How the Atomized Network Changed Enterprise Protection

Cyberattacks rose at a rate of 42% in the first half of 2022 and the average cost of a data breach has hit a record high of $4.35 million with costs in the U.S. peaking at $9.44 million. Unfortunately, this shouldn't come as a surprise. Enterprise networks have changed dramatically, particularly over the last few years, and yet we continue to try to defend them with the same conventional approaches. As an industry, we've hit an inflection point. It's time to fundamentally rethink the problem set and our approach to solving it.

Networks are dispersed, ephemeral, encrypted, and diverse
Our networks have become **atomized** which, for starters, means they're highly dispersed. Not just in terms of the infrastructure – legacy, on-premises, hybrid, multi-cloud, and edge. The capabilities, the nomenclature, and the available data for each type of infrastructure are also dispersed.

The cloud has changed the game quite a bit, making today's networks very ephemeral. Everybody is remote and IP addresses come and go. We're no longer just talking about dynamic host configuration protocol (DHCP). In the cloud, every time we reboot a cloud instance that instance can get a new IP address. Conventions like Canonical Name (CNAME) do that mapping behind the scenes for us. However, it's incredibly difficult to stay on top of what we have, what it's doing, and what's happening to it, when what something is today may not necessarily be what it was yesterday, and teams have limited visibility and understanding of these changes.

Compliance is adding a lot of complexity to security as practices like encryption come into play. When we talk about

protecting sensitive data, we're talking about encrypting potentially all connections and endpoints and, depending on our infrastructure, managing thousands of certificates. So, atomized networks are also encrypted which is not only difficult to manage but introduces more costs and concerns. Additional capabilities for decrypting are required. And the more we decrypt, the more likely sensitive data is at risk. So, we need to try to minimize decryption as much as possible without sacrificing network visibility and control.

Finally, atomized networks are extremely diverse. The temptation with security teams has always been to add a tool that is very specific to the environment that we are watching – tools for the network, for devices, for the web, for email. This was manageable when we were talking about one corporate network or even a handful of networks. But with the addition of new cloud environments, operational technology (OT) environments, and work from home models, we've hit an inflection point where the number of tools that are supposed to make us more secure and make security teams' lives easier actually do neither. Security operations center (SOC), cloud operations, and network teams can only watch and do so many things, so we end up with bloat. In fact, nearly 60% of organizations surveyed say they deploy more than 30 tools and technologies for security and yet incident volume and severity keep rising.

Fragmentation and gaps are rampant

We try to get diverse teams and tools to work together by creating yet other sets of tools, like SIEMs and SOAR platforms that are meant to try to aggregate data and automate analysis and actions. But those tools have their own sets of challenges and require that we add more tools and technologies to our security stack in order to maintain protections.

Security has become so complex that organizations can't possibly hire enough people with the right skills to do

everything required to secure their atomized network. What's more, every tool in the growing security stack serves its own purpose and every team has their own area of focus, with not enough overlap between them. Users move between multiple panes of glass and multiple environments, using tools with different capabilities, which inevitably leaves gaps that are unwatched or not effectively watched. Attackers live in those gaps. No wonder organizations say the top three reasons why cyber resilience hasn't improved are the inability to reduce silos and turf issues, fragmented IT and security infrastructure, and lack of visibility into all applications and data assets.

Rethinking and simplifying enterprise protection

The challenge with letting go of old technologies and methods is that humans are naturally resistant to change because it's disruptive. New expertise, new processes, and new escalation procedures are needed. However, network atomization is even more disruptive, and the time has come to cast aside aging security approaches. Securing atomized networks requires a fundamental rethink. Not a "bolt-on", tacking on a new capability to a legacy toolset and hoping it integrates and solves our problem. It doesn't solve the problem. It makes it worse.

When we are no longer tied to how things used to be, then we can rearchitect the problem from scratch for the way things are today and how they will evolve. We can get to where we need to be – a common tool set, with a common language, and a common set of capabilities that can deal with the dispersed and ephemeral nature of today's networks, doesn't have to decrypt, and can actually help security teams work more efficiently and effectively.

In my next column, I'll take a closer look at the gaps network atomization and conventional tools are creating, and how to close them.

How the Atomized Network Changed Enterprise Protection