IT Operational Security – A data driven approach

IT Ops and Cyber Security – A White Paper

The Hybrid shift in IT - Fighting for Efficiency - Data Security - IT Operations Security Management

ITML
March 2020

Two themes in enterprise technology have emerged in recent years:

- **The rise of the digital enterprise across sectors and internationally.**
- **The need for IT to react quickly and develop innovations aggressively**

Source: McKinsey & Co.

A paradigm shift in IT

Technology is continuously changing society, shaping a new digital world where everyone (and soon everything) is online; people and businesses connect on many levels and this has come to be expected as the norm. More data are constantly created and circulated with relative ICT infrastructure stretched and expanded while software applications are created and operated with unprecedented agility, speed and complexity.

From private datacenters, through the edge and onto the cloud, it is already well indicated that we are experiencing a new, hybrid model[(1)] of IT operations as the current state of affairs and the marker for what is to be expected.

This multilayered grid of systems and networks, however, still breaks down to simple elements: devices, connections, software and data. Even more so, connections of any nature, digital ones notwithstanding, need to be based on some basic principles to exist, with that of trust being at the foundation.
Trust is built on security; in the world of ICT operations, security has righteously become big business and multiple threats are now real and common. But, as more investment and spending is funneled towards security, it is increasingly recognized that the new hybrid paradigm calls for new approaches to address complexity, overspending and operational efficiency.

In the 2020s, we believe that traditional on-premises deployment, not cloud, will require the justification. Welcome to the new world of the Hybrid Default
ZDnet -January 2020[(1)]

Cybersecurity leaders:

- **Invest for operational speed**
- **Drive value from new investments**
- **Sustain what they have**

Source: Accenture

The fight for efficiency

Under the light of digital transformation, IT operations become the most significant element of daily business activities. Combined with developments like the convergence and abstraction of IT resources, they are transforming corporate assets and the way companies are valued and financed.
Business trust and performance evokes thus enhanced cyber security and the corporate world strives to respond: According to Accenture's report on cyber security for 2020, related innovation is growing. Organizations now spend an average of near 11% of their IT budgets on cybersecurity programs[3].
Increasing investment does appear to bring basic results: According to the same report, common security hygiene is better with a 25% average decrease on the number of breaches.
However, increasing new, "hidden" dangers lurk: The report's relevant research indicates that about 40% of businesses face new, masked digital threats, with digital complexity and stretched infrastructure taking their toll. For almost two thirds (69%) of the businesses researched, rising security costs are becoming unsustainable and to a certain extend insufficient: 39% of organizations researched had more than half a million of customer records exposed in 2019. Overall, nearly three quarters (74%) of 4,600+ companies researched, are average performers in cyder security.
From the remaining quarter of businesses researched, a 17% portion (the "leaders") excel above the average performance, applying practices that coincide in the following:

- Invest for operational speed: Prioritizing processes and technologies that enable speed of detection, recovery and response. 88% of leaders detect security breaches in less than one day, on average.
- Drive value from new investments: Scale, train and collaborate more. Only 5% of cyberattacks resulted in a security breach for leaders best at scaling.
- Sustain basic existing resources: Looking after existing resources and succeed with fundamental data protection practices. Making sure the basics of data-centric security are in place. Leaders spend 39% of their budgets to sustain the basics

Source: Accenture

	STOP MORE ATTACKS	FIND BREACHES FASTER	FIX BREACHES FASTER	REDUCE BREACH IMPACT
LEADERS (17%)	1 in 27 attacks breach security	88% detect breaches in less than one day	96% fix breaches in 15 days or less	58% of breaches have no impact
NON-LEADERS (74%)	1 in 8 attacks breach security	22% detect breaches in less than one day	36% fix breaches in 15 days or less	24% of breaches have no impact

Data streaming analytics used as a weapon against cyber threats relies on factors that are critical for a technological tool or platform to achieve maximum efficiency:

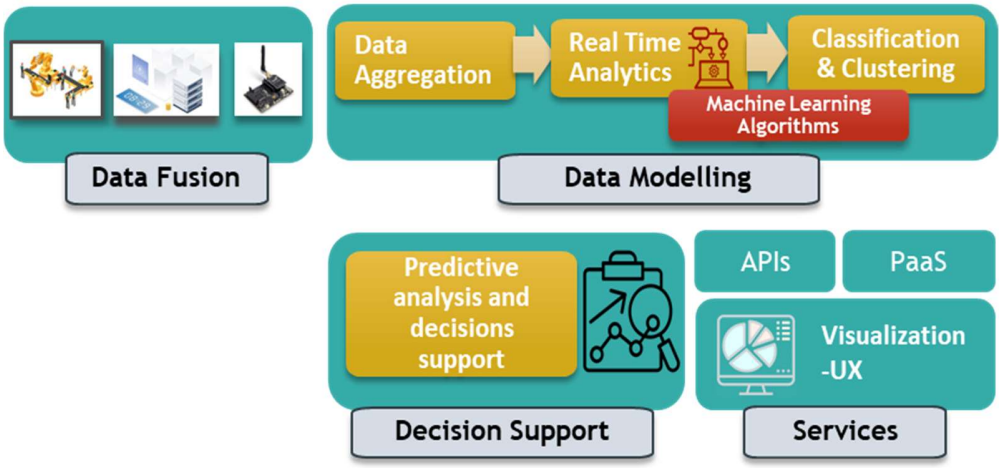
- **Deployment**
- **Data collection**
- **Workload**
- **Integration**
- **User access**

Source: ROXANNE research project [4]

Data Security

The new digital reality is all about data – they are abundant, available and accessible like never before; they contain value, they can be monetized and bring profit. Therefore, over the last years, data mining and analytics have become key players in IT security.
ITML has the opportunity to research and apply security analytics engaged in European projects such as ROXANNE, where data analysis is deployed for investigations on digital security.
Research indicates that real time data streaming analysis from various sources, can make a difference in cybersecurity policies. Streaming analysis is an armor against cyberattacks and network intrusions which have non-static characteristics. Systems that conduct stream analytics can be used for anomaly detection in real-time.

A data driven approach to cyber security



Scalability is important, as IT architectures need to address data growth and complexity. Time is also critical: Outdated data or streaming delays affect the efficiency of security policies.
Protecting data streams with fault-tolerant resources and high throughput is also essential in order to ensure privacy, integrity and operability for data-driven security policies

"Data streaming can be a powerful tool for an organization aiming to a quick reaction to a cyber threat or, even further, to detect trends that lead to timely knowledge and early warning"

Source: ROXANNE research project

Components of data driven IT operations security management platform:

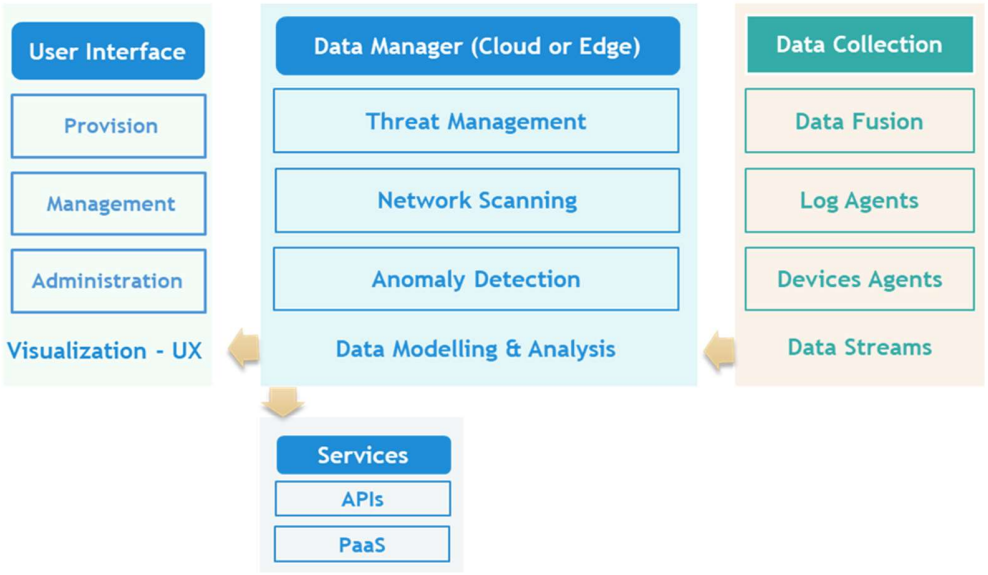
- **Data collection agents**
- **Data processing Manager**
- **Data Based operational monitoring services (APIs, PaaS)**
- **Visualization - UX**

Source: ITML Security Infusion

IT operations and security management

As already outlined, caring for the basic elements of IT infrastructure is fundamental for efficient cyber security policies. Furthermore, averting complexity and excessive spending is paramount.
Complying with these principles, the widely available open source framework can be leveraged to establish data collection from every basic ICT element: From device-related data up to network processes and services, data can be accumulated and streamed as the raw material of IT ops security management.
Data management and exploitation in a world of hybrid IT operations need also to be enabled in a flexible manner: Cloud data processing is as essential as on-premise (edge); hybrid deployment options should be the norm. Edge deployment of data-based tools particularly, can bring considerable additional advantages, especially when it is combined with inbound network scans that complement the collection of primordial operational data.
Finally, all these need to be interweaved into a simple and functional user experience, that saves time money and resources.

IT operations security management platform concept



ITML's **Security Infusion** is a software solution that collects, analyzes and visualizes operational, real time, data of IT resources. Furthermore, the system stores historical (i.e. logs and events) for retrospective analysis when needed. Network scans are also possible (port scanning and vulnerability assessment).
The solution can be deployed either at the edge of the monitored infrastructure or through the cloud to monitor IT operations.

Eventually, built-in machine learning makes time and data growth an ally for better situational awareness and response; the more data it collects the more effective it becomes.
Source: ITML Security Infusion

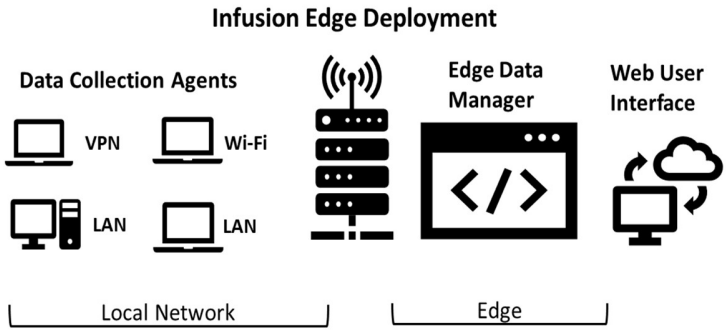
The Infusion Data Manager can be installed on a virtual or a physical machine, either at the network edge (Edge Manager) or in the cloud (Cloud Manager).

Edge vs Cloud Deployment – Case Studies

A rising hybrid world of IT operations has been identified. Platforms and tools used in such an environment incorporate different deployment options and provide flexibility in establishing efficient policies.
Drawing from its experience, ITML has approached different cases and user needs, suitably addressed with the Security Infusion IT operations platform, levering the Edge and Cloud delivery options.

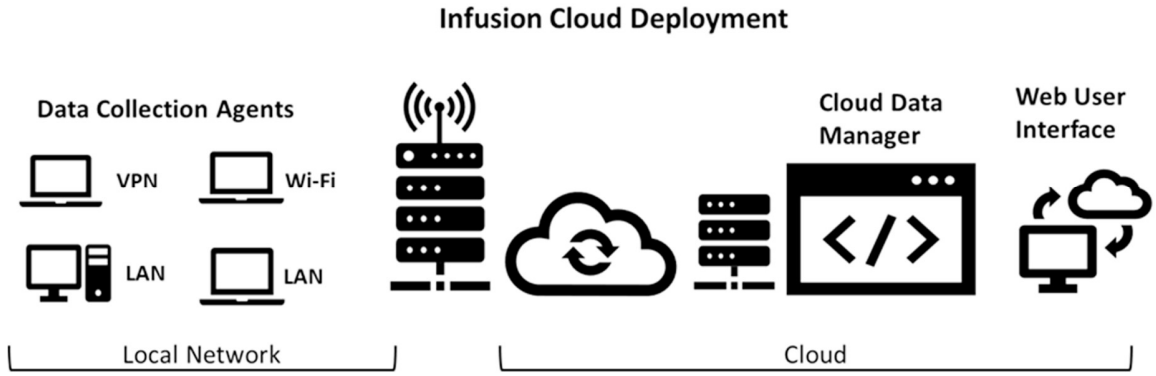
- **Infusion Edge Deployment Case**

A technology company deployed various agents on user's workstations with different profiles for real time operational monitoring. The users included both Windows and Linux terminals. The Infusion Manager was installed at the edge of their network and an operations center was established. Furthermore, as the Edge Manager provides the ability for regular network scans, daily port scanning and weekly vulnerability assessments were established, realizing the basis of the company's cybersecurity policies.



- **Infusion Cloud Deployment Case**

A managed services provider needed a tool to monitor its clients managed IT infrastructure in order to fulfill and improve its SLAs. They looked at a cloud deployed version of Infusion, where they would have their a centrally run multitenant cloud manager with various sub domains, corresponding to their various clients. This deployment fully exploits Security Infusion's innate data analytics and machine learning technologies in order to establish efficient operational service delivery options for different end users. Additionally, versatile and specific network scans can be scheduled according to different end users' attributes.



References:

1. ZDnet : Data 2020 Outlook Part I: The Hybrid Default Era begins, January 2, 2020 - https://www.zdnet.com/article/data-2020-outlook-part-i-the-hybrid-default-era-begins/
2. McKinsey & Co. : Cybersecurity: Linchpin of the digital enterprise – July 2019 - https://www.mckinsey.com/business-functions/risk/our-insights/cybersecurity-linchpin-of-the-digital-enterprise
3. Accenture Security: Cyber Resilient Business, Lessons from leaders to master cybersecurity execution, January 28, 2020 - https://www.accenture.com/fi-en/insights/security/invest-cyber-resilience
4. ROXANNE project: Analysis of streaming data for security by ITML, February 2020 - https://www.roxanne-euproject.org/news/analysis-of-streaming-data-for-security-by-itml

ROXANNE Project

ROXANNE comprises a Project that enhances the efforts of fight against crime and terrorism. The ROXANNE platform, the cornerstone of technical development, will develop and provide criminal network analysis based on speech, language and video technologies. In that direction, extracted data of speech, text and video analysis will comprise the raw material of data fusion processes. ITML is responsible for data streams alignment that will be carried out by ITML's Data Fusion Bus (DFB). DFB enables organizations in developing, deploying, operating and managing a big data environment with emphasis on real-time applications. It combines the features and capabilities of several big data applications and utilities within a single platform.

ITML Overview

ITML provides innovative tailor-made software solutions building on technologies, such as big data analytics, advanced data mining, machine learning, data platforms and network operations.

ITML has engagements through (a) bilateral projects with private sector companies, (b) Public-Private Partnerships (PPP), (c) EU and beyond-EU funded projects, and nationally funded projects.

The team of ITML includes multi-disciplined software engineers, researchers, project managers and product specialists who are experts in analysis, validation and implementation of scientific results produced in the R&I context.

The company has active participation in numerous H2020 projects as technology provider and system integrator. Since 2017, ITML's engagement in R&D projects is almost doubling year over year, subsequently growing the company's headcount proportionally. This has accelerated commercial and market-related activities, including the development of products and services that address specialized business needs on a local and regional level.

ITML has associated its business with the broad R&I of cutting-edge technologies that drive the current digital transformation. Our team possesses working experience in Big Data and Analytics, Cyber Security, Smart Transportation, Logistics, IoT and data platforms.