CHECKLIST

The Rules Have Changed. What to Consider When Evaluating Cybersecurity Solutions

Organizations looking to remain competitive find themselves in a vortex of digital acceleration, continually looking for innovations they can bring to bear on the market. However, while the accelerated adoption of digital innovations can move an organization forward, the strain they put on networks may be a ticking time bomb waiting for the right cyberattack to occur.

The reason? Each innovation brings with it a new edge, whether IT, OT, LAN, WAN, or Cloud, and perhaps the most vulnerable of all, the home working edge. The result is a splintered perimeter and expanded attack surface that makes deploying and managing consistent security a chronic—and growing—problem. And what's at stake for many organizations is their entire digital business strategy.

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

Seeing and effectively responding to new threats across rapidly expanding network edges requires a security infrastructure that can operate as a single, integrated system while automatically adapting and scaling as the network evolves. However, many of the security and networking technologies currently in place that are needed to make things work don't work together. So, as the network expands, new security and performance gaps are created that cyberadversaries are all too willing and able to exploit.

What's needed is an integrated security framework that can span their current network and automatically adapt as new solutions and edges are added. But instead of seamless visibility and control across the network, many IT leaders now face 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.

While the traditional "best of breed" point product approach may have worked in the past, the rapid expansion of the network coupled with a dramatic increase in both the volume and sophistication of today's threat landscape requires something more. What's needed is a converged strategy that brings together networking and security to reduce complexity, combined with a consolidated cybersecurity platform that reduces the number of cybersecurity vendors to deliver improved incident response and enable system-wide orchestration and automation.

Critical Questions to Consider Before Investing in a Security Solution

Achieving the level of convergence and consolidation today's expanding networks require is vital. IT managers should ask the following essential questions when considering any new security investment.

☑ 1. Can the solution converge key networking and security functionalities into a single solution to reduce complexity and improve protection?

☑ 2. Is the solution a continuation of a point product approach or can it consolidate technologies to reduce the number of vendors that need to be managed?

☑ 3. Is the solution capable of working with solutions from multiple vendors through open APIs and other capabilities?

☑ 4. Can the solution be provisioned and deployed with minimal on-site intervention, sometimes referred to as zero-touch provisioning and deployment?

☑ 5. Is the solution sufficiently granular to allow organizations to expand holistically from their initial investment?

☑ 6. Can the solution encompass all potential attack vectors and edges, including those not yet deployed?

☑ 7. Is the solution supported by a single source of threat intelligence derived from its own in-house threat research as well as collaboration with key members of the cybersecurity community?

☑ 8. Does the solution support a “single pane of glass” management philosophy?

☑ 9. Does the solution offer deployment flexibility and choice between hardware appliance, virtual machine (VM), cloud, and container?

☑ 10. Does the solution extend to OT environments, enabling IT/OT convergence?

It’s Not About Products, It’s About How Best to Protect the Organization

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 integration, optimization, and mastery. Security solutions need to be able to dynamically adapt to a constantly evolving attack surface. This starts with choosing vendors able to walk this path. They must be able to do two things: They must be able to converge the network and security so protections can dynamically adapt to changes resulting from digital innovation. And they must offer a consolidated cybersecurity platform that provides a full suite of advanced protections, supports an open ecosystem using APIs and common standards, and can be deployed universally to consistently protect today’s expanding attack surface. 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. This cybersecurity platform should also provide a path for continually enhancing and strengthening security posture over time with solutions designed to work together. This approach 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.

March 9, 2022 1:42 AM
1503704-0-0-EN