ESG Brief

The Importance of a Common Distributed Data Services Layer

Date: January 2019 **Author:** Bob Laliberte, Senior Analyst

Abstract: The IT pendulum is swinging to distributed computing environments, network perimeters are dissolving, and compute is being distributed across various parts of organizations' infrastructure—including, at times, their extended ecosystem. As a result, organizations need to ensure the appropriate levels of visibility and security at these remote locations, without dramatically increasing staff or tools. They need to invest in solutions that can scale to provide increased coverage and visibility, but that also ensure efficient use of resources. By implementing a common distributed data services layer as part of a comprehensive security operations and analytics platform architecture (SOAPA) and network operations architecture, organizations can reduce costs, mitigate risks, and improve operational efficiency.

Overview

Modern business requires organizations to deliver a positive digital experience for both customers and employees. To do this, many organizations are embarking on digital transformation initiatives. Only 13% of respondents to ESG research describe their digital transformation initiatives as mature, while another 82% indicate that they have started or are planning their digital transformations.[1] To remain more competitive, organizations are also transforming their IT environments and distributing more compute across their extended infrastructures. This will provide numerous benefits to those organizations looking to take advantage of data generated from IoT sensors and mobile devices, but it also creates a much larger attack surface and network environment that needs to be protected and secured.

Ensuring Visibility and Security in a Distributed Environment

The shift back to distributed environments creates new challenges for organizations looking to gain visibility and secure their environments regardless of their locations. These challenges are compounded by organizations looking to extend operations to the cloud and deploy compute and data resources in remote locations. In the traditional consolidated model, all of the data was centralized, and all connectivity to the outside world was funneled through a handful of primary data centers. It was easier to have complete visibility and implement security in this model.

In a distributed model, organizations could simply replicate the solutions and personnel used in the data center at each remote location. This approach, however, could be costly, could require tools and people at each location, and would be

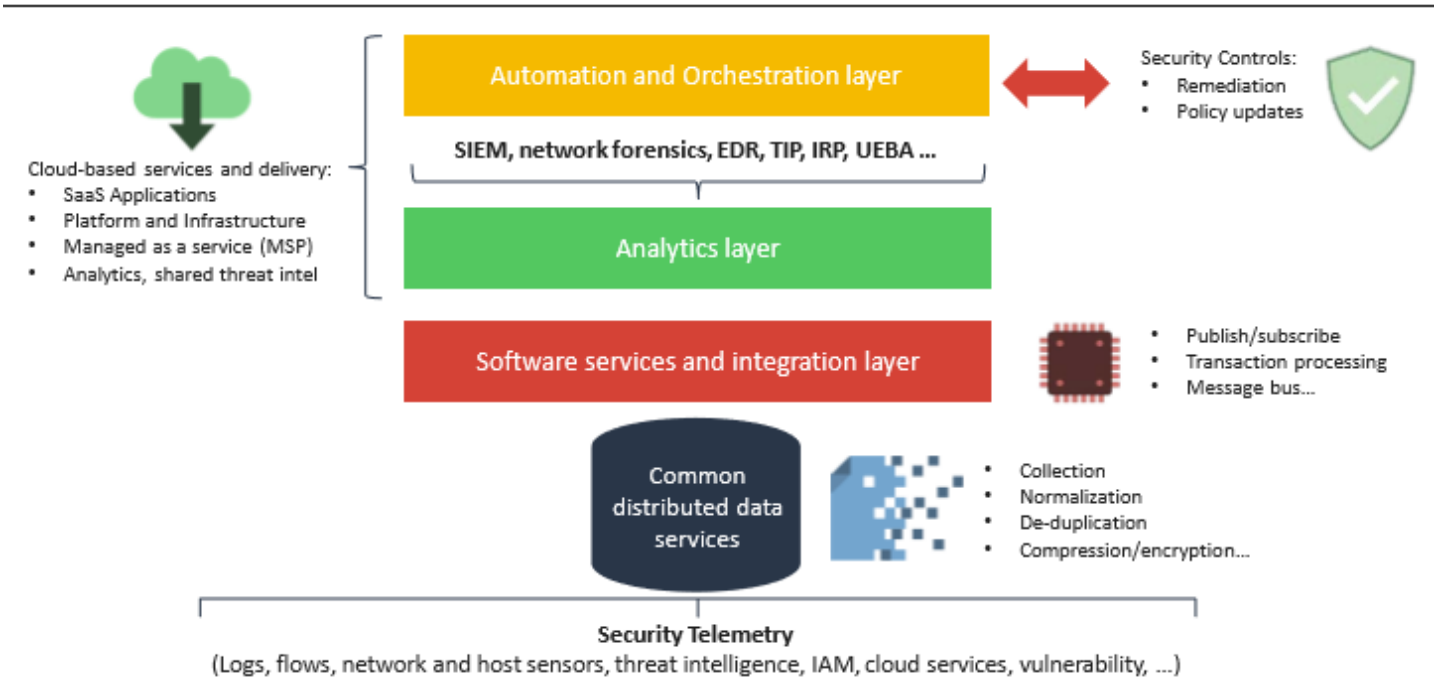
[1] Source: ESG Master Survey Results, *2018 IT Spending Intentions Survey*, December 2017.

extremely difficult to staff. ESG has been advocating that organizations deploy comprehensive visibility as part of both a security operations and analytics platform architecture (SOAPA) and a comprehensive network operations architecture to deal with the ever-changing threat landscape and expanding physical network and IT landscape. A significant part of this architectural approach is ensuring that the analytics tools have visibility to the data regardless of its location. As such, there is a requirement that the architecture provide end-to-end visibility and central management. The data can be distributed and federated as long as there is a common distributed data service to collect, process, and share it. The smarter this service is in identifying the correct data and transforming it for utilization by the target tools, the greater the impact it can have on results.

How Consolidated Visibility Helps

Organizations need to include security and network visibility as part of their digital transformation and distributed computing environments. As Figure 1 highlights for security, ESG's SOAPA concept leverages a common distributed data services layer, which is the first step in providing effective information to security (and network) tools as it collects and processes all the information from core to edge and even in the cloud.

Figure 1. SOAPA



Source: Enterprise Strategy Group

Given the risk associated with security incidents or data breach, potential blind spots, even those caused by encryption, are simply unacceptable, so organizations must have complete and comprehensive coverage over their environments. Yet, given current resource constraints, any solutions deployed need to drive greater efficiency for both staff and existing tools. The goal of a common distributed data service is to ensure that the security and network operations teams can leverage the right data to detect and respond to attacks, quickly and efficiently.

A second benefit of complete visibility across organizations' business infrastructure is the ability for them to use a single approach and data set for threat detection. With today's advanced threats, organizations need quick, consistent access to a view right across the infrastructure to be better able to spot lateral movement of threats and isolate indicators of compromise. A common distributed data services layer provides an excellent way of feeding the data store necessary to enable this.

In addition, deploying a common distributed data services layer can enable organizations to simultaneously expand visibility and reduce costs associated with buying additional security and monitoring tools for remote sites, as well as defer any additional hires to operate new security or network tools. As organizations transform and distribute their IT footprint, these common distributed data services will play a critical role in enabling a secure distributed network environment, regardless of whether they are physical or virtual.

The Bigger Truth

The IT environment is changing and becoming more complex as organizations transform to provider better digital experiences. However, it is important to realize that a better experience can't come at the expense of a data breach or hack. It will be imperative to properly plan and prepare now to ensure that any blind spots are eliminated and risk is mitigated in this increasingly distributed and dynamic environment.

Organizations need to resist the legacy mentality that would involve deploying tools and potentially resources at every location. Given the operational priorities and business initiatives, organizations have to work more efficiently and be able to respond to dramatically changing environments. IT budgets, even for security, are not unlimited, and it may be impossible to even find skilled resources to meet the demand.

To accommodate the business and enable it to be more dynamic and distributed, organizations must take an architectural approach. ESG has defined this approach as SOAPA for security, and a similar approach is required for networking. This foundational step for both is taken to ensure comprehensive visibility across data centers as well as distributed edge and cloud environments. To do this, organizations have to provide a common distributed data service that can collect, process, and distribute the right information to the right tools at the right time.