fuelled growth while mitigating risk. They need MSSPs to help them navigate the new landscape with advanced security services. Unfortunately, the legacy intrusion detection systems (IDS) still widely in use today are no longer fit-for-purpose. They're unable to catch unknown threats or monitor for lateral movement, and burden customers with excessive manual processes and logging costs.

The bottom line is that MSSPs need differentiated solutions to protect both their customers and their own networks — low cost, easy-to-deploy and manage products designed to uncover sophisticated threats across cloud and on-premises environments. In a new era of COVID-related business uncertainty and cost containment, they must look for better.

Key takeaways:

- In a world of advanced threats and highly professionalized cybercrime, legacy intrusion detection solutions are failing to protect MSSPs' customers and can add excessive costs
- Today's post-COVID world requires a greater focus on cost containment, leading MSSPs to consider third-party security providers who can integrate seamlessly into existing offerings
- MSSPs are increasingly a target for cyber-attack themselves, making it more important to find a partner who can offer protection to both service provider and its customers
- Next-gen intrusion detection (IDS) featuring network traffic analysis technology, which is also a key capability for Network Detection and Response (NDR), is the smart choice for MSSPs looking to differentiate on advanced cybersecurity that's easy to deploy and manage, whilst bolstering in-house protection and driving down TCO

Digital first, perimeter-free

[1] www.bromium.com/wp-content/uploads/2018/05/Into-the-Web-of-Profit_Bromium.pdf
[2] blog.malwarebytes.com/reports/2019/08/labs-quarterly-report-finds-ransomware's-gone-ram-pant-against-businesses/
[3] www.coveware.com/blog/q1-2020-ransomware-marketplace-report
[4] www.computerweekly.com/news/252467199/Norsk-Hydro-cyber-attack-could-cost-up-to-75m
[5] www.kaspersky.com/about/press-releases/2019_iot-under-fire-kaspersky-detects-more-than-100-million-attacks-on-smart-devices-in-h1-2019
[6] www.riskbasedsecurity.com/2020/05/11/no-of-records-exposed-in-2020-q1-data-breaches-skyrockets-to-8-4-billion/
[7] www.blackberry.com/us/en/products/resource-center/2020-threat-report

1. Room for improvement – key MSSP challenges

Traditional network security tools offer some form of protection for MSSP customers. But firewalls, IDS, endpoint AV, and gateways are a patchwork of siloed point solutions which don't provide the context and insight CISOs need to mitigate cyber-risk effectively. Crucially, they don't provide visibility into the network once attackers have managed to get inside, which they could achieve via a number of techniques (phishing, credential stuffing, RDP brute force, etc.)

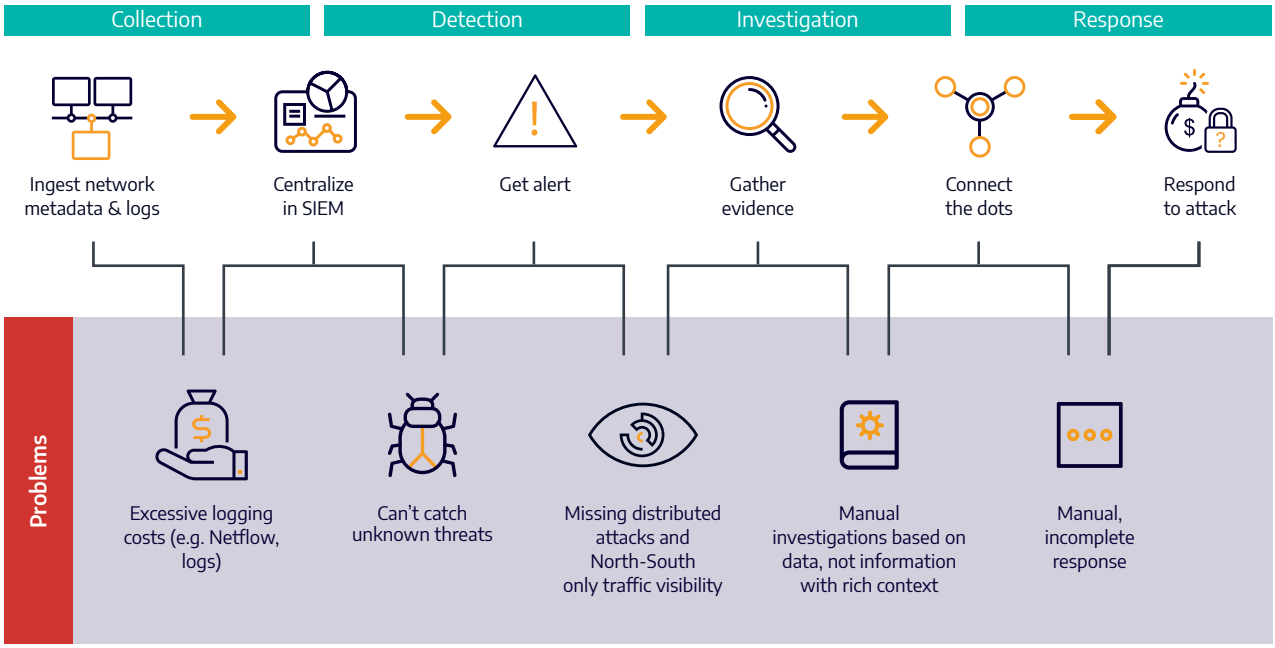

Figure 1: Legacy SIEMs cause challenges at each step

Further, legacy IDS has several deficiencies. Significant costs are incurred from logging vital data, and major manual effort is needed to then evaluate this data. Manual investigation and response processes lack context and insight as the system can't detect unknown threats and only provides North-South visibility. It's no surprise that today the average time to identify and contain a breach is 280 days.[8]

MSSPs instead need a new approach to network intrusion detection that is integrated, automated, and designed from the ground-up to provide insight into advanced threats and suspicious behavior across cloud, on-premises and network edge environments. Tools must be cost effective, easy-to-install and manage and highly scalable.

[8] www.ibm.com/security/data-breach

2. Cost and COVID

TCO has always been a key driver for MSSP purchasing decisions. But in today's post-COVID world, it's more important than ever for MSSPs and their customers.

To deploy security capabilities to their customers, MSSP delivery architectures usually feature a combination of or all of: network and performance monitoring, SIEM management, firewall management, anti-virus, endpoint security, IDS management, vulnerability testing, and penetration testing. In utilizing these solutions, they would typically conform to one of three basic set-ups:

1. A custom set of software developed in-house
2. An off-the-shelf combination of third-party vendors (Fortinet, SolarWinds, Alert Logic, etc.)
3. A hybrid model featuring both bespoke and off-the-shelf components

There's a major cost associated with developing these capabilities in-house. The threat landscape is volatile and fast-changing, meaning products must be constantly reiterated and new features added to keep pace. That becomes a significant financial burden for MSSPs.

Today's "new normal" business environment requires caution and a focus on cost containment without sacrificing functionality. That makes it increasingly important to look for vendors who integrate neatly with homegrown systems, deploy rapidly, and require minimal ongoing management. In this way, the third-party provider does the heavy lifting in developing new features and functionality, lowering TCO for the MSSP whilst still ensuring an optimized experience for their end customers.

3. MSSPs are now a target

Another important factor to consider is whether the security solutions MSSPs are looking to deliver to customers can also be deployed to protect their own environment. Sophisticated attacks on service providers have become an increasingly common occurrence in recent years. These range from potentially state-sponsored attempts to steal data from customers, to financially motivated ransomware efforts.[9] Cognizant revealed earlier this year that a ransomware attack may end up costing the firm $50-70 million in Q2 of 2020.[10]

Whatever the end goal, the Department of Homeland Security has been warning about such threats since 2018.[11] IT security professionals now rank MSPs top of the list of concerns regarding third-party access to systems.[12]

The bottom line: MSSPs need sophisticated intrusion detection tools to offer 2-in-1 protection, of their own IT systems and those of their customers.

[9] www.pwc.co.uk/issues/cyber-security-services/insights/operation-cloud-hopper.html
[10] cognizant.q4cdn.com/123993165/files/doc_financials/2020/q1/Q120-Earnings-Supplement_vF-(Website).pdf
[11] us-cert.cisa.gov/ncas/alerts/TA18-276B
[12] smartermsp.com/cybersecurity-attacks-aimed-at-msps-are-taking-a-toll/

4. Introducing Accedian

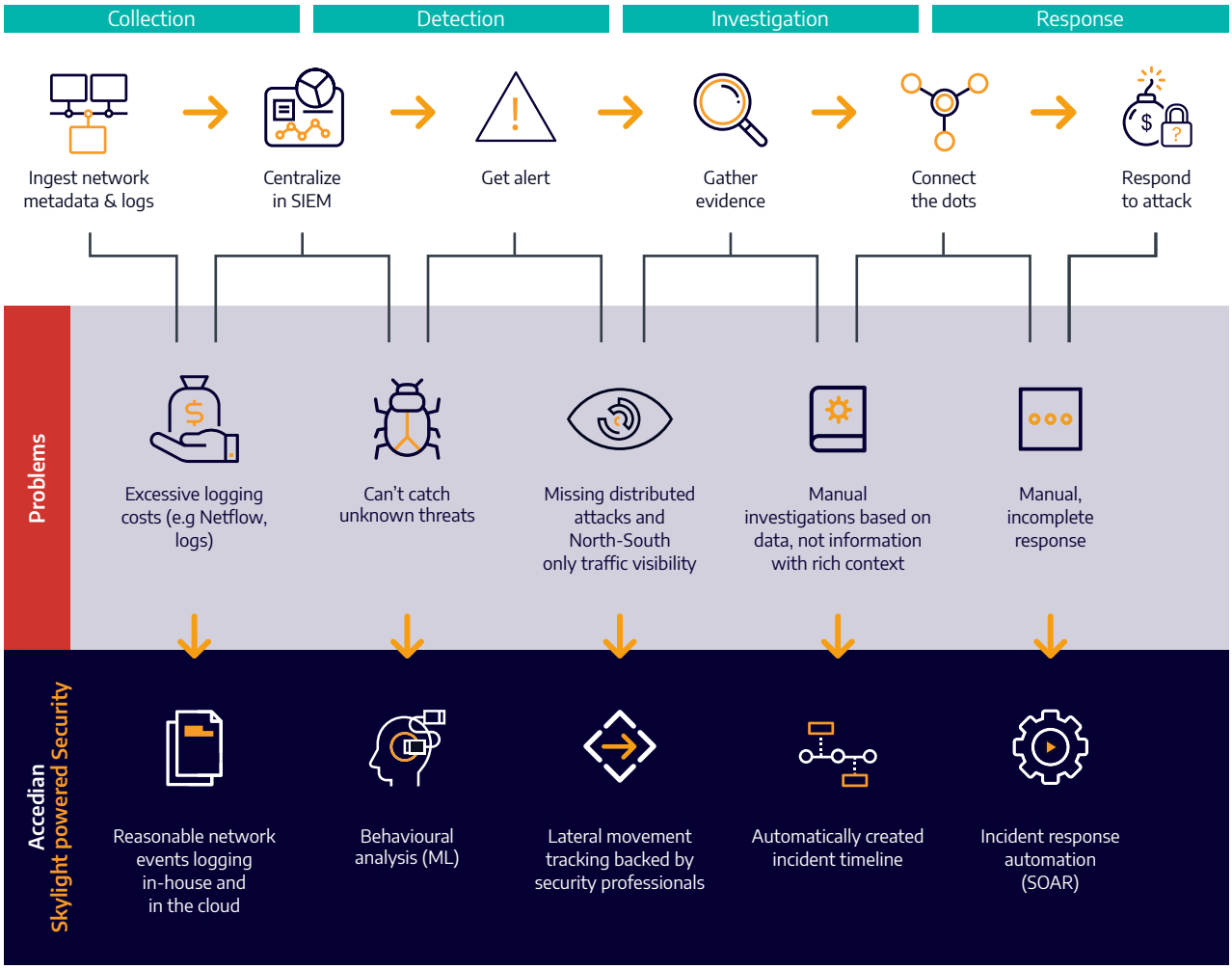

Figure 2: Solving SIEM challenges

Accedian's Skylight™ powered Security capabilities offer a winning combination of network traffic analysis, or NDR, for real-time visibility across complex environments, with open integration and simple SaaS deployment.

It all starts with the data. Rule-less Skylight sensors collect intelligent per-packet intel™, or metadata, to keep traffic capture and retention lightweight, reducing the performance and cost impact. Capable of handling network links of 10GB+, they capture 100% of transactions across network levels Layer 2-7 for comprehensive visibility across on-premises, cloud, private DC, IoT and other environments.

Next come advanced analytics. Skylight uses machine learning to provide statistical, signature, and anomaly threat and behavior detection. This enables: threat detection, investigation, hunting, and alert management; early cyber kill chain warning signals, and high fidelity forensic data. It's visibility on a whole new level, including lateral movement tracking, that traditional IDS and network security point solutions can't match.

The platform matters too. That's why we designed Skylight with an open architecture to integrate neatly with MSSPs' own delivery architectures, as well as third-party threat intelligence feeds. A SaaS deployment option means the platform is viable for all IT environments — cloud, on-premises data centers and hybrid — and can be installed in minutes. Sensors are free-of-charge and can be deployed to multiple MSSP customers via a single license, further streamlining management.

In summary, Accedian Skylight powered Security empowers MSSPs with:

- Two-in-one protection for their own environment and their customers
- Superior network traffic analysis-based detection capabilities to tackle advanced threats
- Ease of deployment and management
- A major differentiator, by serving enterprise-grade security to the mid-market
- Support for customers' digital transformation
- Seamless integration with in-house delivery architecture for low TCO

To find out more on how Accedian Skylight powered Security can drive value for your organization and customers, visit **accedian.com**

About Accedian

Accedian is the leader in performance analytics and end user experience solutions, dedicated to providing our customers with the ability to assure their digital infrastructure, while helping them to unlock the full productivity of their users.

Learn more at accedian.com

Accedian | 2351 Blvd. Alfred Nobel, N-410 | Saint-Laurent, QC H4S 2A9 | 1 866-685-8181 | **accedian.com**