Where Technology Means More®

5 Automations for Visualizing Attack Surfaces and Eliminating Vulnerabilities

By: **Marc Cohen**
ePlus Security Solutions Director

A recent survey of 300 senior executives found that **52% of their multi-cloud and 24% of their hybrid-cloud environments had suffered security breaches** in the previous year.[1] Additional research from Gartner suggests most of these failures were caused by errors introduced by customers and their understaffed IT departments.[2]

I suspect **many of these issues are related to complexity**. As networks have evolved, organizations have added ports, protocols, interfaces, applications, devices, and services. They have connected on-premise data centers to "the cloud" and then extended "the network" to encompass multiple clouds.

All these connections and assets have produced a network architecture that is incredibly fragmented and challenging to manage. **Critically, they also have made attack surfaces much bigger.**

One possible solution is to use automation to shift through the data and alerts and eliminate manual processes and repetitive tasks. But which tools and strategies? IT executives I talk to often wonder where to start. **What is reasonable, cost-effective, and supportive of operational efficiency?**

With these questions in mind, **I came up with 5 automations that, in my experience, are likely to reduce attack surfaces without straining already overburdened IT departments.** I think these are good first steps you can take to increase efficiency and security. See if you agree.

[1] Peter Suclu. "Multi-Cloud Strategy May Pose Higher Security Risk: Study." TechNewsWorld Cybersecurity. September 6, 2019.

[2] Stan Black. "The View from the Gartner Security & Risk Management Summit: Beyond Traditional Models and Vendors." Citrix.com. July 24, 2017.

1. Build a hardened base container image

While hybrid- and multi-cloud architectures improve accessibility and scalability and lower costs, their complexity makes them harder to secure. Containerization offers a huge opportunity for improving internal security by allowing you to automatically isolate applications and services and put measures into place for monitoring east-west traffic activity.

Containers are lightweight logical instances. They run on abstracted layers on top of the host operating system and represent an application or a service or just selected microservice functions.

With containers, it is possible to create visibility at every logical point in the network, such as at any point where two containers interact. You can virtually isolate different workloads and make it harder for hackers to spread attacks without detection.

Container orchestration and security systems allow you to create a base image and then harden it to mitigate intrusion. This hardened "golden" image then becomes the template for containerizing all high-value applications or services. Putting these controls in place reduces your attack surface and makes your infrastructure easier to manage.

You can create automated processes (see IaC in the next suggestion) that make it easy to copy the golden image and launch new environments whenever development, testing, or production has a need for resources. This on-demand approach also reduces the networks attack surface by helping to keep container lifecycles short.

2. Adopt an infrastructure as code strategy

Infrastructure as code (IaC) provides a framework for configuring and managing hardware, software, and containers in hybrid- and multi-cloud environments. Machine-readable rules, scripts, and processes and standard software development versioning techniques take advantage of the API-driven nature of cloud services.

IaC provides an alternative to copying example configurations and code snippets, which tend to be written without much consideration for security. It enforces consistency and helps eliminate the errors that sometimes occurs when applications and services are manually set-up and deployed.

IaC makes it easy to create a code repository of scripts describing each component's ideal state. Along with reducing the attack surface, these improvements standardize operational procedures and eliminate repetitive tasks.

While there is a learning curve to IaC, it builds long-term efficiency by making it easier to launch storage systems, network infrastructure, databases, and services. Since provisioning is based on a proven method, these processes can be completed without manual oversight. Mandating these measures reduces risk further by providing a framework for logging east-west data, reporting anomalies, and controlling access.

3. Use probability scanning to detect abnormal behavior in east-west traffic

Most multi- and hybrid-cloud traffic moves in an east-west between servers and applications inside the network firewall. Traditional monitoring cannot track this internal traffic and that lack of visibility contributes to making the attack surface much larger.

Probability scanning is an emerging technique that uses special algorithms to automatically monitor the behavior of nodes and servers in the network environment. It builds a model of normal activity and learns to identify the assets that are most likely to be targeted for attack.

Probability scanning creates visibility into east-west traffic and the attack surface. With appropriate analytics, you can monitor containers or other internal network segments and respond to threats before assets are compromised. This visibility provides a way to protect core infrastructure, which is vulnerable to stealthy attacks that can go undetected until traffic begins to cross the perimeter firewall.

Because hackers are using increasingly sophisticated methods to disguise their activities, security teams need more efficient ways to identify suspicious traffic. Probability scanning provides another tool for monitoring these workloads even as networks continue to scale up and increase in complexity.

4. Tag network assets to improve visibility

As noted previously, many modern environments contain thousands of assets. Managing, monitoring, and controlling these components is easier when assets are tagged.

An asset management system gives you a real-time view of all your on-premise and cloud-based assets. This inventory provides continuous updates on the state of your attack surface and allows security staff to focus their time on fixing misconfigurations or removing abandoned assets.

Plus, an asset management system can enhance east-west visibility without the need for additional instruments at the network perimeter. With tags, it can assign unique information, instructions, policies, and compliance controls to individual assets. It can detect unknown assets or out-of-policy services and issues alerts to expedite remedial action. These functions are particularly useful for networks that connect with shadow infrastructure, supply chains, and other business partners.

This type of solution also generates data and logs for meeting auditing and compliance requirements. That information helps you implement further controls for mitigating risk and reducing the attack surface.

5. Implement global orchestration to enforce policy compliance

Thousands of network assets also mean thousands of embedded policy rules. To keep those rules current, the Computer Security Alliance recommends a continuous governance, including as it relates to compliance, auditing, and assurance.

But trying to do continuous governance manually is an impossible undertaking. The only realistic option for any modern environment is to rely on automation. Reasonable measures would include compliance automation workflows and reporting tools to manage and track risk assessments, audit automation to collect configuration data for independent assessment, and assurance automation to ensure that all segments of the infrastructure are able to deliver services securely.

Putting these measures in place better positions an organization to identify threats and mitigate risks. And it becomes easier to create usage policies and scripts for enforcing safe choices, managing resource consumption, and controlling the ability of users to change infrastructure or provision new systems or assets.

5. Implement global orchestration to enforce policy compliance

Tools, such as an attack surface visualization system, can visualize the attack surface and correlate detected vulnerabilities with known exposures. It is also possible they can be configured to run automatically and detect and prioritize threats as they emerge.

With more data, you are better positioned to categorize vulnerabilities in groups of assets, such as out-of-date policies or misconfigured rules. For automation to work, however, organizations have to make sure policies are enforced consistently for each type of asset. An asset might have GDPR compliance requirements, for example. If it resides on a third-party cloud, the organization might want to use its software controls to keep that workload isolated to a specific micro-segment or container.

You can roll out these improvements relatively quickly and without disrupting critical processes. Even if the end result is not quite perfect, your infrastructure will be less attractive to cybercriminals when other networks are much easier to access.