Envisioning the Next Generation Cybersecurity Practices

Next Generation Security Critical to Protect the Future of Businesses Across Industry Sectors

D893-TV

December 2018

FROST & SULLIVAN

Contents

Contents (Continued)

1.0 Executive Summary

1.1 Research Scope

Cybersecurity has been in constant focus of enterprises in the recent past, especially in light of the breaches and hacks that have occurred recently. Hackers and criminals are getting more and more sophisticated and are devising more complex attacks which can cause significant damage to the affected parties. Companies are adopting more advanced solutions to protect their vital assets against these attacks.

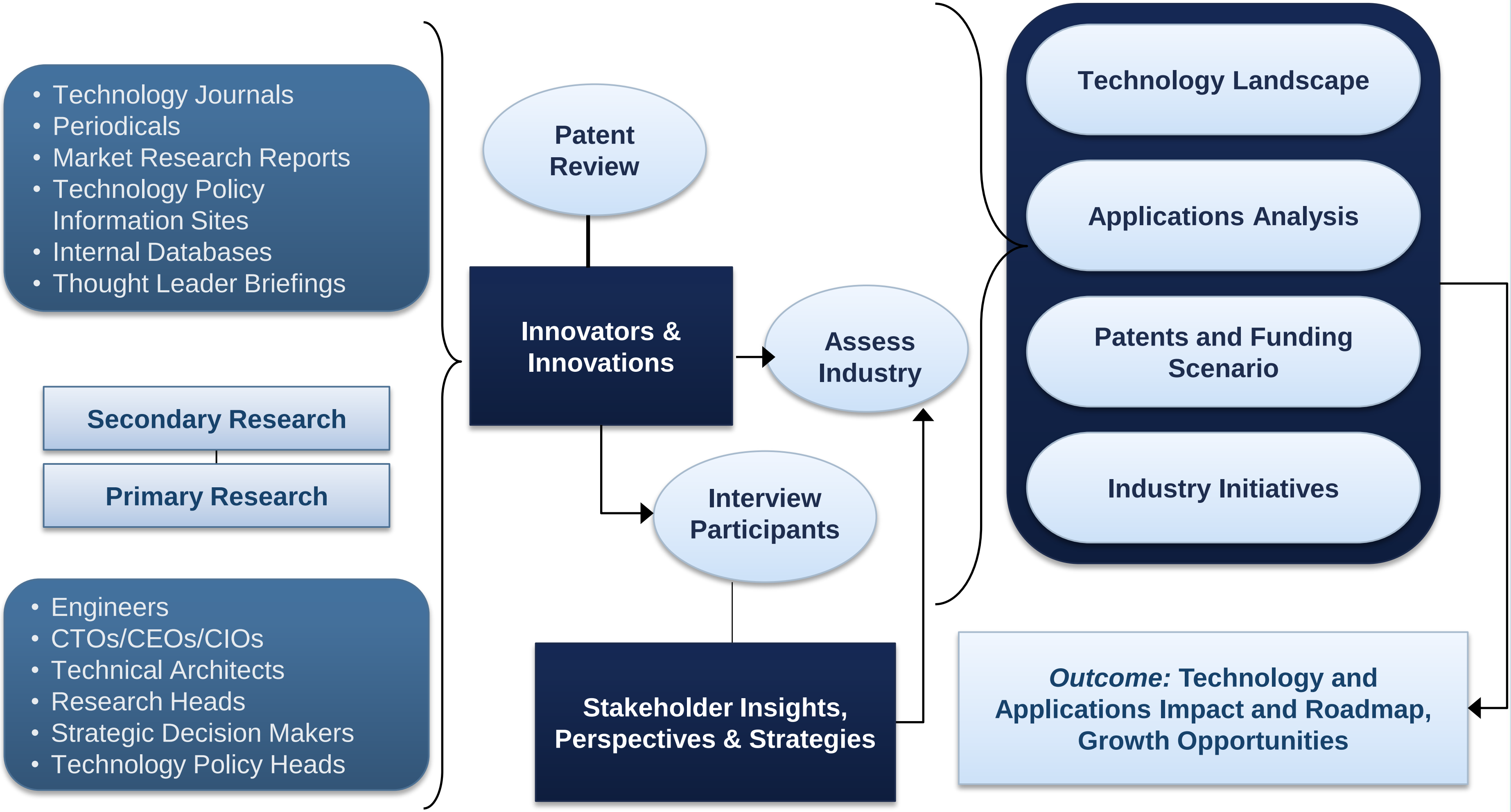
While data security and device usage policies were a concern of security teams until now, they are now becoming a management concern with the implementation of BYOD (Bring Your Own Device) and IoT (Internet of Things). Cybersecurity budgets have been increasing globally among companies in every industry vertical. With increased funding around cybersecurity, more startups have emerged in the space and have leveraged advanced technologies to develop products that have helped enterprises manage their security function better.

In brief, this research service covers the following points:

- Cybersecurity & Enterprises– An overview
- Drivers and challenges for Adoption of Best Practices in Cybersecurity
- Technologies Impacting the Future of Cybersecurity
- Considerations for Management Decision Making.

Source: Frost & Sullivan

1.2 Research Methodology



- Technology Journals
- Periodicals
- Market Research Reports
- Technology Policy Information Sites
- Internal Databases
- Thought Leader Briefings

Secondary Research

Primary Research

- Engineers
- CTOs/CEOs/CIOs
- Technical Architects
- Research Heads
- Strategic Decision Makers
- Technology Policy Heads

Patent Review

Innovators & Innovations

Assess Industry

Interview Participants

Stakeholder Insights, Perspectives & Strategies

Technology Landscape

Applications Analysis

Patents and Funding Scenario

Industry Initiatives

Outcome: Technology and Applications Impact and Roadmap, Growth Opportunities

Research Methodology

Research Process

Source: Frost & Sullivan

1.3 Research Methodology Explained

Step 1: To provide a thorough analysis of each topic, *TechVision* analysts perform a review of patents to become familiar with the major developers and commercial participants and their processes.

Step 2: Building on the patent search, the analysts review abstracts to identify key scientific and technical papers that provide insights into key industry participants and the technical processes, on which they work.

Step 3: The analysts then create a detailed questionnaire with content created to address the research objectives of the study, which functions as a guide during the interview process. While the analysts use structured questionnaires to guarantee coverage of all the desired issues, they also conduct interviews in a conversational style. This approach results in a more thorough exchange of views with the respondents, and offers greater insight into the relevant issues than more structured interviews may provide.

Step 4: The analysts conduct primary research with key industry participants and technology developers to obtain the required content. Interviews are completed with sources located throughout the world, in universities, national laboratories, governmental and regulatory bodies, trade associations, and end-user companies, among other key organizations. Our analysts contact the major commercial participants to find out about the advantages and disadvantages of processes and the drivers and challenges behind technologies and applications. Our analysts talk to the principal developers, researchers, engineers, business developers, analysts, strategic planners, and marketing experts, among other professionals.

Step 5: The project management and research team reviews and analyzes the research data that are gathered and adds its recommendations to the draft of the final study. Having conducted both published studies and custom proprietary research covering many types of new and emerging technology activities as well as worldwide industry analysis, the management and research team adds its perspective and experience to provide an accurate, timely analysis. The analysts then prepare written final research services for each project and sometimes present key findings in analyst briefings to clients.

Source: Frost & Sullivan

1.4 Key Findings

1

Cybersecurity practices are evolving and companies are increasing their IT and security budgets. Cybersecurity startups are coming up with innovative approaches for battling cyber crime and have witnessed high interest from investors. The industry is expected to witness wider adoption and growth during 2020 to 2025.

2

In the coming years technologies such as Machine Learning, Big Data and Blockchain will take the center stage as propelling cybersecurity approaches toward modernization. These modernization efforts would be centered around protecting enterprises from the threats emerging from IoT devices and from an expanding threat landscape.

3

Cybercrime is emerging as a easy way of monetization for cyber criminals and the recent ransomware attacks have motivated cybercriminals to pursue advanced tactics to affect more companies and maximize their revenues. Countries and governments have also made use of cyber crime to wage warfare against other countries and affect their vital assets.

4

The adoption of advanced security tools is on the rise among enterprises but at the same time, enterprises are also facing a sizeable talent gap and are finding it difficult to procure qualified security analysts who can understand and maintain unconventional security tools.

Source: Frost & Sullivan

2.0 Overview

2.1 Easier Monetization From Cybercrime is Driving Criminals to Design and Deploy More Sophisticated Attacks

~$600 Billion
Expected Cost of Cybercrime Globally

~300,000 – 1,000,000
Estimated Viruses and Malware created per day

143 Million
Americans Affected by Cybercrime

Ransomware as Means of Monetization

Ransomware attacks have proven to be easier to orchestrate and are difficult to detect. Additionally ransomware provide a clear path to monetization to the criminals, facilitated even more smoothly with cryptocurrencies.

Encrypted Cybersecurity Attacks

Encryption is now being widely used by attackers with more and more attacks coming from the SSL (Secure Sockets Layer) traffic. Traditional approaches of cybersecurity have largely ignored encrypted traffic which is now also being used by criminals to send data out of organizations.

IoT is the New Battle Ground

IoT devices with weak security controls are getting connected to enterprise networks which are being used by criminals to gain access to networks. The user focused nature of IoT devices stands to put vital personal data at risk of hackers in case of a breach.

Cybercrime as a Service

High profile cyber criminals have made use of dark web and crypto currencies to establish marketplaces for cybercrime, leveraging which anyone can initiate cyberattacks. The success of this business model has placed pressure on law enforcement teams.

State Sponsored Attacks

With almost all developed and developing economies implementing digital initiatives, cyber warfare is gaining momentum. Countries such as China, North Korea and Russia have been known to use cyberattacks as a means of attack and espionage.

Social Engineering

Hackers are now targeting individual users and leveraging lapses in their internet usage behavior to gain access to enterprise networks. Social media is the most prominent channel for hacker groups to share information.

Technology knowledge is abundant and cybercrime is rewarding to criminals. It is easy to orchestrate attacks against vulnerable networks and the chances of getting caught and prosecuted are perceived as low. Complexity of IT infrastructure is increasing day by day and internet penetration among individual users is witnessing tremendous growth. This is undoubtedly the most conducive time for hackers to attack digital assets.

Source: Frost & Sullivan

2.2 Efforts of Enabling Flexibility and User Convenience are Leaving Enterprise IT Infrastructure More Susceptible to Cyber Attacks

BYOD

- **6/10 companies** in US have a BYOD Program
- Using personal devices for work results in 34% increase in productivity
- Security is an inhibitor for 67% of organizations who have not adopted BYOD

- **51% of companies** allowing BYOD have experienced mobile data breach
- E-Mail, calendar and contact management are the most common applications used via BYOD

Cloud Adoption

- **97% companies** globally use cloud services
- 40% IT leaders are slowing cloud adoption due to lack of cybersecurity skills
- 27% of IT security budgets are allocated to cloud security

- 59% of organizations Globally are using Hybrid Cloud
- **84%** organizations store at least some sensitive data in the cloud
- **1/4 cloud users** have been a victim of data theft from their hosted infrastructure

NAC

- **62.3%** of enterprises rely on NAC (Network Access Control) to minimize their attack surface
- NAC compliments BYOD and IoT by helping IT teams maintain visibility into devices and user activity

- 45% of organizations Globally have increased their spending access management in 2018
- 43% organizations secure external user's access to corporate resources with MFA
- **Less than 50%** of enterprises make use of advanced authentication methods such as Biometrics, Key Fobs and OTPs (One Time Passwords)

Security Spending

- Average IT budget of an American organization is **$11.65 Million** out of which **10.6%** is allotted to cybersecurity
- 59% of companies globally are increasing their cybersecurity budgets to acquire better solutions

Top Spenders on Cybersecurity Globally

11.7%	Financial Services
11.3%	Pharmaceuticals & Healthcare

Source: Frost & Sullivan

2.3 Increasing Digitization Results in Significant Damages in Cases of Network Breach or Data Loss

Recent Attacks on Enterprises Globally have Highlighted the Need for Redesigned Security Policies and Solutions

Equifax Breach Unpatched Software Components

- Equifax, a consumer credit reporting agency, was a target of a cyber attack in which hackers gained access to personal details of 143 million customers. This data included sensitive details such as names, social security numbers and birthdates of customers.
- The breach was a result of an unpatched vulnerability in a tool called Apache Straus used in Equifax's online dispute portal. The patch for the flaw was issued by Apache Software foundation two months before the breach implying that timely software updates would have avoided the breach.

Petya, NotPetya & WannaCry State Sponsored Attacks

- 2017 saw multiple high profile ransomware attacks on individual and enterprise systems. Some of the companies infected in the attacks were Merck, Rosnoft and NHS (National Health Service). Although the scale of the attacks was global, some of the attacks such as Petya & NotPetya are believed to have been specifically targeted against Ukraine.
- WannaCry is believed to have been orchestrated by North Korea to cause damage while earning direct revenue.
- Most attacks were carried out and designed using an exploit called EternalBlue, uncovered in a pervious hack.

Mirai Botnet IoT Devices to Blame

- The Mirai botnet initially came to light in October 2016 when it triggered a massive DDoS attack crippling internet access in parts of United States.
- The botnet was designed to leverage poorly protected IoT devices by using telnet to discover devices using factory default passwords and then taking control over them to orchestrate co-ordinated DDoS (Distributed Denial-of-Service) attacks on victims.

Source: Frost & Sullivan

3.0 Drivers & Challenges

3.1 Drivers and Challenges for Adoption of Best Practices in Cybersecurity

Cybersecurity: Key Market Drivers, Global, 2018-2027

Drivers	(2018-2019)	(2020-2021)	(2022-2027)
Expanding Threat Surface Due to IoT & BYOD	High	High	High
Inefficiency of Traditional Security Tools	High	Medium	Low
Automation of Trivial Security Tasks	High	High	High

Cybersecurity: Key Market Challenges, Global, 2018–2027

Challenges	(2018-2019)	(2020-2021)	(2022-2027)
Availability of Qualified Security Analysts	High	High	Low
High Costs of Acquiring & Deploying Solutions	Medium	Medium	Low
Interoperability of Cybersecurity Solutions	High	High	Medium

Source: Frost & Sullivan

4.0 Technologies Impacting the Future of Cybersecurity

4.1 Behavioral Analytics Enabled By Big Data Helps in Thwarting Access Control Frauds

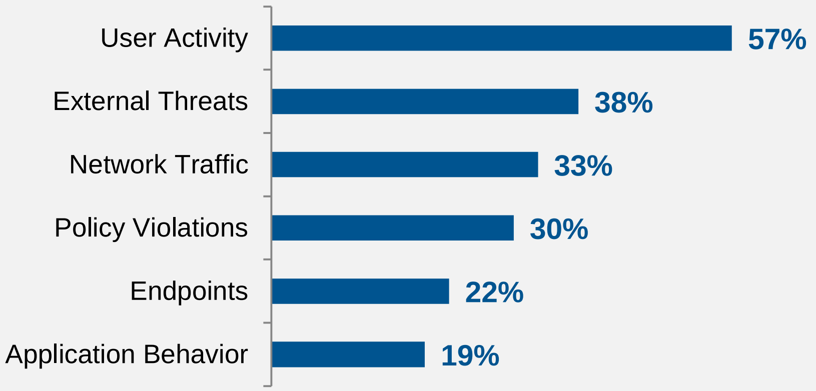
Big Data Analytics

The volume and variety of data being generated from diverse set of devices connected to increasingly complex networks can not be efficiently handled using traditional information security processes. Deploying big data solutions is essential for companies to expand the outlook of cybersecurity solutions beyond detection and mitigation of threats to proactively predict breaches before they happen, uncovering patterns from past incidents to support policy decisions.

Areas of Big Data Implementation

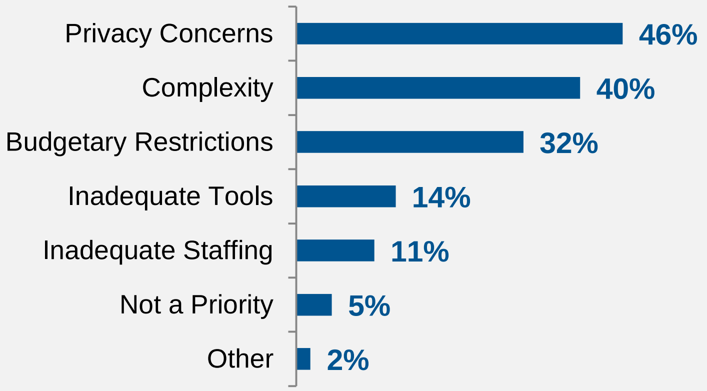
- Behavioral Analytics & Anomaly Detection
- Real-Time Data Analysis
- Data Maintenance

Areas With Need of Data to Enhance Security



The adoption of big data is driven by the interest in understanding usage and behavioral patterns helping SecOps identify anomalies.

Hindrances in Adoption of Big Data Practices



Privacy policies and tightening regulatory environment is creating ambiguity with respect to handling and monitoring of user data in turn affecting big data adoption.

Source: Frost & Sullivan

4.2 Big Data Has Enabled Automated Risk Management and Predictive Analytics

Companies Using Big Data for Cybersecurity

IBM

IBM has developed behavior-based predictive analytics solutions. Leveraging proprietary business analytics modeling patterns, the solutions track user behavior based on large volumes of data from internal and external sources.

Secureauth

Secureauth's access insight solution automates the task of identifying the risks with misalignment of user access rights. The solution aggregates data from identities, access rights, corporate policies and activity data across enterprise systems and applies advanced intelligence to derive actionable insights from the data.

LogRhythm

LogRhythm has developed a multi-dimensional behavioral analytics solution that leverages a behavioral whistling technique along with statistical and heuristic behavioral analytics to detect breaches. The solution combines massive amounts of log data, machine data and data in motion in real-time to detect anomalies from known usage patterns.

Use Cases in Industry Verticals

Using Big Data for Behavioral Analysis of Industrial Control Systems

Darktrace has developed an industrial immune system to help companies identify shifts in behavior of user devices connected to energy ecosystem. The solution uses big data analytics to learn the normal functioning of a system and recognize deviations from the expected network behavior.

This solution has been adopted by major energy companies such as Drax, OpenEnergi, and Enegy+.

Maintaining Visibility and Resilience into Retail Channels Using Machine Data

Splunk provides solutions that help companies analyze, visualize and monitor machine data from sources such as applications, customer devices & POS (Point of Sale) systems.

The omni-channel visibility of the solution reveals the customer's buying pattern, inventory status, supply chain level, and customer interaction feedback all at one place and correlates all the information to identify any changes in the behavioral activities or system operation.

Source: Frost & Sullivan

4.3 Machine Learning Helps Security Teams Prioritize Corrective Actions and Automate Real-time Analysis of Multiple Variables

> *“The way to secure our data, the way to prevent data theft, is more automation, we need new systems. It can’t be our people versus their computers. We’re going to lose that war. It’s got to be our computers versus their computers.”*
>
> ***CTO, A Fortune 100 Cloud Platform Provider***

Machine Learning

Utilizing the vast pools of data collected by companies, machine learning algorithms automate the process of identification and remediation of detected anomalies in the network. The use of machine learning also infuses efficiency into the work of security teams by reducing and prioritizing the actions that have to be carried out manually.

Areas of Implementation

- Automating Remedial Measures
- User Identification
- User & Entity Behavioral Analytics

Challenges in Enterprise Security	How Machine Learning Helps
Alert Fatigue	Automation & Prioritization
Identity and Access Management	Zero Trust Model
Hybrid Cloud Environment	Machine Learning based CASB (Cloud Access Service Broker)

Source: Frost & Sullivan

4.4 ML-based Cybersecurity Solution Can Identify the Root Cause of the Attack and Automate the Process of Remediation

Companies Using Machine Learning for Cybersecurity

Tanium

Tanium has developed a natural language parser that enables user to find information using natural questions instead of using a specialized query language.
The system is designed to automatically correlate the user's question with system data and execute the required changes to self-heal the endpoint networks and ensure smooth functioning.

BehavioSec

BehavioSec offers a non-intrusive behavioral biometrics solution that uses AI to profile users based on their device usage pattern by measuring matrices such as mouse movement, keystroke dynamics and type pressure data.

Anodot

Anodot uses an ML-based anomaly detection method to uncover unusual behavior pattern in data. The solution uses a holistic view of anomalies detected across devices and networks to uncover patters between seemingly unrelated events. The platform is designed to handle complexities such as seasonality, trends, and changing behaviors in the data.

Use Cases in Industry Verticals

Jask Helps Encompass Health Tackle Cybersecurity Skills Shortage

Encompass Health, a US-based provider of various health services was highly reliant on a small security team working on manual solutions. The company's high dependency on its cyber talent made it vulnerable to attacks.

Jask was able to help the company in automating assessments of majority of daily incidents, freeing up analysts to focus on high priority threats and decreasing its response time from hours to seconds.

Cylance Protects Vital Industrial Assets Against Cyberattacks

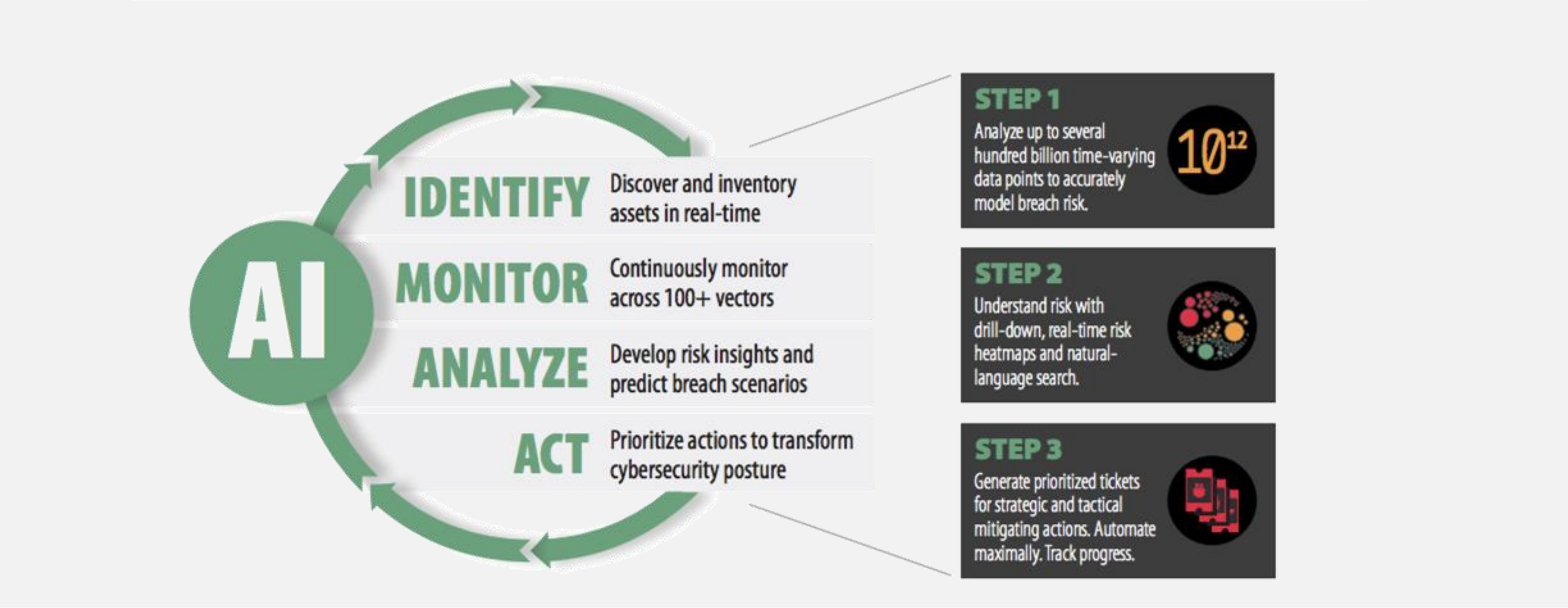
Klaus Union, a producer of pump systems and valves used Cylance's solutions to protect its IP (Intellectual Property) assets after discovering their incumbent solutions were unable to thwart attacks for ransomware and malware.

Cylance uses AI & ML-based techniques to spot the threats before they affect the victim.

Source: Frost & Sullivan

4.4.1 Balbix Leverages ML / AI to Provide Security Posture Visibility and Transformation

Balbix BreachControl leverages machine learning and artificial intelligence to help security teams achieve full visibility of their enterprise attack surface and transform their security posture by providing real-time cyber-risk prediction and prioritized mitigating actions.


AI
IDENTIFY
Discover and inventory assets in real-time
MONITOR
Continuously monitor across 100+ vectors
ANALYZE
Develop risk insights and predict breach scenarios
ACT
Prioritize actions to transform cybersecurity posture
STEP 1
Analyze up to several hundred billion time-varying data points to accurately model breach risk.
10¹²
STEP 2
Understand risk with drill-down, real-time risk heatmaps and natural-language search.
STEP 3
Generate prioritized tickets for strategic and tactical mitigating actions. Automate maximally. Track progress.

- Balbix BreachControl performs continuous, real-time cyber-risk assessment of all IT asset types (managed, unmanaged, BYOD, IoT, third-party) across 100+ attack vectors – not just unpatched software.
- Balbix's five-dimensional risk assessment model uses multiple ML algorithms including deep learning to assess risk based on vulnerability severity, threat level, business criticality, exposure/usage and compensating controls – resulting in a list of prioritized actions to reduce cyber-risk.

Source: Balbix

4.5 Data Stored on Blockchain Cannot be Manipulated or Erased By Design

> *“Single points of failure can be avoided. When they are distributed, an attacker would have to hack each single device to obtain each single key. Devices talk to each other over this decentralized blockchain, which does not have a single point of failure.”*
>
> ***Co-founder, Blockchain Services Startup***

Blockchain

The inherent nature of blockchain makes it nearly impossible for hackers to corrupt data stored on them. The absence of central authority and tractability of activities performed on blockchain are integral to establishing a trustworthy network between endpoints, where the authenticity of the data can be assured based on the consensus mechanism.

Areas of Implementation

- Data Storage & Access
- Change Logs & Access Records
- Global Web Security

Challenges in Enterprise Security	How Blockchain Helps
Attacks on Critical Assets	Distributed Architecture
Data Tampering and Change Logs	Cryptographic Hashing
Identity and Access Management	Distributed PKI (Public Key Infrastructure)

Source: Frost & Sullivan

4.6 The Cost of Breaching Blockchain-based Networks Dissuades Hackers From Attacking

Companies Using Blockchain for Cybersecurity

BLOCK ARMOUR

- Block Armour offers a blockchain defined perimeter (BDP) which renders critical enterprise assets and data sets invisible to unauthorized users.
- The BDP provides users with cryptographically secured access to critical assets and also maintains immutable logs of each and every transaction within the network.

Key Features

- Phishing Resistant Authentication
- Zero Trust Model
- Invisible Locked Down Critical Systems
- Immutable Tamper Proof Logs

xage SECURITY

- Xage Security offers blockchain-based tools that help utilities and infrastructure providers secure their assets and systems using blockchain.
- Xage's policy management tool is aimed at providing a decentralized solution to implement end-to-end security for companies with simpler and safer access controls on remote or on-site connections.

Key Features

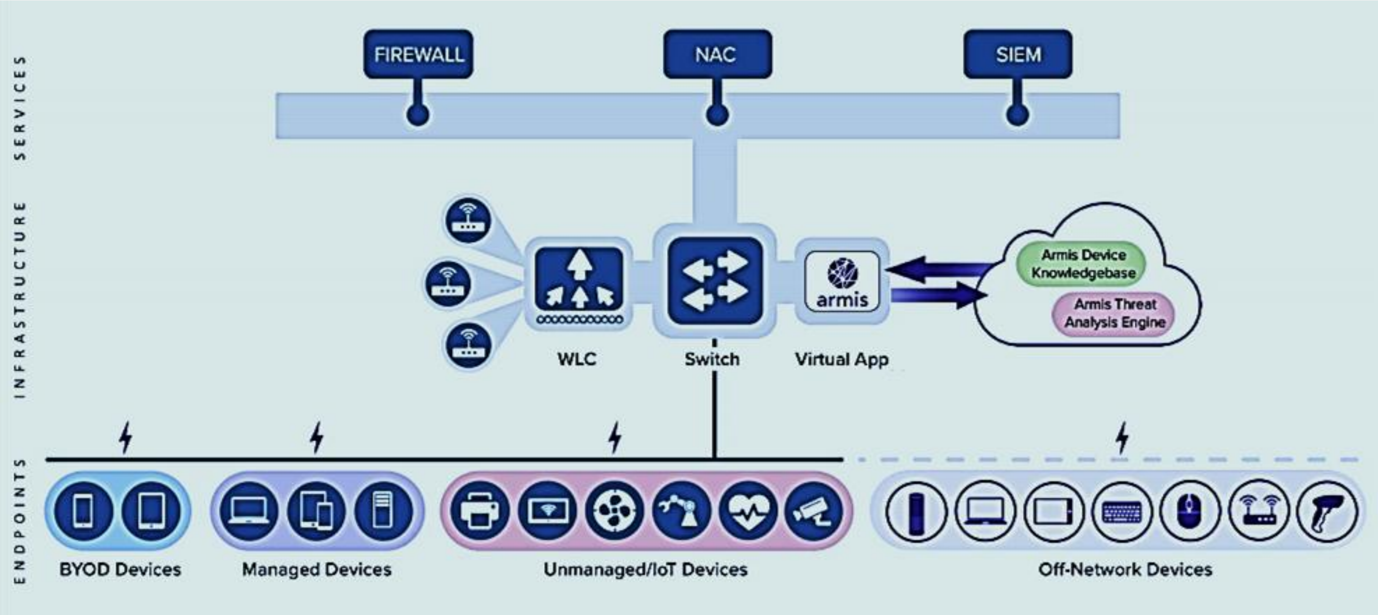
- Role-based Access Controls
- Automated Policy Enforcement
- Edge Authentication and Identity
- Device Lifecycle Management

Source: Frost & Sullivan

5.0 Companies to Action

5.1 Armis Automates the Task of Discovering, Managing and Protecting Enterprise IoT Devices

Armis offers security solution for a range of enterprise IoT devices on managed and unmanaged networks and monitors behavior of these devices to automatically initiate remediation measures in sync with the existing tools enforced by the organization.



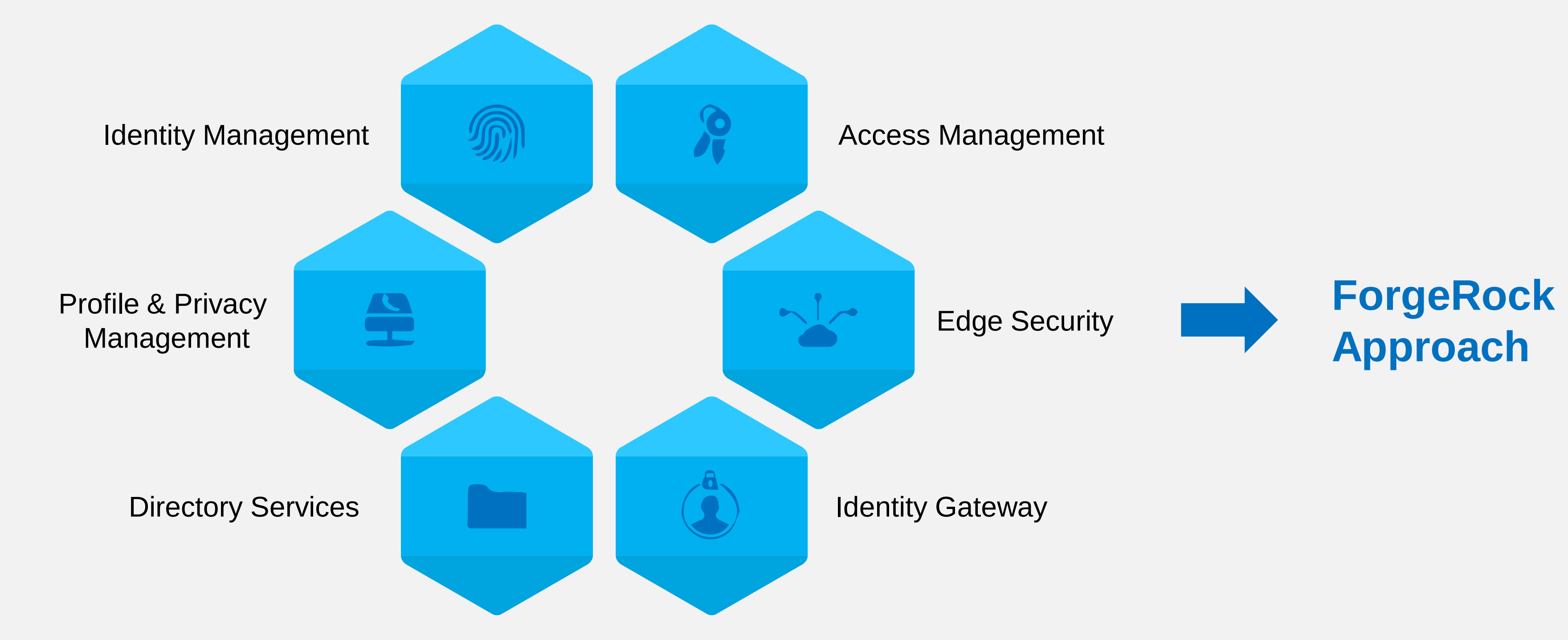
Armis Approach

- Armis provides a agentless security solution which does not require installation of any hardware. The solution leverages a virtual appliance for data collection which is then used to provide security for all devices connected to the network by default.
- The company has amassed a device knowledgebase of over six million unique behavioral profiles that can be leveraged to detect threats based on behavioral anomalies.

Source: Armis

5.2 ForgeRock has Designed an Identity and Access Management Solution to Support Modern Businesses Adopting IoT & BYOD

ForgeRock uses a relationship model to operate a context-based security system, connecting identities of users to the devices and data they use. While maintaining a highly secure authentication environment the company's solutions are also strongly focused on devolving a seamless user experience across endpoints



- The ForgeRock Identity platform is built to tie the identities of users, connected things and services together into a single user profile to personalize and protect the user experience.
- ForgeRock Identity platform provides real-time data and situational context on the basis of data that a customer can choose to share which can ultimately be used to improve customer engagement and can strengthen the compliance standing of the provider.

Source: Frost & Sullivan

6.0 Considerations for Management Decision Making

6.1 Negligence in Adhering to Security Directives Renders Advanced Security Controls Ineffective

Device Management

- Policy enforcement on personal devices remains a area of concern with the rise in adoption of BYOD.
- Smaller businesses with limited IT budgets are more likely to implement BYOD policies driven by cost benefits.
- IoT deployments are at times carried out outside the realm of IT departments and processes, leaving the endpoints unmonitored.
- Unsecure IoT devices are the weakest entry points into enterprise networks.

Recommendations

- Enforcing Security Controls from Ground-Up
- Ownership Models
- Virtualization Management

Data & Cloud Management

- Cloud Misconfigurations and misuse of employee credentials are emerging as the biggest threat to cloud security.
- Companies migrating to the cloud are overly reliant on CSPs (Cloud Service Provider) for security maintenance.
- Companies often deal with third party vendors who have access to the company’s network but have weak security controls.

Recommendations

- Shared Responsibility Model
- Identity and Access Control Management

Source: Frost & Sullivan

6.2 Stricter Regulatory Norms Globally Are Compelling Enterprises to Adopt Better Cybersecurity Practices

Risk Assessment & Compliance

- Every business activity and flow of information needs to be evaluated in terms of the company's security posture to gauge the effectiveness of cybersecurity controls.
- Unification and streamlining of risk assessment and management practices is necessary to develop a single cybersecurity approach.
- While mandatory compliance directives are followed strictly among enterprises, adherence to voluntary guidelines is on the decline.

Recommendations

Crisis Response Planning and Testing

Selecting a Cybersecurity Framework

Maintaining Global Yet Regionally Compliant Policies

Budget Planning

- Post-Breach solution and recovery mechanisms need more investments.
- Investing in hiring and training IT staff is being prioritized to accelerate the adoption of advanced security solutions against legacy practices.
- Companies are leaning toward adopting cyber-insurance to leverage additional services provided by insurers to improve cyber resilience.

Recommendations

Balancing Budget Allocations between Preventive & Reactive Controls

Internal Talent Building vs. Outsourcing

Source: Frost & Sullivan

Legal Disclaimer

Frost & Sullivan takes no responsibility for any incorrect information supplied to us by manufacturers or users. Quantitative market information is based primarily on interviews and therefore is subject to fluctuation. Frost & Sullivan research services are limited publications containing valuable market information provided to a select group of customers. Our customers acknowledge, when ordering or downloading, that Frost & Sullivan research services are for customers' internal use and not for general publication or disclosure to third parties. No part of this research service may be given, lent, resold or disclosed to noncustomers without written permission. Furthermore, no part may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the permission of the publisher.

For information regarding permission, write to:

Frost & Sullivan
331 E. Evelyn Ave. Suite 100
Mountain View, CA 94041