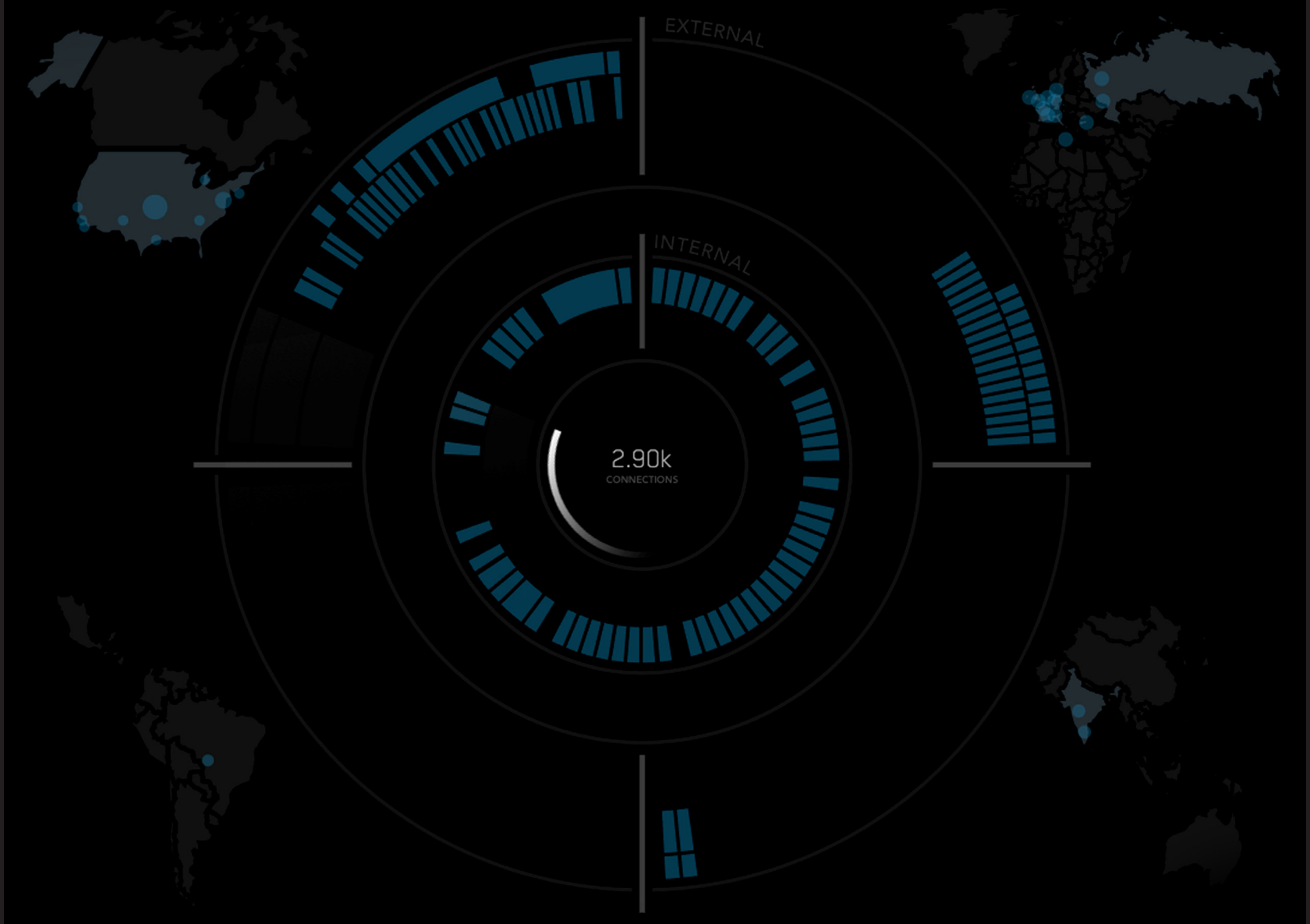
White paper

5 Considerations for Evaluating a Modern Enterprise Security Platform.



verizon

If you spend any time testing security products, you are likely bombarded with sales pitches touting "next generation" of X, "real-time prevention" of Y, or "advanced" Z. These are all good things, but security professionals are in short supply, and they are busy fighting fires caused by existing products and lack the time to evaluate new ones.

This five-point guide for security professionals looking to embark on the path of security enlightenment can help.

1 Comprehensive.

Are you excited about buying point products?

An all too common customer pain point is the lack of context associated with a partial view of a security event. You need a full picture and visibility into what's happening at the network and the endpoint and with the user and device. Be sure products you deploy provide:

- An understanding of what's happening on cloud networks not fully owned or controlled by the organization.
- Correlation of netflow, full packet and logs in a comprehensive platform to illuminate the full picture.

2 Connected.

How connected is your security architecture?

You have probably deployed many disparate products and management consoles to power your security program. It's shocking that most of these are not extensible, and prefer insularity to connectivity. Modern platforms are built with extensibility and ecosystems as a key design goal. Be aware of key indicators that you may be using the wrong product including:

- The product doesn't have APIs, or APIs are "coming in future releases."
- The product only connects to other products from the same vendor.
- The product forces you to consume your vendor's "premium" threat intelligence at the expense of discontinuing the "free" intelligence you had been using.

3 Cloud.

Are your security products built for the cloud?

A growing number of security professionals benefit from the unconstrained processing power and almost unlimited forensic windows enabled by cloud powered security platforms. Legacy security vendors are also keen observers of this shift and have started "cloud washing"[1] their legacy products. Products architected in and for the cloud are relatively uncommon but should be prioritized over legacy approaches. Be skeptical when:

- A traditional security appliance vendor says you can use their firewall or web gateway on cloud infrastructure. These products are virtual appliances of the original hardware spec and are not architected to be delivered from or in the cloud and are often minimally featured.
- Cloud–washed products don't significantly improve and automate your existing threat detection. An inherent benefit of the cloud is the ability to implement a data science approach to detection and training resulting models with billions of attributes. This approach does not work with legacy products.

1 "Cloud washing (also spelled cloudwashing) is the purposeful and sometimes deceptive attempt by a vendor torebrand an old product or service by associating the buzzword "cloud" with it." From: searchcloudstorage. techtarget.com/definition/cloud-washing

verizon

4 Continuous.

Does having hindsight into security events sound like valuable information?

According to Gartner, "adversary 'dwell time' (the time a person or group are inside an environment undetected) is still a serious problem today. Organizations are still taking a long time to find out that they have been breached."[2] Real-time detection of complex security threats is necessary but often elusive. What is needed is a new approach that takes the latest, updated threat intelligence and replays historical network traffic and packet data to discover threats that were previously missed. Organizations that are trying to detect and prevent security threats in real time should also expand their efforts to include:

- A "retrospective" approach to continuous analysis that introduces the concept of time into the security paradigm.
- Shortening adversary dwell time by using what you discover in the past to inform predictive discovery of security threats using this historical context and knowledge.

2 Gartner Magic Quadrant for Intrusion Detection & Prevention Systems,16 January 2017 by Craig Lawson, Adam Hils and Claudio Neiva

5 Coverage.

Why should security be constrained by network locations or computing platforms?

Security needs to be a flexible utility that can be deployed where and when it's needed. While it is possible to send cloud traffic through legacy security products including firewall and gateway appliance mechanisms, it often requires architecting them into the cloud at the start. Organizations should be able to

- Extend the power of security simply and easily to the cloud.
- Collect and store relevant contextual information for as long as needed and valuable.
- Conduct forensic investigations to determine whether a new zero-day vulnerability has ever impacted the business as soon as news of it breaks.

Summary

Security teams will be stretched thin. The jobs they perform will become increasingly more complex given the continued proliferation of attacks and skills required to understand what is happening amidst the lack of situational awareness that exists in most organizations. To meet these challenges, practitioners should consider the above criteria when evaluating new solutions and approaches.

Learn more

Find out more about Network Detection and Response at enterprise.verizon.com/network-detection-and-response.

verizon