CHECKLIST

# 10 Questions To Ask Before Making a Security Investment

**The demand for ongoing digital innovation has led to the rapid expansion of network edges. The LAN, data center, WAN, and cloud environments now include the convergence of IT and OT, 5G and LTE networks, CASB, off-net workers, edge computing and distributed cloud, and most recently, the home edge. The result is an expanded and splintered perimeter that has made deploying and managing consistent security a chronic, and growing, problem. Complicating the issue further, attacks are developing new levels of sophistication, doing things like leveraging cloud compute to deliver polymorphic attack sequences at rapid scale and with full automation.**

The typical enterprise has an average of 45 security solutions deployed across its distributed environment.[1]

As organizations continue to accelerate their digital innovation initiatives, ensuring their security can keep up with both an expanding network founded on existing and new technologies and today's complex and fast-evolving threat landscape is critical. What's at stake for many organizations is their entire digital business strategy.

The challenge with rapidly expanding the network edge and the growing complexity of attack sequences that span the network is that seeing and responding to new threats requires a security infrastructure that works as a single, integrated system. However, many of the security and networking technologies needed to make things work don't work together. This creates new security and performance gaps that cyber adversaries are all too willing and able to exploit. As a result, many IT leaders are now facing a complex security environment plagued with vendor and solution sprawl, isolated and siloed security solutions, and a lack of a coherent management, orchestration, and enforcement strategy that is not only able to span their current network but also can automatically adapt as new solutions and edges are added.

Consolidation and simplification are essential components of any security strategy. This requires developing a security framework that can tie their distributed attack surface together, increasing visibility and control and enabling a coordinated and automated threat response. This also means that every new security solution needs to function as part of that overarching framework. And this needs to happen while avoiding the ripple effects a decision like this may have on their network's overall performance.

## Critical Questions To Consider Before Investing in a Security Solution

The following essential questions should be asked by IT managers when considering any new security investment. This will help support a single security platform strategy that ties essential security and networking solutions into an effective, integrated solution.

1. In addition to adding singular protections for a network segment or service, does this solution also add important point of control through a central management system to enhance overall visibility and control?
2. Is the digital innovation journey leading to the cloud? Where it makes sense, look for solutions that can be consumed consistently in various deployment models (HW, VM, X-as-a-Service, PaaS, IaaS) supporting your journey.
3. Can the solution be integrated with external systems to provide global community threat-intelligence sharing? Having the right information helps ensure an organization is not the victim of an emerging threat when it could be avoided.

4. Who is behind the various security solutions in place across the network, especially X-as-a-Service models? Does the vendor have the expertise needed to deliver a reliable security solution? Has any of it been tested and validated by third-party labs? Remember, AI and ML models are only as good as the data and patterns they are trained on.
5. Can the datasets from both traffic and security events be added and correlated effectively in a common analytics environment? Such an integrated approach is essential for effectively analyzing a full attack sequence, and not just product or location-based symptoms.
6. Can this solution effectively participate in the creation of new threat insights and an integrated prevention strategy for addressing previously unknown threats?
7. Is the prevention generated by this solution able to span the full attack life cycle by sharing information with the different security technologies and capabilities deployed across the organization?
8. Can the solution be automatically "reprogrammed" using new information from other sources? This ability for every deployed solution to participate in a coordinated threat response in a timely manner is critical because it allows an organization to break an attack sequence before it can complete its mission.
9. Has the "people aspect" been considered? What impact will this solution have on things like learning curve, policy management and orchestration, SOC and NOC processes, and the unification of visibility and span of control.
10. Change is the only constant. Does this solution allow continuous consumption of new innovations for networking, security, and operations, as well as ongoing expansion of the ecosystem, without exposing the organization to the risks of unprotected attack surfaces due to security gaps?

## It's Not About Selecting a Single Vendor. It's About Selecting the Right Vendors.

The days of simply plugging an isolated point security solution into some segment of the network to monitor traffic are long over. Today's security is a journey of optimization and mastery. Security solutions need to be able to dynamically adapt to a constantly evolving attack surface. This starts with choosing vendors ready to walk this path, enabling a fabric-based, open ecosystem, security platform designed for today's expanded and expanding networks. This must include tools that collect, correlate, and share threat intelligence, and that can participate in a unified threat response regardless of where they have been deployed or in what form factor they exist.

This integrated approach allows security teams to continually evaluate the current state of even the most dynamic infrastructure, spanning every corner and ecosystem. A unified security fabric should also provide a path for continually enhancing and strengthening security posture over time with solutions designed to work together. This enables organizations to make the most of their security investments because every element can function as part of a comprehensive and evolving strategy.

[1] Charlie Osborne, "The more cybersecurity tools an enterprise deploys, the less effective their defense is," ZDNet, June 30, 2020.

FORTINET

www.fortinet.com



March 6, 2021 4:03 AM

D:\Fortinet\2021Rebrandedtemplates\Checklist\March\AccelerateSecurityFabricandFortiOS7\cl-FA-10-questions-to-ask-before-making-a-security-investment-362021\cl-FA-10-questions-to-ask-before-making-a-security-investment-362021

919944-0-0-EN