ACCEDIAN

Guide
Next-Gen Intrusion Detection: A new security approach to unlock value and drive down risk

Introduction: Legacy security leaves firms high-and dry

While the world works from home, cyber-criminals continue to do what they do best. Ransomware cases are estimated to have increased 20% in the first half of 2020 to top 121 million attacks.[1] The number of corporate records exposed in Q1 2020 alone soared 273% year-on-year to reach 8.4 billion.[2] In their wake, these attacks have left victim organizations reeling from the cost of lengthy service outages, investigation and clean-up and reputational damage — at a time when they can least afford it.

The global average cost of a data breach is now $3.9M,[3] but some organizations have revealed losses in the tens of millions from serious ransomware attacks.

The global average cost of a data breach is now:
$3.9M

121 million
ransomware cases in the first half of 2020

Why read this paper?

- Global organizations are being over-whelmed with cyber-attacks, resulting in serious reputational and financial damage
- Digital transformation, including cloud investments, are creating complexity and expanding the corporate attack surface
- Legacy IDS tooling is no longer fit-for-purpose as it can't spot unknown threats and adds excessive cost
- Next-gen IDS leveraging network traffic analysis delivers a new approach, providing rapid detection and response of sophisticated threats to minimize breach cost and preserve corporate reputation

[1]https://www.channelpro.co.uk/news/11834/121-million-ransomware-attacks-recoreded-in-the-first-half-of-2020#:~:text=Ransomware%20cases%20around%20the%20world,5.9%20million%20in%20the%20UK.
[2]https://www.riskbasedsecurity.com/2020/05/11/no-of-records-exposed-in-2020-q1-data-breaches-skyrockets-to-8-4-billion/
[3]https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/

This is where next-generation intrusion detection (IDS) comes in. Leveraging machine learning-powered network traffic analysis, now commonly referred to in the industry as Network Detection and Response (NDR),[4] it is designed to:

- Shine a light on the entire IT environment, to spot suspicious behaviors and unknown threats before they can make a serious impact
- Accelerate and enhance incident response
- Effectively mitigate cyber-risk
- Minimize the resulting financial and reputational impact of breaches on the organization

Here we explain everything you need to know about next-gen IDS tools and the key questions you need to ask of prospective vendors.

Threats evolve as the attack surface expands

COVID-19 has given new emphasis to the push for digital transformation. One study claims the pandemic has already accelerated the digital communications strategy of global firms by as much as six years.[5] Another reveals that 82% of companies have increased their use of cloud services in direct response to the crisis.[6]

These trends are having an unintended consequence: as IT infrastructure becomes more complex and distributed, security gaps start to appear which allow threat actors to sneak in. Three factors should be ringing the alarm bell.

1. **First**, it's increasingly challenging for IT teams to determine how business-critical applications are delivered at scale globally, and how best to protect them.
2. **Second**, mass remote working means even more potentially unsecured endpoints for attackers to target.
3. **Third**, threat actors are increasingly taking advantage of organizations, thanks to a thriving underground cybercrime economy that provides a ready-made market for stolen data and an exhaustive source of expertise on hacking tools and techniques.

[4]Source: Gartner

[5]https://www.computerweekly.com/news/252486191/Covid-19-accelerates-UK-digital-transformation- efforts-by-over-five-years

[6]https://www.computerweekly.com/news/252484865/Coronavirus-Enterprise-cloud-adoption-accelerates-in-face-of-Covid-19-says-research

As a result, Advanced Persistent Threat (APT) tactics, once the preserve of nation states, are increasingly common — and not just used in high-profile data-stealing raids against large organizations. SMEs are often targeted as a "stepping stone" for threat actors to target along the way to getting access to more valuable organizations with whom they may partner, or in their own right, due to the perception that SMEs are less well defended. Even ransomware groups are starting to adopt APT tactics to first steal data and then infect corporate systems.[7] By phishing employee log-ins or buying them from the dark web sites, attackers can gain a foothold into victim organizations without setting off any alarm bells.

If they aren't detected in time, the business may suffer a serious breach leading to:

- Costly remediation, investigation and clean-up (potentially requiring expensive third-party expertise and IT overtime)
- Major service outages and bad publicity, resulting in customer attrition
- Productivity losses during outages and incident response processes
- Regulatory fines
- Legal costs from possible class action suits
- Brand damage and reputational impact, potentially impacting share price

average time to identify & contain a breach today

280 days

Legacy solutions aren't up to par

The problem facing business leaders is that the tooling used by their IT department is often ill-equipped to cope with the new reality of advanced threats and cloud-centric architectures. The old "hub-and-spoke" model for network security, where monitoring and controls are centralized, is no longer fit-for-purpose in a new era of mass remote working and distributed computing. It leaves simply too many blind spots for hackers to exploit.

Now with digital transformation, hybrid cloud and multi-cloud infrastructure models are becoming the norm, creating security threat visibility challenges, as each public cloud provider has their own shared security model.

While traditional signature-based IDS techniques can be useful for known signatures, they are unable to detect the ever-evolving changes in signatures that threat actors employ over 80% of the time. These tools rely on manual analysis by stretched IT security teams which lack context. They even add excessive costs through the way they capture logging data.

The result: attacks can too easily fly under the radar, resulting in a breach of the perimeter.

Attackers then maintain persistence inside the corporate network until they have achieved their goals. The average time it takes to identify and contain a breach today stands at 280 days.[8] The longer the bad guys are inside your network, the more data they can steal and the more files they can encrypt with ransomware.

This is bad news for the bottom line and corporate reputation.

[7]https://threatpost.com/lazarus-group-apt-tactics-ransomware/157815/
[8]https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/

Four reasons to invest in next-gen IDS

Next-gen IDS is different, for four key reasons:

1. It provides maximum visibility across the entire organization, including on-premises data centers, cloud and network edge environments. Crucially, it also analyzes Layer 7 of the network: this is the layer and protocols used to deliver applications and are therefore the ones exploited by attackers.
2. It discovers assets to speed investigations, providing insight not just into IP addresses but also users, servers and organizations. These are the details which can rapidly accelerate incident respond and reduce cyber risk.
3. It rapidly detects suspicious behavior, as it is behaviour-based, which makes it much harder for even advanced attackers to hide. Network traffic analysis leverages the power of machine learning to build a baseline of normal activity so it can accurately flag events like unusual lateral movement inside the network to stop attacks in their tracks.
4. It reduces false positives, by correlating data across IP addresses, users and other elements to automatically produce an incident timeline.

Why Accedian?

Accedian's Skylight™ powered Security solution offers business decision makers next-gen IDS to tackle serious cyber-threats head-on via a highly cost-effective solution. There are five key elements:

Visibility and cost reduction: Lightweight Skylight sensors collect key data from 100% of transactions across the entire IT environment. By using intelligent "per-packet intel"™, or metadata, you can keep costs down as networks do not need to be rearchitected or enhanced to deploy the technology. Further costs are saved on CPU and disc space thanks to this lightweight data collection.

Advanced threat protection: Skylight uses analytics leveraging machine learning, statistical, and signature methods for anomalous behavior threat detection. Additionally, the data used is very rich, precise, complete, and unsampled, making analysis more robust and reliable than solutions which lack this fine-grained and complete data set. The bottom line is that security responders get rapid, high fidelity alerts to stop attacks in their tracks, minimizing the impact on reputation and the financial bottom line.

Timeline of connected events: Skylight not only alerts when there is a suspicious or malicious incident, but then correlates these incidents and artifacts over a timeline by asset, user, IP, etc. to reduce the risk of false positives that a security analyst must deal with.

Easy to deploy and manage: Skylight is built with an open architecture to integrate neatly into third-party threat intelligence feeds and security tools, to add further value. 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.

Not just a threat detection platform: Skylight not only alerts when threats are detected, but it offers investigative workflows, identifies and classifies asset classes, provides the experienced threat hunter with access to the raw data for deep inspection, and retains the data for long term forensics. This is invaluable if and when a breach occurs, to rapidly determine the extent of the breach.

With Accedian Skylight powered Security you can:

- Reduce cyber-risk for your business
- Minimize breach costs by detecting threats early on
- Preserve your corporate reputation with customers, partners and shareholders
- Reduce the TCO associated with legacy logging tools
- Support remote working and digital transformation at a time of business uncertainty

If you're interested in next-gen IDS, consider the following:

Six questions to ask IDS vendors

1. What's the TCO including cost of network, disc space, CPU, etc.?
2. Can you get visibility everywhere, including across all cloud infrastructure and the network edge?
3. Will machine learning detect lateral movement and suspicious behavior?
4. Can it provide context-rich insight including an incident timeline to minimize false positives?
5. How quickly can it detect and notify of suspicious behavior?
6. Does your solution provide long-term forensic data and investigative and hunting workflows?

About Accedian

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

Learn more at accedian.com

ACCEDIAN

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