ARCTIC WOLF

TechTarget | Custom Media
White Paper

How to Build Out Your Cybersecurity **Technology Stack**

When it comes to building out a cybersecurity technology stack, there are so many different vendors and categories that it can be difficult for a rapidly growing company to understand where to even start.

As organizations begin their journey toward cybersecurity maturity, there is a key set of major capabilities they should be trying to achieve.

The individual technologies themselves can vary, but an organization's aggregate cybersecurity stack needs to cover a range of risk areas in order to establish a sustainable security posture. As the organization builds out its stack, decision-makers also need to consider the role security services will play, since human expertise is critical for getting the most out of cybersecurity technology.

Here's what organizations should be seeking out, along with some ways they can get started on evaluating vendors and service providers to create a solid cybersecurity technology stack.

Five capabilities to seek out

The following five capabilities are fundamental to building out a comprehensive and effective security program. These capabilities can be achieved through a mix of both products and services, and depending on the architecture, the technology used may vary greatly by organization. The important thing to remember is these are areas that can't be ignored.

Maximized visibility

Effective cybersecurity demands maximum visibility into the IT environment. Foundational to everything is knowing what to protect, which means organizations need a thorough and up-to-date inventory of all hardware and software assets. Additionally, security teams need solid visibility into software vulnerabilities and configuration problems. This is necessary to prioritize by criticality and business importance so they can properly manage flaws based on risk.

Another key for cybersecurity is having visibility into network traffic and user behavior. That means organizations need to maintain proper logs of all device and network activity. They must also layer in some kind of capability for analyzing this data to discover and act on suspicious activity in a timely fashion.

Boundary defense

While the increasing reliance on cloud services has required organizations to reduce their reliance on perimeter protections, such boundary defenses still remain important in protecting infrastructure and assets at headquarters. Firewalls, intrusion detection and gateways all remain key parts of a well-balanced security stack. These protection mechanisms are increasingly used not just at the perimeter but within the bounds of the network as organizations increasingly mature their segmentation strategy.

Many organizations segment their network by business groups, application criticality, user groups and more. This is the heart of the zero-trust movement, which has pushed the idea of moving from flat networks toward more strict enforcement of the least-privilege rule—in other words, allowing employees to access only the systems or information they need to get their job done. No more, no less. It sounds simple in practice but requires a great deal of architectural planning and sound tactical execution to carry out elegantly.

As previously alluded to, the hybrid cloud realities of most modern IT infrastructure require that boundary defenses are built with cloud-native capabilities so that security policies can be applied consistently across both internal and external networks.

Effective cybersecurity demands maximum visibility into the IT environment. Foundational to everything is knowing what to protect, which means organizations need a thorough and up-to-date inventory of all hardware and software assets.

Access control

Boundary defense, segmentation and zero trust can never be effective without solid means of proving a user is who they say they are and that they're allowed to access the data or systems they request. This means organizations need healthy authentication and authorization mechanisms built into all of their applications and systems.

Device hardening

So many threats today manage to work their way into networks through vulnerable and poorly protected devices. This is why device hardening is so crucial for a well-balanced cybersecurity stack.

Simply, organizations need capabilities to help them securely configure devices on the network and manage vulnerabilities within them.

Threat detection and response

According to Verizon's 2019 Data Breach Investigations Report, 52% of breaches in the past year involved hacking, 33% involved social engineering and 28% involved malware.[1] Because of this, organizations need the kind of malware detection and threat activity detection that can address these problems effectively. This means building capabilities into the cybersecurity stack that provide the visibility needed to draw information from all the data elements—and to look at each of those elements in context of one another to find threats quickly.

The security-tech paradox

Technology is just one element of strong cyber-protection. The importance of human expertise combined with solid technical capabilities can't be understated. The best security makes good use of this human + machine equation.

The problem is that too many organizations fall prey to the security-tech paradox. There's a growing security skills shortage that leads to a lack of human-powered security expertise at most organizations. This hole in available talent drives some organizations to rely too heavily on a growing laundry list of shiny new security tools. But without the talent to manage those tools, they end up being a waste of money.

Building a big security team to run all those tools may be one way to achieve the automation plus brainpower necessary to maximize security investments. But that doesn't scale affordably.

Because of this, smart organizations are increasingly turning to a mix of services where the human power is built into the product itself and the human + machine element is a recurrent service the organization can pay for monthly, quarterly or annually.

[1] "2019 Data Breach Investigations Report," Verizon, May 2019

Justifying investment in security starts with understanding risk

Whether you're a security professional or IT decision-maker, keep in mind that almost all C-level executives view security as a cost center. That means they need to be presented with a fuller picture of the dynamics at play before they'll move funding up to a level that matches their risk appetite. Security buyers need to do that by performing a quantitative threat risk analysis that speaks to the language of the C-suite. This means assessing the cost and probability of incidents like ransomware attacks and breaches of personally identifiable information, and providing a C-level analysis of what ransomware and other malware will cost in today's threat environment.

One of the commonly used formulas to accomplish this is as follows:

Single Loss Expectancy = Asset Value * Exposure Factor

Using the right assessment, buyers can justify to their executives that the cost of a breach is often more than multiple years of detection and response services.

Tips for evaluating vendors and service providers

Building out and perfecting an effective cybersecurity stack isn't an overnight process. As your team evaluates components and capabilities, keep the following tips in mind:

- Use a controls framework like CIS Controls to look for gaps in the stack.
- Ask a vendor or provider how it can help you quantify risk.
- Look beyond the technology, and ensure the insights or actionability is backed by true security expertise.
- Make sure there's a way, both through automation and expertise, to glue together the information and insights from all the disparate parts of the security stack.

The experts at Arctic Wolf can help walk security and IT teams through the process of building out a cybersecurity stack. To help your organization make sound security decisions tailored to your business, Arctic Wolf staffs a dedicated Concierge Security Team that is ready to apply knowledge from the billions of security observations it analyzes every day across the company's client portfolio. Arctic Wolf's proactive risk monitoring, asset classification and vulnerability assessments provide cover for some of the major capability requirements in building a security stack. On top of that, its staff's high level of security expertise makes it perfectly placed to offer best practices recommendations for getting the most out of your stack.

To learn more, visit **arcticwolf.com**.

Arctic Wolf's proactive risk monitoring, asset classification and vulnerability assessments provide cover for some of the major capability requirements in building a security stack.