The Six Fundamentals of Cybersecurity

Today's cybersecurity climate presents unprecedented challenges for organizations. Not only are sophisticated threats like ransomware surfacing at alarming frequency, but increases in mobile traffic and multi-cloud adoption confront IT teams with even greater complexities.

- By the end of 2019, there will be a ransomware attack every 14 seconds.[1]
- Wi-Fi and mobile devices will account for nearly 80% of IP traffic by 2025.[1]
- 84% of enterprises have a multi-cloud strategy.[2]
- Visibility into cloud infrastructure is the #1 control challenge facing decision makers.[3]

The Status Quo isn't Enough

These next-level challenges require next-level solutions, and legacy security approaches leave much to be desired. Traditional firewalls are great for securing the network perimeter, but what happens if a threat breaches the network? Or even worse yet, what happens when the threat comes from within your network? What's more, these perimeter-focused solutions often lack the elasticity and sophistication to protect the multi-cloud environments and mobile-first user bases seen at many enterprises today. Not to mention that as networks grow in size and complexity, more sophisticated and fast-acting incident response and remediation solutions are required.

All Signs Point to a Multi-Vendor Solution

Today's cybersecurity challenges coupled with the shortcomings of legacy solutions lead many companies to leverage multiple cybersecurity solutions from a variety of different vendors. This only makes sense given each area of your IT infrastructure presents unique security technicalities and considerations.

However, multiple vendors can lead to multiple points of vulnerability. Most cybersecurity vendors have their own validated fabric, making it difficult to integrate technologies from different vendors, leading to costly blind spots and dangerous vulnerabilities across the posture. This puts organizations in a dilemma: "Creating a multi-vendor cybersecurity posture is complex and challenging, but we have to do it anyway."

The good news is all multi-vendor cybersecurity solutions protect and secure the same fundamental components of your infrastructure. Understanding these fundamentals can help you better prioritize your needs, identify best-fit vendors and make smarter overall investments.

The Six Fundamentals of a Multi-Vendor Solution

Internet

Anytime, anywhere protection from malicious Internet destinations

Public cloud

Detect threats, achieve greater insight, and verify compliance in your public cloud infrastructure

Email

Protection against phishing, ransomware, confidentiality breaches

Hybrid / multi-cloud environments

Stop threats with next-gen firewalls virtualized for private, public and hybrid clouds. Provide secure connectivity with SD-WAN

SaaS apps and shadow IT

Visibility and control to enable highly secure cloud adoption

Data, workloads and applications

Workload and application protection via application visibility and segmentation solutions and services

---

Don’t Know Where to Start? That’s Okay.

Understanding the fundamentals puts you in prime position to create an airtight multi-vendor solution. From here, many organizations take the next step of assessing their existing posture and identifying vulnerabilities, and ConRes can help with that.

Visit ConRes.com/AssessMyIT to explore our various no-cost cybersecurity assessments.

ConRes
IT SOLUTIONS

[1]Cybersecurity Ventures

[2]Flexera, 2019. *State of the Cloud Report*.

[3]Cybersecurity Insiders, 2018. *Cloud Security Report*.

conres.com | solutions@conres.com | (888) 643-0010