

Powering clients to a future shaped by growth

A Frost & Sullivan White Paper

A Modern Solution for Modern Problems: How XDR Solves Tomorrow's Biggest Security Challenges

Hamstrung security teams stand to benefit from a solution designed from scratch to address the most pressing post-digital transformation pain points

Commissioned by Hillstone Networks



Contents

- 3** State of Today's Contemporary Threat Landscape
- 6** Evolved Enterprise Environment
- 9** More Data, More Problems
- 11** Asset or Liability: Perception of Cybersecurity
- 14** XDR is a Modern Solution for the Modern and Evolving Enterprise
- 15** Appendix: Frost & Sullivan survey cited
- 16** About Hillstone iSource: AI-powered XDR Solution

State of Today's Contemporary Threat Landscape

In 2020 and 2021, news headlines of successful ransomware attempts, data breaches, and stolen credentials gripped the world. Name brands recognized by most, such as Twitter, Microsoft, and Marriott International, were the targets of such high-profile attacks. More worryingly for the security community, hackers attacked federally contracted SolarWinds, allowing state actors to reach dangerously deep into several US agencies' systems.¹

“In a recent Frost & Sullivan survey of security leaders from Australia, Singapore, and the United States, 86% of respondents said that they are modernizing their cybersecurity operations—and more than 20% of those surveyed will overhaul half or more of their security infrastructures.”

In response to this increased cyber-risk, enterprises are considering cybersecurity modernization programs. In a recent Frost & Sullivan survey of security leaders from Australia, Singapore, and the United States, 86% of respondents said that they are modernizing their cybersecurity operations—and more than 20% of those surveyed will overhaul half or more of their security infrastructures. Despite increasing awareness and intent to raise the degree of security, organizations face several implementation challenges, ranging from the obvious technological standpoint to the lesser-seen cultural and managerial aspects.

REASONS FOR MODERNIZATION

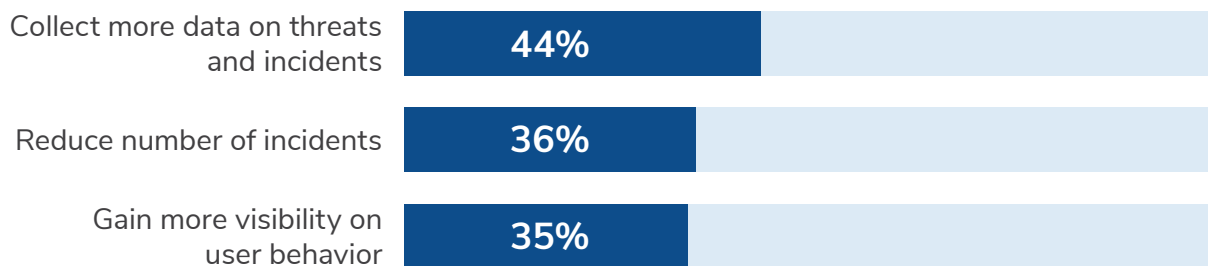


Figure 1: In a recent survey of cybersecurity decision makers, the primary reason for modernization is to improve data collection relating to threats and incidents.

Source: Frost & Sullivan

1 [A “Worst Nightmare” Cyberattack: The Untold Story of the SolarWinds Hack, NPR, 2021.](#)

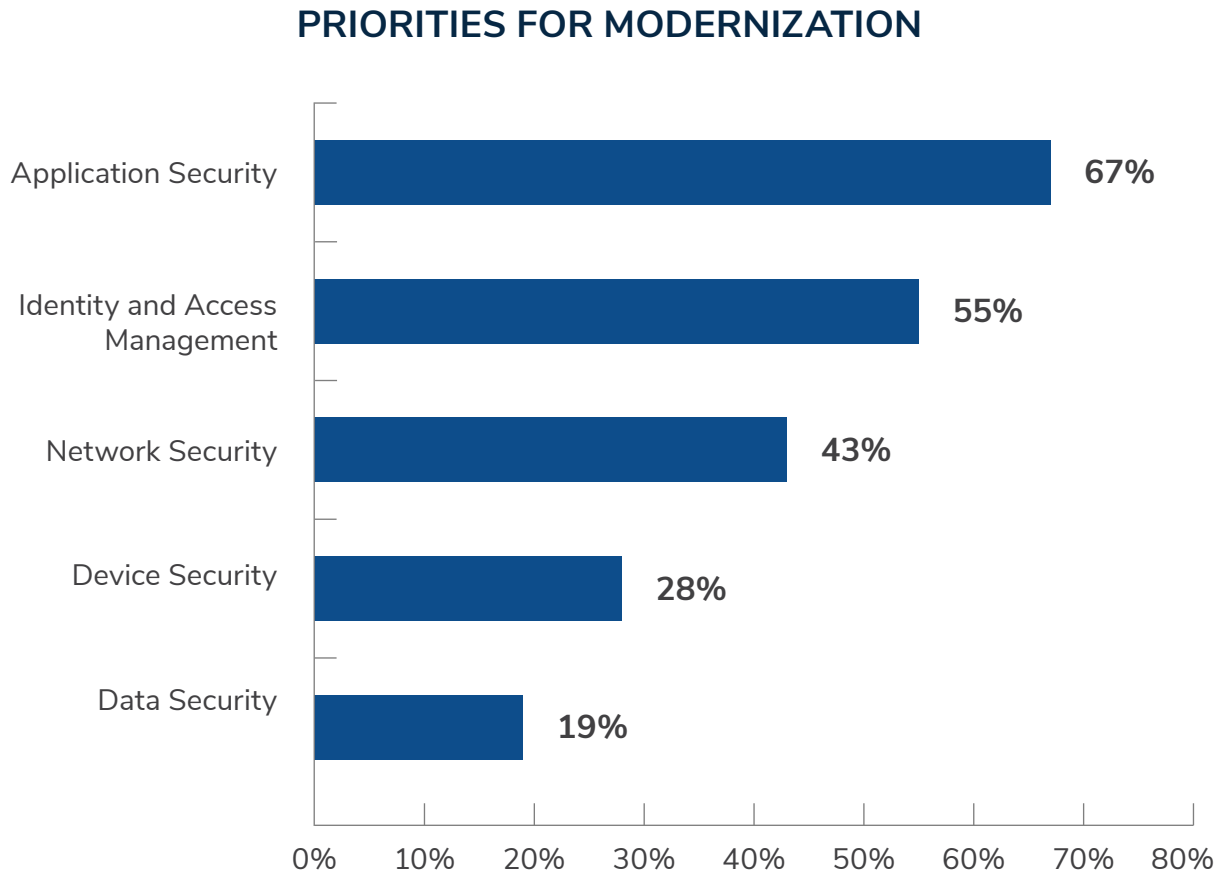


Figure 2: Of the Singaporean respondents, 100% indicated that network security is a priority for modernization. On average, application security is the primary focus across all countries surveyed. Third-party application use has grown quickly as enterprise complexity has deepened. The availability of software-as-a-service-deployed applications has also aided in reducing the cost and management needs of these programs.

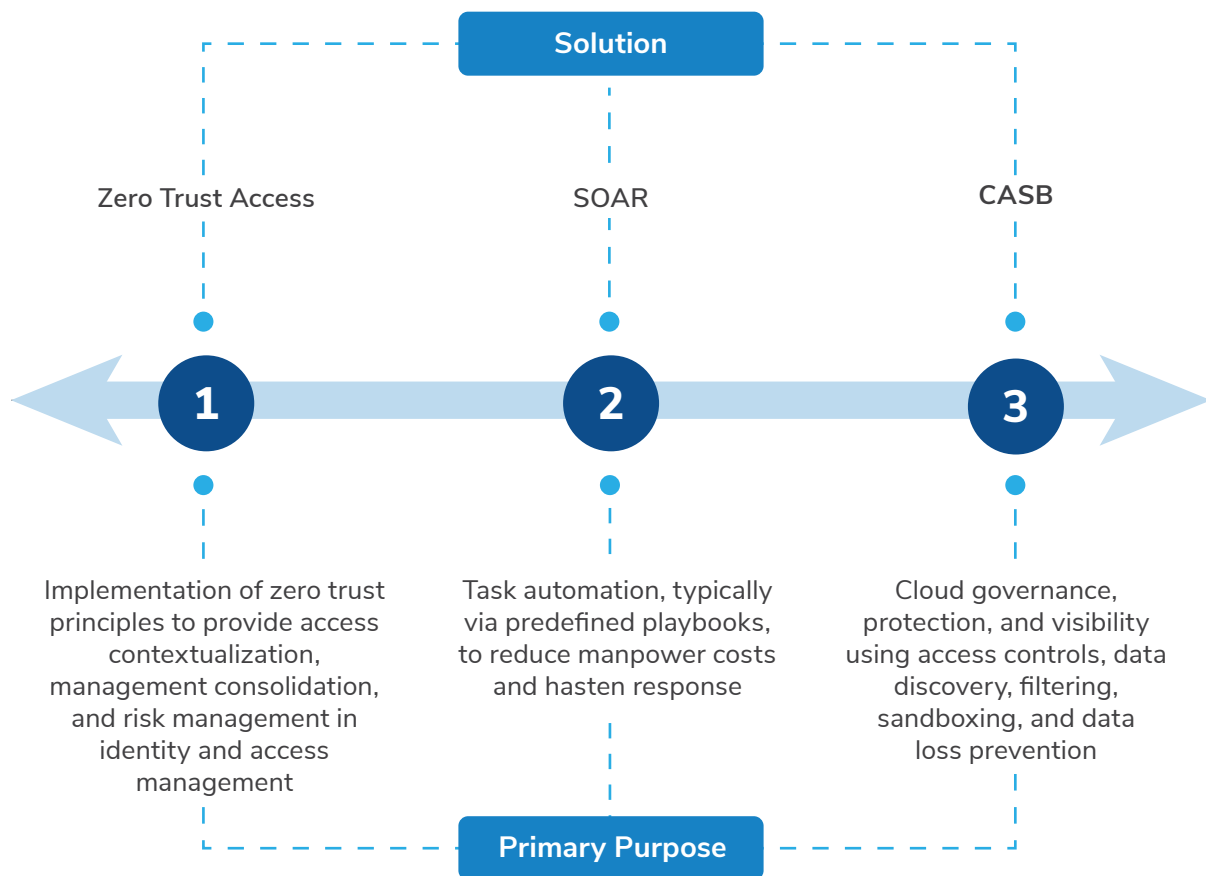
Source: Frost & Sullivan

Larger, more sophisticated organizations' planned security purchases are for securing users and the cloud, enhancing detection and response (D&R), and implementing zero trust, in contrast to the prevention-oriented approaches of the past. The threat landscape is evolving quickly and is too diverse to viably employ best-of-breed prevention across the board. Security leaders have developed emerging security solutions, such as zero trust access; security orchestration, automation, and response (SOAR); and cloud access security brokers (CASBs) to solve the novel issues that organizations face in the modern threat environment.

Another solution has garnered the attention of security leaders in recent years. Extended detection and response (XDR) is a budding security solution that addresses most, if not all, of these use cases.

Briefly, XDR combines the capabilities of security information and event management (SIEM), endpoint DR (EDR), network DR, and threat analytics while supplementing these with automation, user behavior analysis, cloud nativity, and widespread integration to provide greater visibility, quicker responses, and superior threat detection. The next chapters explore XDR's value in the context of today's organizational needs.

SOLUTIONS PRIORITIZED IN MODERNIZATION PLANS






Evolved Enterprise Environment

The modern enterprise environment bears little resemblance to the past environment. An organization's entire information technology (IT) stack no longer consists entirely of owned on-premises solutions. The ongoing move to the cloud has allowed businesses more flexibility, affordability, and scalability.

“According to a Frost & Sullivan survey of security decision makers, 43% of respondents across the United States, Australia, and Singapore indicated their organizations were cloud first, with most workloads in the cloud.”

According to a Frost & Sullivan survey of security decision makers, 43% of respondents across the United States, Australia, and Singapore indicated their organizations were cloud first, with most workloads in the cloud. Despite the positive uptake, only a third of respondents had secured their cloud workloads across all environments. Unsurprisingly, monitoring cloud environments is the second-largest operational challenge that security teams face—exceeded only by the cost of operating monitoring solutions in the first place.

WHAT DOES THE CLOUD OFFER ORGANIZATIONS?

Flexibility	Affordability	Scalability
 <p>Unlike on-premises deployment, the cloud does not require organizations to commit to lengthy licensing arrangements or vendor lock-ins.</p>	 <p>Barriers to entry for cloud-deployed solutions are almost always lower than their on-premises counterparts. Organizations do not have to grapple with installation and recurring hardware maintenance costs, but instead pay a prorated sum depending on the vendor's fee structure.</p>	 <p>Because cloud providers manage the infrastructure for cloud deployment, organizations can add capacity as needed simply by making a call.</p>

The move to the cloud is closely related to the increasingly wide distribution of the workforce. Spurred by perpetual COVID-19 concerns, most organizations have acknowledged that they will have at least some degree of remote working in their future work plans, and organizations that previously relied on foot traffic have accepted that most of their sales touchpoints will now be online. To illustrate, the eCommerce share of global retail sales grew from 16% to 19% in 2020,² totaling \$26.7 trillion in revenue.

These changes mean that organizations are now even more dependent on maintaining their online websites and services' uptime, underlining the necessity to keep them secure.

ORGANIZATION FUTURE WORK PLANS

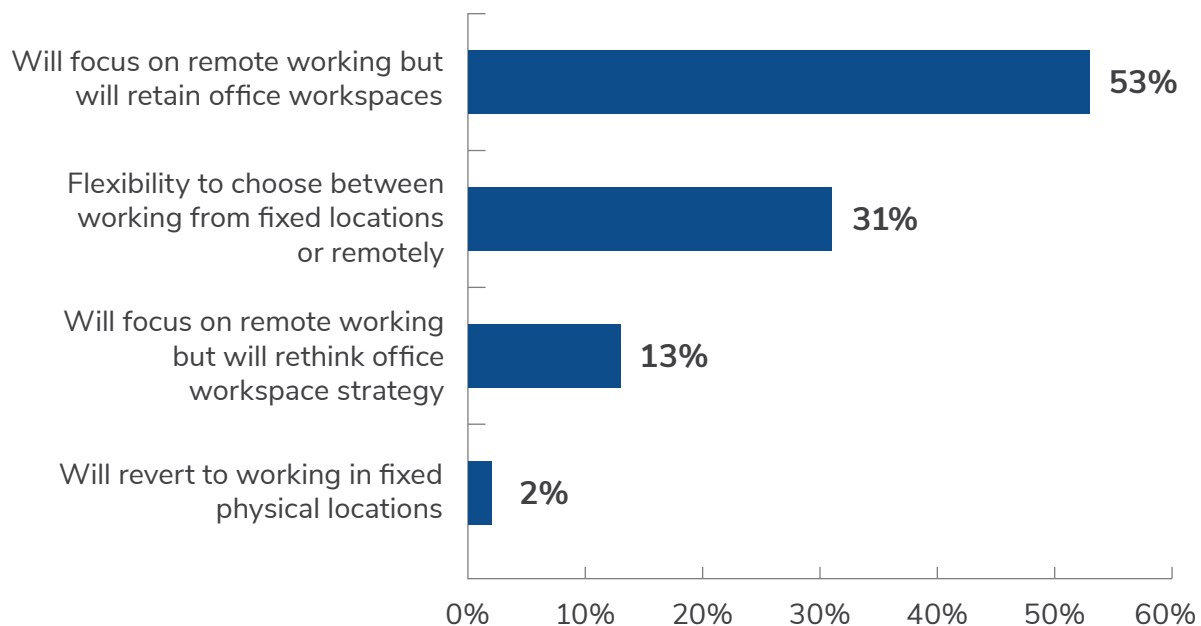


Figure 3: The overwhelming consensus among respondents is that remote working will be a significant part of how employees work in the foreseeable future.

Source: Frost & Sullivan

The Internet of Things (IoT) and operational technology (OT) are also undisputed points of significance in the evolution of the enterprise environment. The lines between traditionally separated IT and OT are blurring as industrial enterprises seek to drive efficiency in their production processes.

In a survey conducted by Frost & Sullivan, 45% of respondents deem robotics the most important emerging technology for digital transformation (DX), while 32% of respondents consider the IoT the most important. Despite their benefits to organizations, the IoT and OT expand the threat surface as adopters introduce additional avenues of attack not typically covered by IT-oriented security solutions.

² [Global eCommerce jumps to \\$26.7 trillion, fueled by COVID-19, United Nations, 2021.](#)

In the IT space, organizations do not optimize legacy security solutions for the fast-changing enterprise environment and are thus left dangerously vulnerable to new threat vectors. These changes have also made it exceedingly difficult for organizations to keep track of their distributed and varied assets, as little uniformity exists between deployments, application types, device types, and user locations.

XDR integration can better protect and respond to threats in the evolving enterprise

By design, XDR is a flexible, easy-to-integrate, comprehensive, and comprehensible security solution for organizations dealing with extensive technology sprawl. For one, XDR integrates with as many data sources as possible and collects more contextual metadata—giving security teams the ability to generate insights from across the IT/OT environment. Moreover, D&R becomes cross-layered across these data points, mitigating the tunnel vision that sometimes comes from traditional methods such as EDR.



More Data, More Problems

Data, the lifeblood of the network and, by extension, cybersecurity, feeds into the various security solutions, threat intelligence, and SIEMs that ultimately generate the reports and recommendations on which analysts depend. Security teams have a bigger problem dealing with too much data than too little for several reasons:

- Too many false positives
- Analysis paralysis
- Lack of skilled cybersecurity professionals

Too many false positives

The false positives of traditional D&R solutions overwhelm security teams. These traditional methods do not separate the noise from the useful data and do not discern between priority alerts and alerts that are incidental, due in large part to the low fidelity of the data gathered by SIEM and centralized log management (CLM). The situation has kept security teams on the back foot, reactively responding to threats rather than proactively preventing them. Ideally, security alerts should efficiently point security teams toward preventive or remedial actions.

Analysis paralysis

Security teams are stuck analyzing benign and nonconsequential alerts, impeding their ability to act on alerts that pose actual threats. In a survey conducted by Frost & Sullivan in June 2021, 70% of surveyed organizations with more than 500 employees in the United States and Singapore had mean times to detect of more than a week. In the same survey, 90% of respondents had mean times to respond of more than a day.

Considering how some of the most damaging attacks that target organizations, such as privilege misuse and system intrusion, take the longest time to find,³ damage can accumulate quickly.

³ 2021 Data Breach Investigation Report, Verizon, 2021.

In a survey conducted by Frost & Sullivan in June 2021, 70% of surveyed organizations with more than 500 employees in the United States and Singapore had mean times to detect of more than a week.



Lack of cybersecurity professionals

The severe lack of available cybersecurity is the most glaring problem that every organization faces today, and it is a longstanding problem⁴ that has significantly affected the cybermaturity of organizations as a whole.

Even with the best data available, organizations will struggle to stay ahead of threats without enough people to perform the tasks needed to run an effective security operations center. Consequently, analysts wear many hats and can become overwhelmed and ineffective. Security leaders have been finding ways to solve the data problem. In fact, according to Frost & Sullivan's survey, 43% of respondents said that the primary purpose of their plans to deploy XDR is to better deal with increasing volumes of data.

XDR can address data paralysis

The pillars of XDR are cross-layered D&R, AI-enabled analytics, and automation. Gathering data from across the IT and OT environments, normalizing it, and then performing correlation fulfills these functions. The security posture and threat environment are then combined. The quality of the derived insights is enhanced by the application of analytics. Overall noise is reduced, and insights are immediately actionable. Human input on repetitive tasks is then eliminated by leveraging automation, giving security teams the bandwidth to work on higher-order tasks and mitigate one of the most serious security liabilities.



⁴ [Cybersecurity Skills Crisis Continues for Fifth Year, Perpetuated by Lack of Business Investment, ISSA, 2021.](#)

Asset or Liability: Perception of Cybersecurity

Management teams have recently thrust cybersecurity into the spotlight, but for years they viewed it mostly as a cost of doing business and a component to meet regulatory compliance.

In Frost & Sullivan's survey, 40% of respondents indicated that one of the main setbacks to improving their organization's security posture was the lack of awareness of data breach implications and costs, while 36% said they had difficulties communicating the importance of cybersecurity to the board. In parallel, almost a quarter of respondents have experienced reduced security budgets in the past year.



Figure 4: The most common inclusion in security roadmaps is the restructuring of management's security perception. Management's disregard for security is one of the biggest hurdles that security teams face in bolstering their defenses and capabilities.

Source: Frost & Sullivan.

Essentially, organizations—particularly businesses—have been hesitant to invest heavily in cybersecurity because they see it as an expense rather than an element of risk management. This perception is greater in small organizations as they dedicate larger proportions of cash flow to running more essential systems. The constant changes to the business environment, such as the COVID-19 pandemic that is forcing widespread remote working, also contribute to the reluctance in committing heavily to capital-intensive investments.

Nevertheless, the rise in cybercrime and increasing pressure from regulatory bodies have spurred organizations to rethink cybersecurity. Cybersecurity Ventures estimates that global cybersecurity spending will increase from \$262.4 billion in 2021 to \$458.9 billion in 2025, at a compound annual growth rate of 15%.

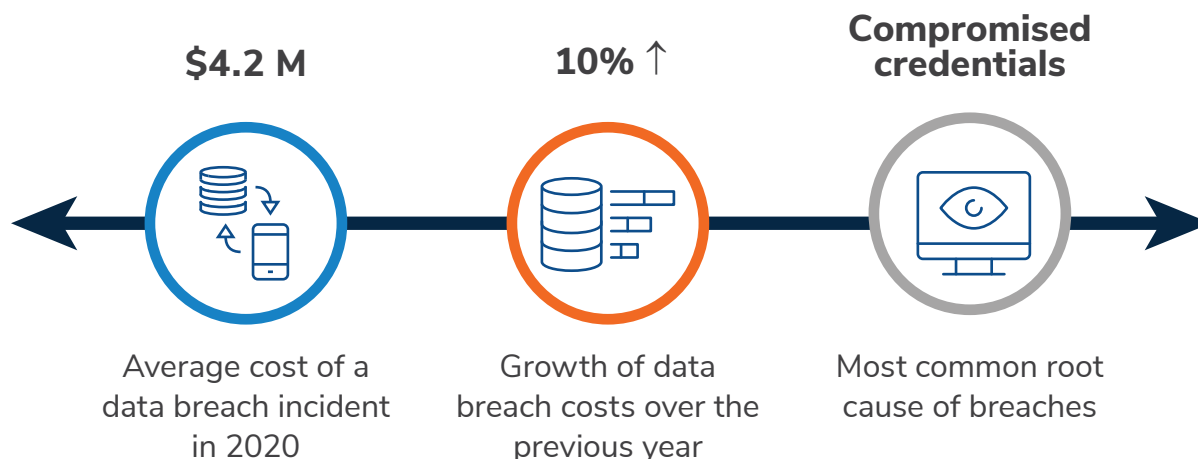


Figure 5: The risk of data breaches has increased significantly over the past year. Remote working incurs an average cost of more than \$1 million compared to traditional work environments.

Source: [IBM](#).

A joint report from IBM showed that organizations that have undergone DX during the COVID-19 pandemic have seen an average \$750,000 reduction in data breach costs.⁵ Organizations with mature zero trust strategies have seen average reductions of \$1.8 million compared to those without, indicating that the cost of breaches correlates with organizations' digital maturity and cybermaturity.

XDR can flexibly support enterprise cybersecurity

Cybermaturity and investments are directly tied to business outcomes, and XDR is one way in which businesses can enable flexibility, drive down data breach costs, and contextualize cybersecurity's value.

With its subscription-based approach and minimal hardware requirements, XDR's initial investment demand is much lower than traditional on-premises point solutions. This solution could be viable for the often-overlooked medium to small segments, with the cost spread over time rather than front-loaded. XDR's ability to derive insights from across the threat environment also allows it to provide business context to cybersecurity.

For example, management teams can compare the most targeted areas of their businesses with the relative investments in these areas to create a priority list of future cybersecurity expenditures. This information is also useful for assessing the direct cybersecurity risk to a company's bottom line.

⁵ [IBM Report: Cost of a Data Breach Hits Record High During Pandemic, IBM, 2021.](#)

XDR can maximize existing cybersecurity investment

XDR helps protect existing security investments in 2 ways:

- Mitigating the costs of siloed, disparate security solutions
- Extending the value of security solutions at risk of obsolescence

The multivendor environment that organizations find themselves in often incurs both obvious and hidden costs. For example, the silos created from deploying solutions that do not speak to each other by default cost organizations time and money in manual integration, causing burnout in employees burdened with menial and ungainful tasks. Organizations are thus compelled to audit the costs of maintaining a current solution—even if it works well with their needs—against the cost of operating it. XDR breaks down these silos, serving as the central hub connecting all deployed solutions. Organizations can normalize their data and mitigate their current integration costs and future upgrades and additions.

With the arrival of new security products every year, the phasing out of older models or iterations that serve the same purpose is a risk. Reasons for this include an inability to integrate with the overall security environment, reduced effectiveness in combating modern threats, and insufficient or unactionable data. XDR helps reinvigorate the utility of older solutions because of its ability to tap into deeper metadata and perform cross-layered D&R. As such, each deployed security solution at least plays the role of feeding contextual information into XDR—raising overall security readiness. At best, XDR could open new use cases, even for older solutions.

XDR is a Modern Solution for the Modern and Evolving Enterprise

The modern enterprise requires modern solutions to keep it safe and cognizant of the adversaries that are a threat. To determine which set of solutions fit best with the organization, management teams should ask themselves the following:

- How effective are the organization's current D&R capabilities?
- How well do the organization's current security solutions work with each other?
- How much time does the organization's security team spend on repetitive, low-value tasks?
- How much visibility does the organization have of its network, users, workloads, and devices?
- How effective at leveraging threat intelligence is the organization?

Answering these questions can give organizations a better idea of the viability of XDR in context. Through its integration, automation, and native D&R capabilities, XDR enables organizations to improve their cybersecurity effectiveness from a cost and efficacy standpoint by:

- Combining visibility to consolidate intelligence
- Supporting overloaded IT teams
- Accelerating D&R

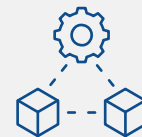
KEY VALUES FOR CYBERSECURITY EFFECTIVENESS



Combining visibility
to consolidate
intelligence



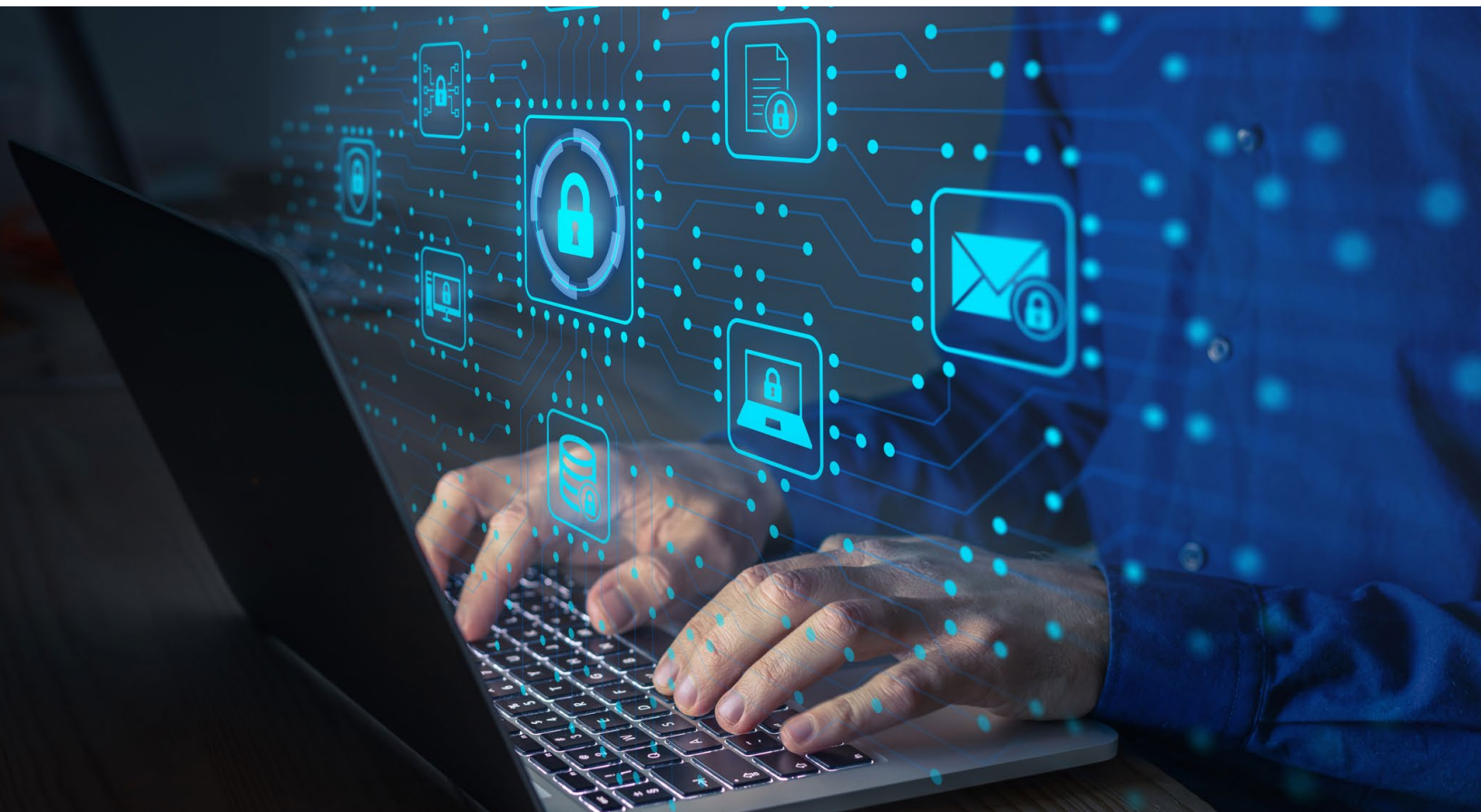
Supporting overloaded
IT teams



Accelerating D&R

Appendix: Frost & Sullivan survey cited

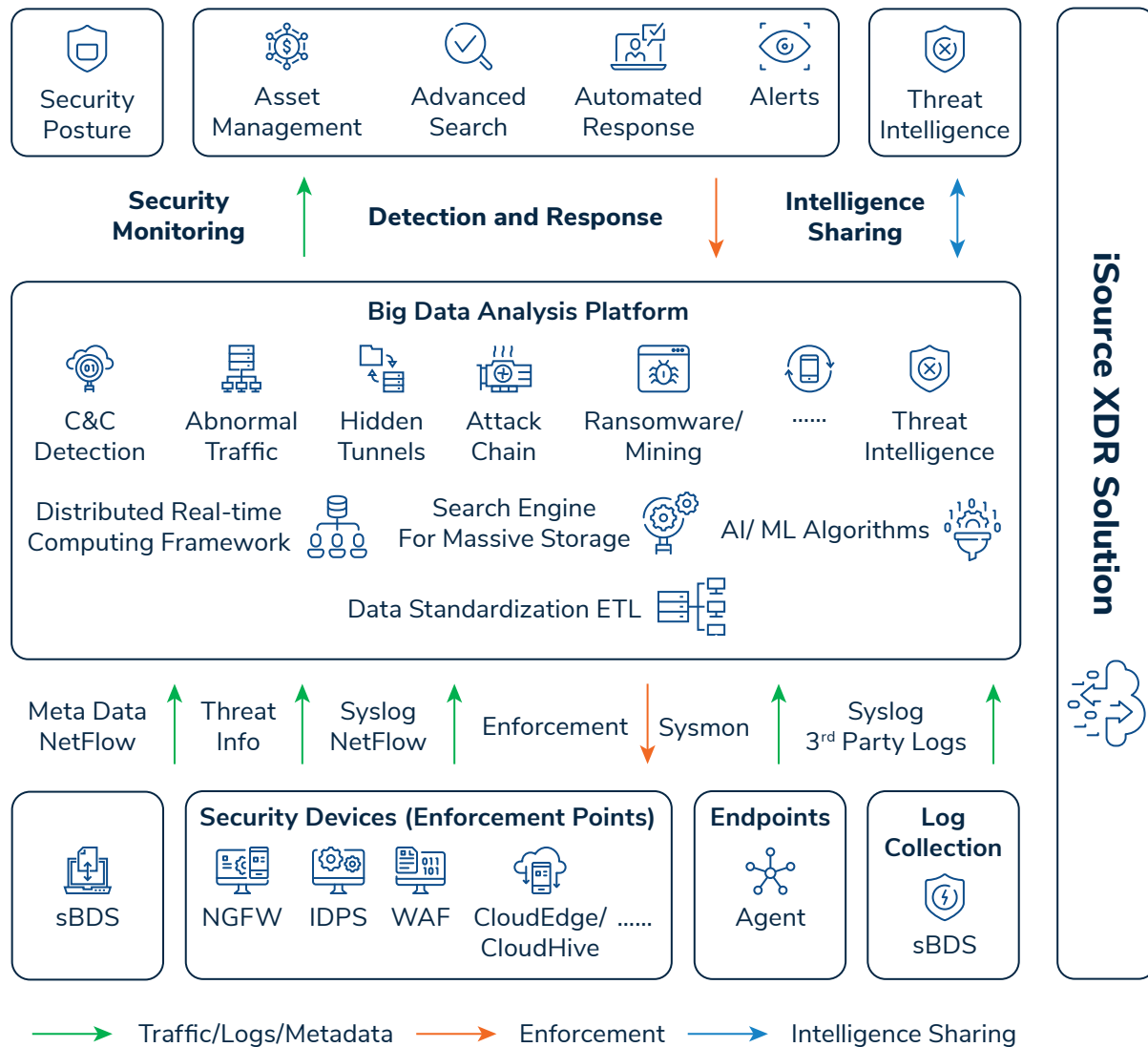
Frost & Sullivan C-level Survey on Cybersecurity Posture, Cyberthreats, and State of the Enterprise	
Sample size	150 respondents
Countries	Singapore (50) United States (50) Australia (50)
Role	CEO, CFO, COO (35%) CISO, CSO, CIO (65%)
Industries	BFSI, IT & Technology, Telecommunications
Employee size	>500 employees
Survey date	September 2021



About Hillstone iSource: AI-powered XDR Solution

Hillstone iSource is a data-driven, AI-powered XDR platform that integrates massive security data, correlates and investigates incidents, identifies potential threats, and automatically orchestrates security to respond cohesively across multiple security products and platforms. iSource brings a radical new approach to cybersecurity with unrivaled security operation efficiency.

HILLSTONE iSOURCE XDR SOLUTION ARCHITECTURE



The iSource XDR solution exemplifies Hillstone's embodiment of "see understand act." iSource embodies "see" through its ability to integrate native and third-party data from various point products scattered across a security infrastructure. It embodies "understand" through its ability to run siloed, fractured, low-confidence data through a centralized correlation analysis engine to create an affiliated, united, high-confidence report. Finally, iSource embodies "act" through its simplified remediation process, shared via customized playbooks or default templates.

Hillstone Networks' proven Infrastructure Protection Solutions provide enterprises and service providers with the visibility and intelligence to comprehensively see, thoroughly understand, and rapidly act against multilayer and multistage cyberthreats. Favorably rated by leading analysts and trusted by more than 20,000 global companies, Hillstone protects all organizations from the edge to the cloud, and from the user to the application with a lower total cost of ownership. With a reputation for "security that works," Hillstone's holistic product suite includes next-generation firewalls, extended detection and response solutions, software-defined wide-area networks, cloud security, and application security. Hillstone's cutting-edge solutions leverage AI/machine learning and integrate seamlessly into security operations frameworks, providing assurance to chief information security officers that their enterprises are well protected. To learn more, visit www.hillstonenet.com.



FROST  SULLIVAN

Growth is a journey. We are your guide.

For over six decades, Frost & Sullivan has provided actionable insights to corporations, governments and investors, resulting in a stream of innovative growth opportunities that allow them to maximize their economic potential, navigate emerging Mega Trends and shape a future based on sustainable growth.

Contact us: [Start the discussion](#)

The contents of these pages are copyright ©2022 Frost & Sullivan.