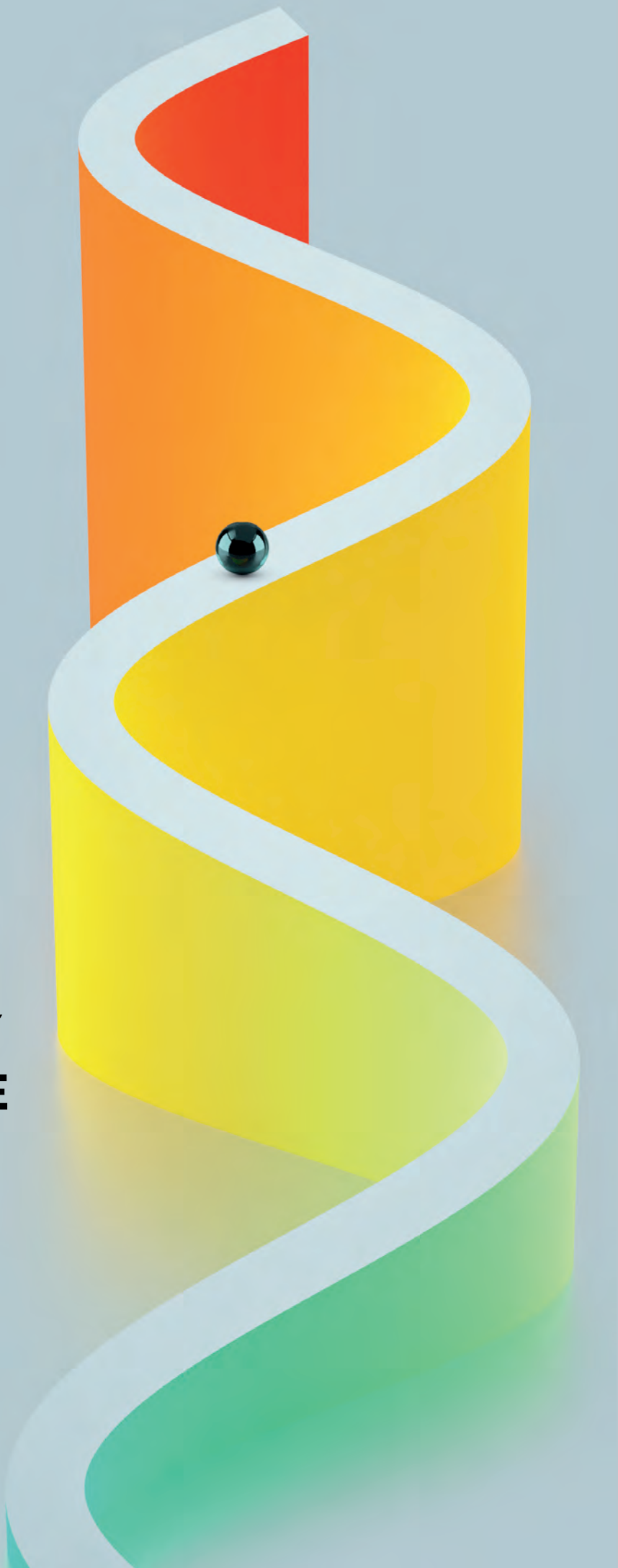
CyberProof™

PROVIDING A CYBER SECURITY SERVICES FRAME WORK

HOW CYBERPROOF HELPS SOLVE YOUR ORGANIZATION'S CYBER SECURITY NEEDS



EVALUATING RISK - INCREASING CYBER RESILIENCE

CyberProof is a security services company that aims to manage cyber risk for organizations by providing pioneering, next-generation services and technologies. These adapt to the evolving threat landscape, with cost effective prevention, detection, and accelerated response and recovery.

Let's look at how CyberProof's platform approaches cyber security by clarifying risk and investment thereby meeting the challenges of providing organizations with a stronger cyber resilience in an increasingly complex threat environment.

STUCK BETWEEN THREAT LANDSCAPE AND SECURITY PERFORMANCE ISSUES

Organizations trying to improve their cyber security profile face multiple external threats and challenges. At the same time, they handle a range of significant internal security performance issues.

Key Takeaways

Organizations put most of their security spend on prevention. Since nobody is ever 100% protected, it's essential to reassess risk and investment, and shift the focus from prevention towards detection and response.

Organizations trying to improve their cyber resilience face a number of external threats, and they handle with a range of internal security performance issues. Meeting these challenges involves leveraging new technologies that helps you to identify breaches faster and adopt more streamlined response processes.

Effective cyber defense requires a holistic approach including: contextualized threat intelligence, pervasive, continuous threat assessment, data-driven decision-making; and agile processes that rely on automation & orchestration.

Breach and Attack Simulation (BAS) tools are needed to test resilience by simulating real world attackers.

Security Operations Analytics and Reporting (SOAR) is needed to streamline security operations by leveraging external and internal intelligence.

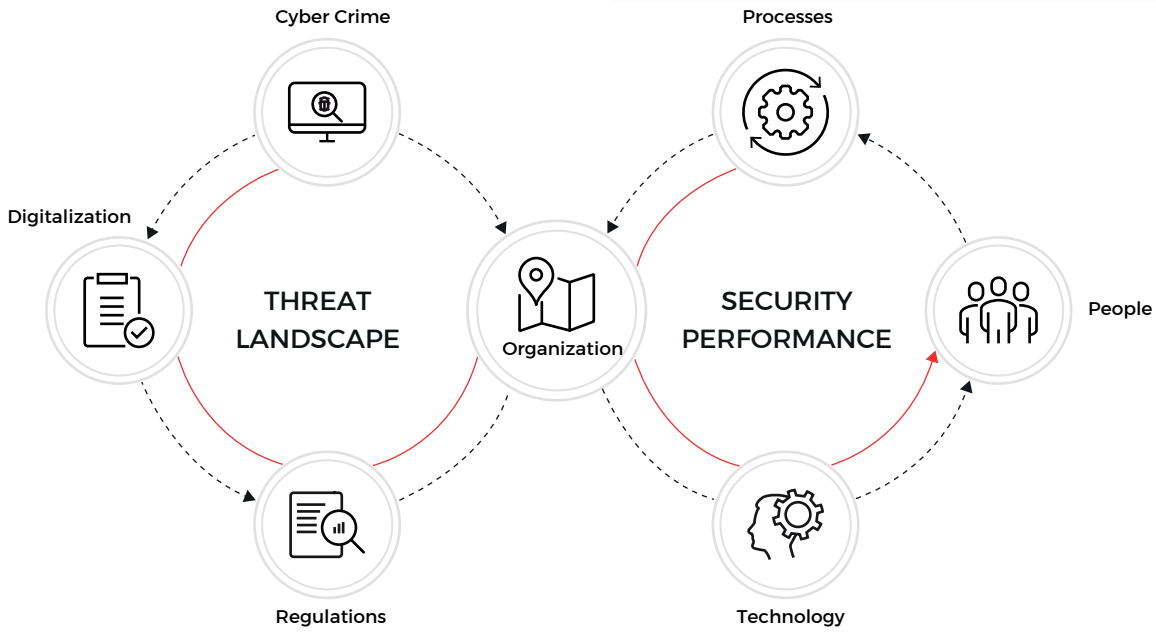


Figure 1: Challenges to cyber security

Some of the significant external threats and challenges faced by today's organizations include:

Cyber crime – The number of cyber attacks continues to increase, partly due to the growing profitability of cyber crimes. According to ISACA's State of Cybersecurity 2018 research, 50 percentage of security leaders surveyed mentioned that they experienced an increase in attack volumes as compared to last year. Since the attacks are increasingly sophisticated and difficult to identify and because they occur fastly, they are likely to cause more extensive damage, which makes the matter worse.

Digitization – Digitization is no longer a luxury; it's a matter of business survival. Even well-known and well-established businesses are offering new services on top of their core businesses to remain relevant and support methodologies to better reflect how the real world is evolving.

Regulations – New data privacy rules impose stricter regulations on organizations hosting and processing personal data. "As pointed out by Gartner", the EU's General Data Protection Regulation (GDPR), which became enforceable in May 2018 – as well as other new cybersecurity laws, for example in China, California, and New York State require that authorities be notified promptly of data breaches or loss of personal data, and demand that organizations provide data breach response plans. But few organizations have measures in place to comply with these regulations, and the difficulties involved in meeting the requirements are many. For example, shadow data is a threat for many organizations and most apps do not provide sufficient security, compliance controls, and features to effectively protect enterprise data in the cloud.

INTERNAL CHALLENGES THAT IMPACT SECURITY PERFORMANCE

Beyond these external challenges, organizations are also handling certain internal challenges that directly impact security performance, including:

Processes – A Gartner report published in 2018 that points out that many organizations are implementing DevOps processes. In fact, most companies have replaced the question of "What is DevOps?" with "How do I implement securely and at scale?" But DevOps methodologies uncover new challenges. The fast pace of application releases strains the ability to maintain the robustness of application security. Bottom line: Those shorter deployment cycles and increased deployment frequency that are inherent to the DevOps approach require fast track, frictionless security processes.

People – There's a scarcity of talent globally, according to the (ISC)2 Cybersecurity Workforce Study (2018): The cybersecurity job gap grew to almost 3 million in 2018 from 1.8 million in 2017. The shortage hits hardest in the Asia/Pacific region but is also significant in North America, EMEA, and Latin America. That's why it's hard to keep the professionals you have on staff for long term, we're all competing for the best people. There's also burn out: alert fatigue, routine tasks, and a complex and ever-growing technological stack leading to stress and attrition. Finding new people is not just a matter of searching for a specific know-how on a resume. When it comes to security, having the right mentality is crucial. The work requires a different attitude than that of an IT professional or a developer. The person should be able to look at each situation from a hacker's perspective.

Technology – Once, everything was behind a firewall. But now the surface includes mobile, the Cloud, the Internet of Things – which makes the organization exponentially harder to protect. Challenges include an extended and diluted perimeter, shadow IT – and a myriad of security solutions, each of which operate independently.

In today's world, the constant pace of change is inherently challenging to business, making it hard to know how to plan for the future: Should we continue to conduct business as usual or attempt to move in the direction of current and developing trends? "According to this Wired", forward- looking companies are investing in digital transformation to adapt and outperform their peers.

NEW OPPORTUNITIES FOR IMPROVING SECURITY

To maintain a healthy security stance in this increasingly complex environment, it's essential to figure out how to leverage these new realities and find ways to turn the fast developing technologies and shifting external dynamics to your advantage.

Here are some examples

- In the area of cyber crime, focus on the fast-morphing business context, attack surface, and emerging threats to increase the speed of remediation and minimize damage.
- Regarding digitization, adopt DevSecOps speed and performance that heip in finding ways to keep track of Infrastructure as code, rather than relying on physical hardware configuration or interactive configuration tools.
- While the new regulations create a range of difficulties, they also help to detect and respond faster in the cyber kill chain, thereby minimizing loss to the organization after an attack.
- Adopt new processes leveraging an Agile Security Integrated operating model i.e. use new services to drive agile and adaptive threat detection, vulnerability management, and incident handling.
- Keep your best people in the team for longest period by augmenting their teams. This lowers fatigue levels and reduce your organization's attrition rates.
- Leverage innovative technologies to identify breaches faster i.e. organizations are being driven towards Security Orchestration Automation and Response (SOAR) technologies by the increasingly hostile threat landscape, combined with a lack of people, expertise, and budget.
- Reassess your financial investment – by assessing your organization's potential loss exposure and adopting a business-oriented prioritization of your security spend on defense and response.

IMPROVING PREVENTION WHILE UPSHIFTING DETECTION & RESPONSE

Most organizations invest 80 percentage of their security spend on prevention and invest very little in detection & response. Even then, bad guys manage to break through anyway.

The logical conclusion is to shift the investment focus from prevention towards detection & response.

This requires adopting a differential approach based on orchestration and automation, and using breach and attack simulation technologies that enables you to improve detection and response, without hurting existing prevention capabilities. Upshifting detection & response requires implementation of a new approach to organizational security, which can be summarized in five steps:

1. **Identify** – Appropriate external threat intelligence is necessary in risk management efforts to understand in-depth the complete business context, the actual attack surface, and new or lately emerging threats.

2. **Protect** – Unmanaged devices and services, application bugs, and misconfigurations are some of the issues that force organizations to invest so much in establishing effective prevention. Ensure that before investing on new, advanced security tools, it's worth reassessing whether more can be done with your existing, possibly underutilized security solutions.

3. **Investment Balancing** – Complete prevention is impossible, and to minimize damage, prevention efforts must be accompanied by agile and effective detection & response.

4. **Detect** - Globally reported data breaches due to simple yet rapid attacks. This is clear sign that as prevention seems to be failing, we should prioritize investing in improving detection capabilities.

5. **Respond & Recover** – Establish specific procedures to follow in response to an attack. It's not advisable to improvise in such situations, and if you don't have an in-depth plan in place for containing and remediating incidents, that will increase the damage, especially in reputation and customer trust.

KEY ATTRIBUTES THAT IMPROVE CYBER DEFENSE

By maintaining an awareness of following key concepts to threat management there will be an improvement in an organization's cyber security stance and risk reduction:

Contextualized – For up-to-date, accurate risk management, threats should be placed within the broader picture of their business context and attack surface. This includes the supply chain and emergent external and internal threats.

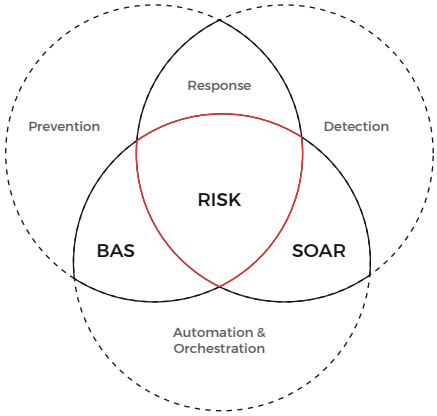
Pervasive – Effective defense requires high frequency, consistent assessment of attack surface reachability, exploitability, and prevention capabilities.

Data driven – Big Data, analytics, and data visualization must be applied to tune up and enhance detection against sophisticated outsider and insider attacks and to improve security capabilities.

Fast track – Security processes depend on enterprise agility and leveraging automation & orchestration. Although security is human-guided, it relies on interactive collaboration tools.

A HOLISTIC APPROACH TO CYBER SECURITY

CyberProof's fundamental approach to cyber security involves clarity of risk and investment. Our risk management platform involves several basic components that interact and overlap, creating a holistic and optimally effective solution:



CyberProof's Approach to Cyber Security Risk Management

"Tuning" prevention and increasing detection, so that the necessary response will be minimal – Our philosophy help customers to balance prevention, detection, and response. The goal is to prevent and detect more efficiently, so that data breaches are minimized and the necessary response to them is reduced to the absolute minimum while still being agile and lean.

Simulations and streamlined operations – Breach and Attack Simulation (BAS) tools help CyberProof test the resilience of customers by simulating the techniques, tools, and procedures of real world attackers. Security Operations Analytics & Reporting (SOAR) helps to streamline security operations whether preventative, detective, or responsive by leveraging external and internal intelligence for accurate prioritization. According to Gartner, by the end of 2020, 15 percentage of organizations with a security team larger than five people will leverage SOAR tools for orchestration & automation reasons, from less than 1 percentage in 2017.

Risk management driven by threat intelligence – All CyberProof services are based on customer-tailored threat models, considering insights regarding the exposure of assets to threats (both external and internal) as opposed to simplistic compliance requirements. This allows CyberProof to identify and assess risks in an agile manner, thus facilitating fast track risk management.

Automation & orchestration – BAS offers pervasive, accurate, high-frequency prevention while SOAR offers prompt, accurate detection and agile, efficient response due to high-level automation and orchestration capabilities. CyberProof's AI based chatbot technology, SeeMo, provides the essential capability of facilitating effective collaboration across teams.

SUMMARY

Bottom line: Investing in detection and response is as crucial as investing in prediction and prevention.

And handling both these aspects of security effectively requires a sophisticated and integrated approach that leverages BAS and SOAR technologies, threat intelligence, and the power of AI.

But how do you determine how to stretch and maximize your security spend?

By adopting an approach that first, clarifies risk and investment and second, covers all aspects of cyber protection, it becomes possible to improve cyber resilience by optimizing prevention, detection, and response.

ABOUT CYBERPROOF

CyberProof, a fully owned subsidiary of UST Global, is a platform-enabled company, whose mission is to reduce cyber risk with flexible service models. At CyberProof, we approach risk modelling using a top-down model where we define the magnitude of attack and focus on the top attack scenarios. We then facilitate a business-oriented prioritization of a customer's investment in defense and response.

CyberProof was recently ranked Leader in the Forrester Wave™ Report: Emerging MSSPs Q3 2018, validating our disruptive approach to cyber security services.

For further information visit www.cyberproof.com.

LOCATIONS

Aliso Viejo | London | Singapore | Tel Aviv | Trivandrum