Zero Trust Architecture:
Only One Side of a Multi-Faceted Cybersecurity Approach

By Joseph Norton and Jun Yu

Since the SolarWinds attack in 2020, private companies and government agencies have generally agreed that implementing a Zero Trust Architecture is the best approach to combat future cyber-attacks. But how does it work in the real world?

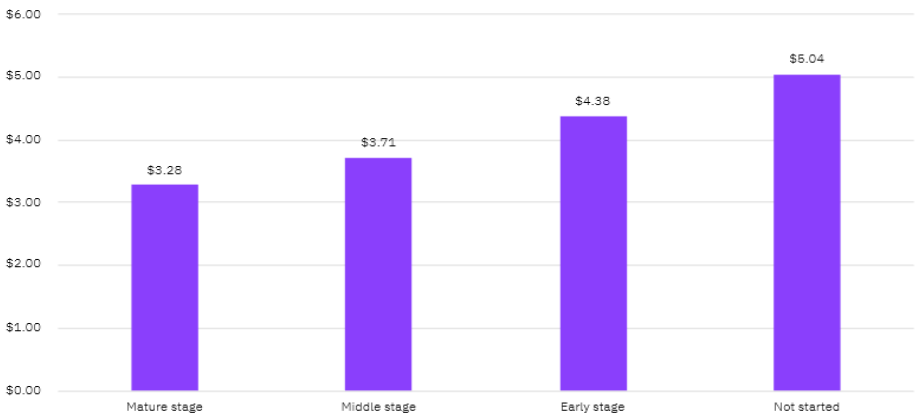
In the 2021 edition of its "Cost of a Data Breach Report," IBM included the impact of Zero Trust implementation for the first time. Thirty-five percent of reporting companies said that they had either fully or partially initiated Zero Trust programs. Significantly, those firms experienced reductions of expenses related to data breaches of up to forty-two percent when compared to companies that had eschewed Zero Trust efforts.

As impressive as that cost reduction might be, companies with mutual Zero Trust implementations still lost an average of $3.2 million, as a result of what might be considered a "run of the mill" data breach. This could be classified as a very disappointing result for a cybersecurity architecture that carries very high hopes as the solution to prevent the next SolarWinds attack, which has been dubbed as the "most sophisticated cyber-attack ever" and believed to be carried out by Russian intelligence services.

Figure 18

Average total cost of a breach by the state of zero trust deployment

Measured in US$ millions



Source: "Cost of a Data Breach Report – 2021" – IBM

Zero Trust is **originally described and published in 2010 by Forrester Research and** designed to respond to a sobering new reality in cyber space. The proliferation of mobile devices, the quickly expanding Internet of Things (IoT), and remote working arrangements have obliterated enterprise network perimeters and have made the prevailing perimeter defense strategy – keep the bad guys out – demonstrably less effective.

The difference? The National Security Agency (NSA) believes that Zero Trust should embrace the concept of an "assumed breached" and build protections for critical assets with the assumption that the network has already been breached. But Zero Trust implementation in cyberspace is still in its early stages. The National Institute of Standards and Technology (NIST) started drafting its Zero Trust Architecture (SP 800-270) in 2018 and it was finalized in August 2021. It is the most comprehensive Zero Trust Architecture guide today.

NIST's version of Zero Trust "is not a single architecture but a set of guiding principles for workflow, system design and operations that can be used to improve the security posture of any classification or sensitivity level," and building the architecture "is a journey concerning how an organization evaluates risk in its mission and cannot simply be accomplished with a wholesale replacement of technology."

Just how complicated might it be to implement a Zero Trust Architecture that aligns with NIST SP 800-270? The National Cybersecurity Center of Excellence (NCCOE) recently collaborated with 24 software and cloud providers to build a SP 800-270 reference site. Integrating all of these components would be a tremendous task for any company, let alone taking into consideration the ongoing patches and upgrades. But wait – companies go through all that and still lose millions of dollars' worth of data to a cyber-attack? Something has to change!

In fact, SP 800-270 is a network-centric security management approach that relies heavily on access control of **user identities,** devices, services, and applications, and not at all on protecting the unstructured data or files. It assumes that if access to a device is protected, so are the files stored on that device. But if we apply the "assumed breach" mindset and assume the attacker obtained a valid user credential, the attacker will be able to access the device after the stolen credential is successfully verified and can then exfiltrate all the files on the device. This is not to say that access control is useless; rather, it simply reiterates that device access control depends on the absolute security of user credentials, which is a very tall order in a network that is assumedly breached.

Realizing the lack of ability to protect data after the SolarWinds attack, the Department of Defense published the "Department of Defense Zero Trust Reference Architecture", in which it declared "The Department of Defense (DOD) next generation cybersecurity architecture will become data centric and based upon Zero Trust principles." NSA echoes the same sentiment in its publication "Embracing a Zero Trust Security Model," asserting that in a "data-centric security model," Zero Trust should "focus specifically on protecting critical assets (data) in real-time within a dynamic threat environment." The Cybersecurity and Infrastructure Security Agency (CISA), the federal agency that oversees the federal government's cybersecurity activities, combined both network-centric and data-centric approaches in the "Zero Trust Maturity Model," the CISA document designed to guide federal agencies' migration to Zero Trust. The data pillar of that model, one of the five pillars that aligns with data-centric management, requires the encryption of "all agency data" at all times.

For companies and government agencies that are on the path to Zero Trust, data-centric management is the key to preventing data breaches that are profitable for intruders. How can data-centric management protect data in a way that network-centric approaches cannot? First of all, data are encrypted persistently and seamlessly in a data-centric management model. Secondly, every time a user needs to access data, s/he must be authenticated using dynamic data access policies and only then will the data be decrypted for the user to access.

Let's assume that the network has already been breached and a valid user credential is stolen by the attacker. The attacker wants to exfiltrate the files; in a network-centric Zero Trust environment, the attacker could use the stolen credential to make one request to access a device or cloud container and steal the 1000 files stored on it. The cloud data encryption would not stop the breach because the files were retrieved by an authenticated user.

On the other hand, with a data-centric solution in place, the attacker would have to use the stolen credential to make 1000 requests to access the encrypted data, one for each file. The access control process would detect the excessive number of requests from the user that would be a departure from the usual pattern, and an alert would simultaneously be issued while the user's access request is denied. In this case, only a tiny number of files could potentially be breached. Since the attacker doesn't know the content of each encrypted file before the request to access is granted, s/he cannot select the files to exfiltrate first, minimizing the chances of losing critical data. Implementing more advanced measures including classified data access control can further reduce or eliminate the chance of a data breach.

If Zero Trust is to become the preferred approach to effective cyber defense efforts, it is essential that Zero Trust Architectures are paired with a data-centric management solution that is laser-focused on the protection of critical data around the clock and around the globe. Otherwise, Zero Trust will become just another overused but underwhelming buzz term in the cyber-speak metaverse.