CyberProof Recognized for

2021

Technology Innovation Leadership

European Managed Security and
Professional Services Industry
Excellence in Best Practices

FROST & SULLIVAN

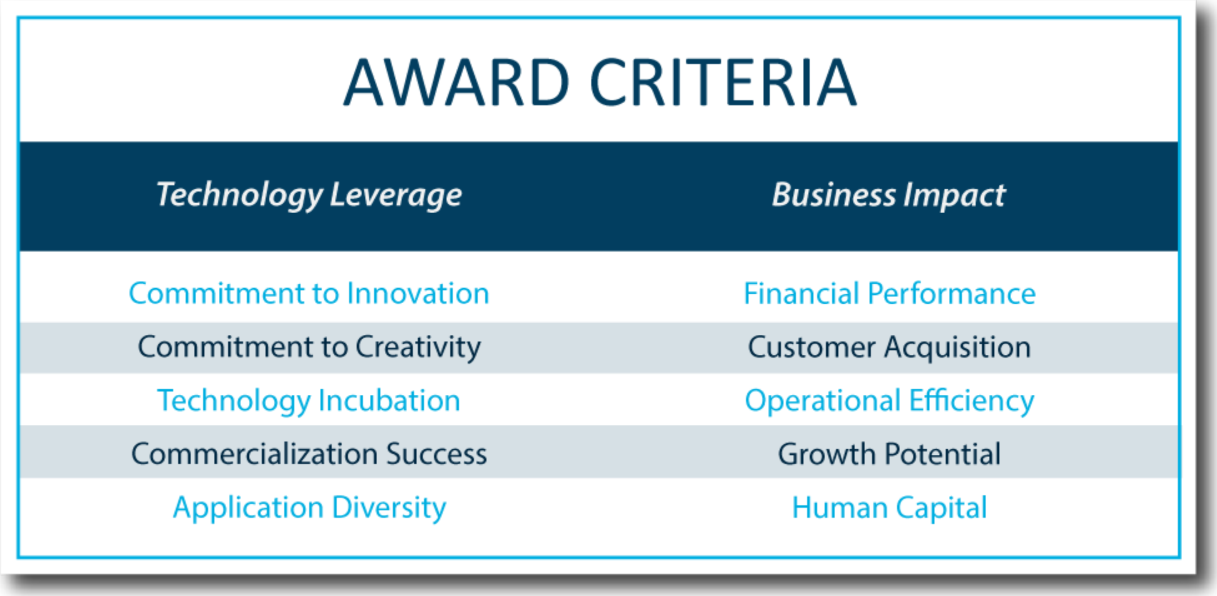
Strategic Imperatives

Frost & Sullivan identifies three key strategic imperatives that impact the security industry: geopolitical chaos, disruptive technologies, and innovative business models. Every company that is competing in the security space is obligated to address these imperatives proactively; failing to do so will almost certainly lead to stagnation or decline. Successful companies overcome the challenges posed by these imperatives and leverage them to drive innovation and growth. Frost & Sullivan's recognition of CyberProof is a reflection of how well it is performing against the backdrop of these imperatives.

SI8	GEOPOLITICAL CHAOS	DISRUPTIVE TECHNOLOGIES	INNOVATIVE BUSINESS MODELS
Why	• The COVID-19 pandemic caused manufacturing operations that rely on multi-national supply chains to experience significant disruptions. • Project extensions are delaying contract fund allocation, which will affect contractors and subcontractors' bottom lines. • Commercial and passenger-centric industries will experience sharp declines in revenue due to the impact of COVID-19, whereas opportunities in the public sector will grow exponentially. • National security skirmishes between nations continue to cause piecemeal disruptions to security technology deals.	• Investment in digitization will increase to improve the intelligence cycle and address the current threat landscape, which includes ransomware, digital intrusion, and data theft. • Wearables, drones, and augmented reality will find application in crime scene mapping, automatic translation, border surveillance, search and rescue, and threat detection. • Demand will increase for artificial intelligence (AI)-enabled remote or cloud interactions to foster better communication and system support.	• Security forces are gradually transitioning from ownership to subscription-based business models. New business models (e.g., screening as a service, biometrics as a service, ISR as a service, and infrastructure as a service) are reducing the cost of ownership. • Increasing need for niche security solutions, rapid tech advancements, and budget pressures will drive the industry to explore innovative revenue models. • Customers want modular surveillance alternatives that allow for the contracting and scaling of long-term system design.
When	• Firms will need to pursue strategic partnerships between vendors with complementary solutions and local suppliers to improve global customer reach, without increasing their overhead costs. • After the pandemic, larger security companies will realign and acquire portfolios and businesses in growth areas (such as digital security) to expand their solution portfolios across end-user verticals. • Cloud access, zero-trust and multi-factor authentication, and security-as-a-service solutions will become imperative to business continuity in the next 1 to 5 years. • Security firms must understand the national security policies applicable to specific international customers because policy affects security technology.	• Firms must prioritize the development of data analytics and sensor networks' capabilities to provide increased value to customers. • Security companies will need to invest in contactless technologies, biometrics solutions used with AI technology, remote access and authentication, and multi-use analytics in the next 4 to 5 years. • Firms will need to differentiate technology offerings for vertical-specific solutions (i.e., analytics tailored to an airport or public safety function) among multiple end-user industries. • Actionable intelligence and multi-source data aggregation will gain prominence in the next 5 to 10 years, as will the desire to shift some security operations away from a physical location to a cloud-based, remote system.	• Competitive strategy, technology, and IP opportunities will push vendors to re-examine their solutions and road maps to account for market slowdowns. This will lead them to reposition existing offerings to meet new market demands in the next 2 to 3 years. • Achieving vertical market expansion and distribution channel optimization through strategic partnerships and acquisitions will become top priorities in the next 3 to 6 years. • Businesses will seek flexible business models to stay lean by minimizing capital expenditure while ensuring scalability and redundancy in critical operations processes. These models include leasing/renting and moving toward a security as a service (SECaaS) approach in the next 5 years.

Best Practices Criteria for World-Class Performance

Frost & Sullivan applies a rigorous analytical process to evaluate multiple nominees for each Award category before determining the final Award recipient. The process involves a detailed evaluation of best practices criteria across two dimensions for each nominated company. CyberProof excels in many of the criteria in the managed security and professional services space.



AWARD CRITERIA

Technology Leverage	*Business Impact*
Commitment to Innovation	Financial Performance
Commitment to Creativity	Customer Acquisition
Technology Incubation	Operational Efficiency
Commercialization Success	Growth Potential
Application Diversity	Human Capital

Enabling a Stronger and Smarter Security Operations Center

Founded in 2017 and headquartered in Aliso Viejo, California, CyberProof is a global company that enables smart security operations with a management platform for incident detection and response. The company is a subsidiary of UST, its parent company which provides IT services and solutions to more than 140 clients globally in industries such as banking and financial services, healthcare, retail, technology, media, and telecommunications. CyberProof focuses on revolutionizing customer's daily operations through digital transformation by offering agile managed security services with unique attention to each client's network and security operation's needs for optimizing threat detection and response. To meet customer needs, the company deploys its services from its Cyber Defense Centers (CDC) located in California, Barcelona, Tel Aviv, Trivandrum, and Singapore. While driving its security operation centers' (SOC) initiatives, the company recognized three key challenges that impact the managed security and professional services market space.

> *"CyberProof focuses on revolutionizing customer's daily operations through digital transformation by offering agile managed security services with unique attention to each client's network and security operation's needs for optimizing threat detection and response."*
>
> ***- Steven Lopez, Best Practices Research Analyst***

These challenges include the demand for enhanced visibility of threats that matter the most, the desire to improve detection and response continuously, and the need for a hybrid engagement model. Receiving enhanced visibility means identifying the vulnerabilities that will impact the overall business the most and mitigating the threats as quickly as possible. The next challenge is showing teams steps towards making improvements that require agile development and maintenance for specific use cases and ensuring that the use cases align with business risk mitigation needs. Lastly, the need for a hybrid engagement includes working with the right skills at the right time, i.e., having a cyber defense platform that provides a collaborative hybrid SOC environment, enabling transparency into both in-house and outsourced activities, and a co-sourced delivery model to augment the customer's existing investments without losing control or relinquishing vital knowledge. Frost & Sullivan notes that CyberProof nicely proves its innovative strides by offering its best-in-class platform that ensures that customers overcome such challenges.

The company's CyberProof Defense Center (CDC) platform displays what CyberProof describes as "a single pane of glass" view of security operations for an organization's security team, providing transparency and collaboration with analysts and stakeholders that boost opportunities to make real-time decisions about cyber initiatives. The platform's features include smart automation, incident enrichment details, risk detection visibility, and rapid response tools, including SeeMo (the company's artificial intelligence bot), all working to strengthen a client's SOC architecture service. SeeMo operates as a virtual analyst for SOC operators to improve efficiency and routine tasks, reducing human effort and errors, and streamlining a course of action when minimizing risk through increased security operations. SeeMo also adds an extensive preliminary analysis of an incident (and sometimes a complete scan) before sending the data to a SOC analyst. SeeMo working with the CDC platform is how the company properly establishes enhanced visibility for teams.

Enforcing a hybrid model gives the company a leg up compared to other competitors as it can meet the demand for on-premise, cloud, and hybrid systems. The hybrid model focuses on a top-down and bottom-up approach, driving engagement and board-level conversations between stakeholders and CyberProof. Improving detection and response has always been at the forefront of CyberProof's platform offerings. The company helps customers shift from legacy to modernized platforms easily, and reap the full advantage of cloud-based security. CyberProof services are pre-integrated with the leading SIEM and EDR technologies including Microsoft Azure® Sentinel and Defender for Endpoint to enhance cyber risk preparedness, making systems more resilient while lowering costs.

CyberProof as a platform can integrate into any existing security analytics solution, driving high flexibility during deployment. Moreover, onboarding customers and providing services ready-for-use within weeks gives the company a unique advantage for enabling flexibility. CyberProof adds clear value by understanding that the type of loss occurrence for an attack varies in regards to the actual response time window. Slower responses can increase the negative impacts for an organization such as increasing the number of compromised assets, identity spoofing, increased operational costs, and ultimately brand erosion and loss of digital trust with customers. Addressing these negative outcomes drives CyberProof's added value to its customers. Frost & Sullivan recognizes CyberProof for its strategic offerings and use case models that revamp how enterprise security teams identify and respond to threats.

Commitment to Innovation: Creating Human-centered Innovation

CyberProof's innovation strategy stems from offering its customers flexibility and thinking outside of the box. The company co-creates with large companies to build next generation security operations and solve detection and response problems for both on-premise and cloud platforms through cloud-based security monitoring. The company streamlines innovation by strategically implementing its Use Case Factory model, i.e., the company maps the customer's business risks to the most likely attack scenarios (leveraging the MITRE ATT&CK framework) and develops and continuously refines operational content packages (including log sources, detection rules, response workflows, API integrations etc.) for detecting, preventing, and responding to these threats with the goal of measurable cyber risk reduction. The Use Case Factory is the brain of SeeMo; it requires experts to provide solutions to use case needs and reduce risks overall, optimizing detection, prevention, and response actions. As a unique offering to the Use Case Factory model, CyberProof maintains its Use Case Gallery by adding new use cases into use case bundles. For example, the company provides access to a library of more than 500 use cases, making this a key differentiator compared to other competitors. CyberProof's goal is to create use case bundles (prevention, detection, and response) by vertical with a "price multiplied by quantity" pricing model. In the near future, the company aims to build use case bundles by verticals that are not only limited to IT - but also cover areas including operational technology and the Internet of Things.

> *"The company's strong customer focus enables its growth potential to reach new benchmarks for the next couple of years, working with many of the world's leading organizations. Frost & Sullivan commends CyberProof on its innovative strategies to enhance operational efficiency for its customers."*
>
> ***- Steven Lopez, Best Practices Research Analyst***

Frost & Sullivan notes that CyberProof's knowledgeable team embodies agile performance, commitment, and innovative thinking. Innovation is an essential quality that the company exudes, with key differentiators such as how it provides exceptional service to customers through the hybrid model and how CyberProof is closing the gap between what the customer needs and what a security service provider can offer. The company commits to offering flexibility and how to work in parallel with the customer during their security innovation journey - especially with clients working with various business models. CyberProof develops its platform in-house, which allows it to constantly adjust and align its approach to its customer base. By continuing the importance of innovation in the security industry, the company established an office of innovation backed by experienced professionals with deep nation/state cybersecurity expertise. As a unique advantage to developing in-house, CyberProof is also building unique capabilities around migration between team knowledge and security analytics platforms, in particular, with enterprises that plan to accelerate digital transformation initiatives and record their knowledge to the cloud while modernizing their SOC. Given the strategy to migrate existing content and knowledge, CyberProof builds unique tools internally that rapidly reduce time and costs.

Customer Acquisition and Operational Efficiency: Offering Customers Complete Transparency

Transparency is a vital attribute for the company to meet and exceed evolving customer needs and partner with multiple customers simultaneously. CyberProof has a sophisticated sales process backed by extensive thought leadership that includes virtual events, white papers, and maintaining the flow of new research and development. The company has a dedicated sales team and defined sales process specific to cybersecurity demand, making it stand strong against some of the leading service providers in the managed security services industry. CyberProof monitors and adapts its price-times-quantity model to on-premise asset monitoring, and now innovates around the cloud, creating outcome-based pricing models that help CyberProof expand its customer centricity even further. The company's feedback mechanism envelops ongoing communication with its partners, ensuring it meets their needs. Moreover, CyberProof channels its attention to customer perception, an area that has not been traditionally focused on in the industry. In 2021, the company plans to implement initiatives for a smarter SOC summit that includes building a community around developers, security engineers, and organization leaders.

Overall, the company strives to market and increase innovation through automation, leading to increased internal efficiencies and efficacy. Ensuring operational efficiency remains steadfast, CyberProof internally provides a Service Maturity Steering group program, one of the internal governance programs, in addition to quarterly updates with senior management through its product management board that is lifecycle process-driven. The company's strong customer focus enables its growth potential to reach new benchmarks for the next couple of years by working with many of the world's leading organizations. Frost & Sullivan commends CyberProof on its innovative strategies to enhance operational efficiency for its customers.

Conclusion

Managing an organization's detection and response capabilities remains a necessity for companies struggling to stay one step ahead of security threats and reduce cyber risk. The challenges that affect customers using managed security and professional services are the lack of threat visibility that impacts business security the most, offering transparency through hybrid engagement, and improving detection and response.

CyberProof provides a cutting-edge platform that enables smart automation, data interpretation, detection and threat visibility, and real-time collaboration tools with its SeeMo chatbot. The Cyberproof platform helps enterprises manage a clear landscape of incident detection that allows teams to respond efficiently and effectively, reducing time and costs. Frost & Sullivan acknowledges the company's strategic business model and commitment to empowering customers with its comprehensive platform.

With its strong overall performance and industry-leading business impact, CyberProof earns the 2021 Frost & Sullivan Technology Innovation Leadership Award.

What You Need to Know about the Technology Innovation Leadership Recognition

Frost & Sullivan's Technology Innovation Award recognizes the company that has introduced the best underlying technology for achieving remarkable product and customer success while driving future business value.

Best Practices Award Analysis

For the Technology Innovation Leadership Award, Frost & Sullivan analysts independently evaluated the criteria listed below.

Technology Leverage

Commitment to Innovation: Continuous emerging technology adoption and creation enables new product development and enhances product performance

Commitment to Creativity: Company leverages technology advancements to push the limits of form and function in the pursuit of white space innovation

Stage Gate Efficiency: Technology adoption enhances the stage gate process for launching new products and solutions

Commercialization Success: Company displays a proven track record of taking new technologies to market with a high success rate

Application Diversity: Company develops and/or integrates technology that serves multiple applications and multiple environments

Business Impact

Financial Performance: Strong overall financial performance is achieved in terms of revenues, revenue growth, operating margin, and other key financial metrics

Customer Acquisition: Customer-facing processes support efficient and consistent new customer acquisition while enhancing customer retention

Operational Efficiency: Company staff performs assigned tasks productively, quickly, and to a high-quality standard

Growth Potential: Growth is fostered by a strong customer focus that strengthens the brand and reinforces customer loyalty

Human Capital: Commitment to quality and to customers characterize the company culture, which in turn enhances employee morale and retention

About Frost & Sullivan

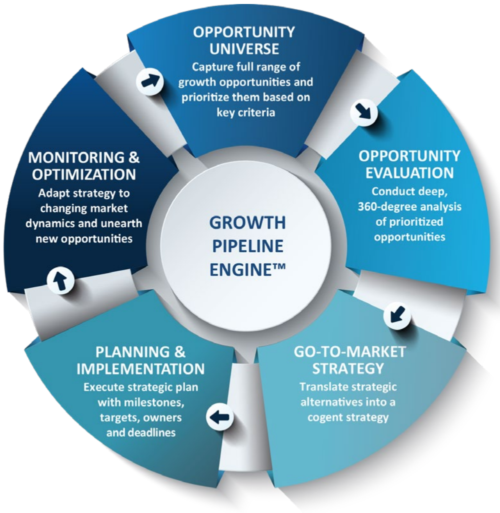
Frost & Sullivan is the Growth Pipeline Company™. We power our clients to a future shaped by growth. Our Growth Pipeline as a Service™ provides the CEO and the CEO's growth team with a continuous and rigorous platform of growth opportunities, ensuring long-term success. To achieve positive outcomes, our team leverages over 60 years of experience, coaching organizations of all types and sizes across 6 continents with our proven best practices. To power your Growth Pipeline future, visit Frost & Sullivan at http://www.frost.com.

The Growth Pipeline Engine™

Frost & Sullivan's proprietary model to systematically create on-going growth opportunities and strategies for our clients is fuelled by the Innovation Generator™. Learn more.

Key Impacts:

- ■ **Growth Pipeline:** Continuous flow of Growth opportunities
- ■ **Growth Strategies:** Proven Best Practices
- ■ **Innovation Culture:** Optimized Customer Experience
- ■ **ROI & Margin:** Implementation Excellence
- ■ **Transformational Growth:** Industry Leadership



OPPORTUNITY UNIVERSE
Capture full range of growth opportunities and prioritize them based on key criteria

OPPORTUNITY EVALUATION
Conduct deep, 360-degree analysis of prioritized opportunities

GO-TO-MARKET STRATEGY
Translate strategic alternatives into a cogent strategy

PLANNING & IMPLEMENTATION
Execute strategic plan with milestones, targets, owners and deadlines

MONITORING & OPTIMIZATION
Adapt strategy to changing market dynamics and unearth new opportunities

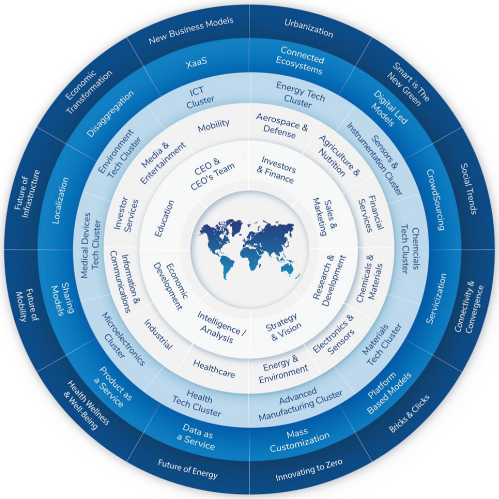
GROWTH PIPELINE ENGINE™

The Innovation Generator™

Our six analytical perspectives are crucial in capturing the broadest range of innovative growth opportunities, most of which occur at the points of these perspectives.

Analytical Perspectives:

- ■ Mega Trend (MT)
- ■ Business Model (BM)
- ▨ Technology (TE)
- □ Industries (IN)
- □ Customer (CU)
- ■ Geographies (GE)


Urbanization
Smart is The New Green
Social Trends
Connectivity & Convergence
Bricks & Clicks
Innovating to Zero
Future of Energy
Health Wellness & Well-Being
Future of Mobility
Future of Infrastructure
Economic Transformation
New Business Models
Connected Ecosystems
Digital Led Models
CrowdSourcing
Servicization
Platform Based Models
Mass Customization
Data as a Service
Product as a Service
Sharing Models
Localization
Disaggregation
XaaS
Energy Tech Cluster
Sensors & Instrumentation Cluster
Chemcials Tech Cluster
Materials Tech Cluster
Advanced Manufacturing Cluster
Health Tech Cluster
Microelectronics Cluster
Medical Devices Tech Cluster
Environment Tech Cluster
ICT Cluster
Aerospace & Defense
Agriculture & Nutrition
Financial Services
Chemicals & Materials
Electronics & Sensors
Energy & Environment
Healthcare
Industrial
Information & Communications
Investor Services
Media & Entertainment
Mobility
Investors & Finance
Sales & Marketing
Research & Development
Strategy & Vision
Intelligence / Analysis
Economic Development
Education
CEO & CEO's Team