



# A MODERN APPROACH TO CYBERSECURITY

## Cybersecurity is becoming a hot topic for organizations that are quickly adopting modern technologies and moving into the digital space

Organizations operating in the growing digital environment are facing increasing complexities in managing technology-savvy employees, customers, and regulators while defending their technology platforms and data against cybercriminals.

Accelerating requirements and available capabilities imposes an unprecedented burden on organizations in terms of adapting to rapidly changing digital conditions. This is not about a single, revolutionary technology, but a convergence of humanity's entire conduct of activity with a significant digital dependency, in such a short period of time relative to the previous century.

From a security perspective, each new service that society moves into the digital space creates more risk for organizations to manage. Cybersecurity professionals and programs are scrambling to keep up as businesses employ improving technology to accelerate their growth. Compounding this challenge are the realities around recruiting from a talent pool where supply is lower than the demand and ongoing efforts needed to retain existing talent. This dose of reality makes it difficult for organizations to keep pace and maintain a strong security posture.

The good news is that the technology that is enabling digital acceleration (e.g., cloud) for businesses is now on the verge of enabling security in an equally impactful way. This paper explores the areas where smart cybersecurity is being employed, and how it is enabling organizations to secure their business like never before.



## THE BURDENS WE SHARE

There are several reasons why security teams and organizations struggle to optimize their security posture. Below are several of the challenges all organizations face in the current environment:

**Overly-Complex Solutions** – Many solutions can be overly complex to operate in an optimized and meaningful way. Not being able to properly configure and operate a solution often leads to organizations turning to expensive vendor professional services or adding gap-filling technologies, which can lead to technology sprawl and increased costs.



**Technology Sprawl** – Adding technologies to fill visibility gaps need to be carefully considered. Will the organization be able to acquire the people and skills necessary to operate the solution, and does the solution create other issues as a result? Are costs being considered when looking to layer on a new solution?



**Increasing Costs** – As technology redundancy and overlap grow in an organization so do the associated costs to manage them. Attempts to rationalize technologies and remove duplication become difficult as other business demands take priority. The cycle continues, which then drives inefficiencies we cannot afford and can create blind spots in your security program.



**Skill Acquisition** – Acquiring skilled cybersecurity professionals is a challenge in terms of attracting, equipping, and sustaining strong talent across a variety of technologies. Many factors are driving the security resource shortage including a lack of trained professionals, surging demand, a lack of historical business investment, staff burnout due to understaffing, increasing volume and sophistication of threats, and new challenges presented by more automation and remote work.



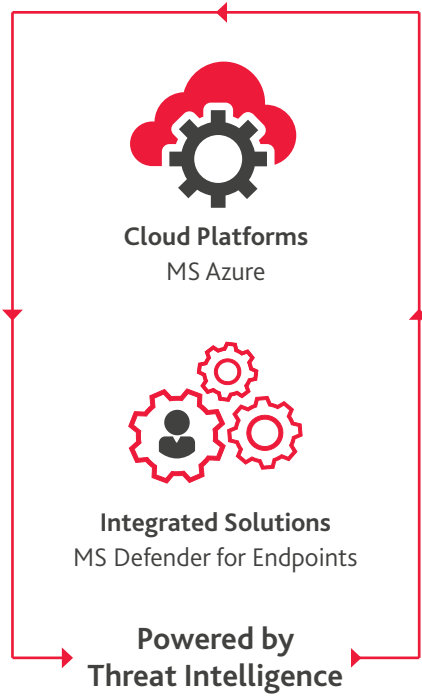
**Alert Fatigue** – Security teams spend too much time chasing alerts resulting in dead-ends. This is often a result of sensors not being configured properly or alerting thresholds set too wide. Chasing low priority, non-correlated, alerts distracts and beleaguers teams increasing the risk of breach and staff turnover.



The burdens described above are widely shared and experienced in the field of cybersecurity. Organizations are quickly realizing that no one vendor or solution corners the market in terms of eliminating all risk. However, with a risk-based approach to security programming one can gain a significant security advantage by employing strong technologies (e.g., Microsoft Security Solutions), strong processes (e.g., incident management), and strong talent (e.g., qualified on the tools).

## WHAT CAN ORGANIZATIONS DO?

Modern cloud platforms, AI, and intelligence-enabled solutions are helping organizations gain confidence and further reduce risk by embracing the ease and reach of security in the contemporary IT environment. This convergence is enabling unprecedented levels of cybersecurity capabilities. This paper goes on to outline how emerging technologies are changing the paradigm and how smart processes can alleviate burdens without high cost and complexities.



## EMERGING CAPABILITIES CAN HELP

**Cloud Platforms** – Selection of a best-in-class cloud platform, such as Microsoft Azure, is a cornerstone for enabling a contemporary, feasible and functional cloud security program. The primacy of the cloud platform in your security operations cannot be underscored enough. These service providers afford their customers state-of-the-art security frameworks and methods by prioritizing platform detection capabilities over third-party vendors; not to mention the budget to deliver complete solutions. It is a hard case to make that other solution providers could know more about Microsoft Azure than Microsoft. Third-party solutions have a place, but the core platform capabilities are essential and are being delivered through mature, security-first, service providers.



**Integrated Solutions** – Identifying the need to move away from signature-based detection and towards behavior-based detection to deliver a deeper level of visibility, solution providers have been integrating their capabilities to make them smarter and more reliable, leading to better outcomes. Endpoint Detection & Response (EDR) is an example of an integrated technology where correlation and detection of suspicious activity occur away from a central Security Information and Event Management (SIEM) solution. By focusing on endpoint behaviors, vs signatures and infusing it with threat intelligence quality and confidence of alerts go up.



**Threat Intelligence** – The proper use of threat intelligence helps organizations prioritize their security investments as it provides insights into the most likely and most dangerous threats facing an organization. This awareness and prioritization help drive what cyber investments and initiatives should be focused on to help increase security posture, accelerate remediation, and informs us of attacks that may have gone by undetected.





## A PRACTICAL APPROACH TO REDUCE BURDEN

We often find organizations take a short-term tactical approach when delivering security capabilities. This is typically driven based on reactions to breaches, audits, vendor, or professional services advice, etc. There is a significant risk to this approach in terms of overall effectiveness, cost, staffing, and can lead to a decrease in security posture.

BDO proposes the following approach to enabling an organization's security posture.

**Enable Investigations** – The first step is to address if you have the access and reach to effectively investigate and act on any security issue brought to your attention. BDO prepares your environment in this regard to help ensure that the information required to track threats is available, accessible, and timely.



**Prioritize Integrated Alerts** – The highest fidelity, most integrated technology sets are prioritized to help provide maximum visibility across the widest possible aperture. We prioritize integrated technologies such as cloud platforms, EDR, and solutions that incorporate threat intelligence filtering.



**Enhance Operational Processes** – In order to help ensure quality, sustainability and good organizational outcomes, one of the critical areas is the requirement for internal process. With high-quality alerts available, the organization needs to be able to act. For example, without a documented and understood security incident response process, organizations may find themselves taking longer to contain and recover.




**Enhanced Use Cases** – Once the fundamentals are firmly in place, BDO expands the security aperture to add additional surveillance layers such as applications, business logic, or insider threat. We deploy custom use cases to illuminate threats across all of your attack surfaces, which can maximize the organization's visibility into security events.



**Sustainment** – BDO continuously assesses the market along with its tech stack to help provide maximum effectiveness, efficiency, and value for our clients. Sustainment is a core aspect of maintaining a valid security posture, and right-sized skilling, and tooling. Defense in depth is critical to the success of any security program, so knowing when to re-configure vs. replace a technology based on the market and your specific position is critical.





Drastic improvement is within reach and starting to happen. Smarter technologies are completely upending the industry's approach to security. Modern security programs are changing faster than ever and the use of contemporary technologies alongside a smart approach and experienced advisors such as BDO are helping to increase the pace of change and improvement, for those who are embracing it.

## CONTACTS

### **ROCCO GALLETTO**

Partner, National Cyber Security Leader  
BDO Lixar  
416-729-2609 / [rgalletto@bdo.ca](mailto:rgalletto@bdo.ca)

### **ROB PHILPOTTS**

Director, Cyber Threat Management  
BDO Lixar  
437-237-3502 / [rphilpotts@bdo.ca](mailto:rphilpotts@bdo.ca)

### **BRAD ELLISON**

Managing Director, Managed Services Group  
630-286-8196 / [bellison@bdo.com](mailto:bellison@bdo.com)

### **STEVE COMBS**

Director, Infrastructure Solutions Group  
713-576-3417 / [scombs@bdo.com](mailto:scombs@bdo.com)



#### About BDO Lixar

BDO Lixar is the technology advisory arm of BDO Canada. We are an end-to-end technology solution provider, helping businesses accelerate and grow.

Our teams have been accelerating our clients' innovation journeys through Data & AI, Cybersecurity, Digital strategies, Modern Workplace solutions and Application Development, underpinned by the BDO Lixar Cloud Adoption Framework. From finding cost-savings, efficiencies, and insights, to predicting future outcomes, we're dedicated to helping our clients not only navigate the disruptive technology landscape, but also stay competitive and successful. We have proven expertise in a wide breadth of industries and deliver innovative, stable, and extensible solutions that tackle the toughest problems and capture growth opportunities.