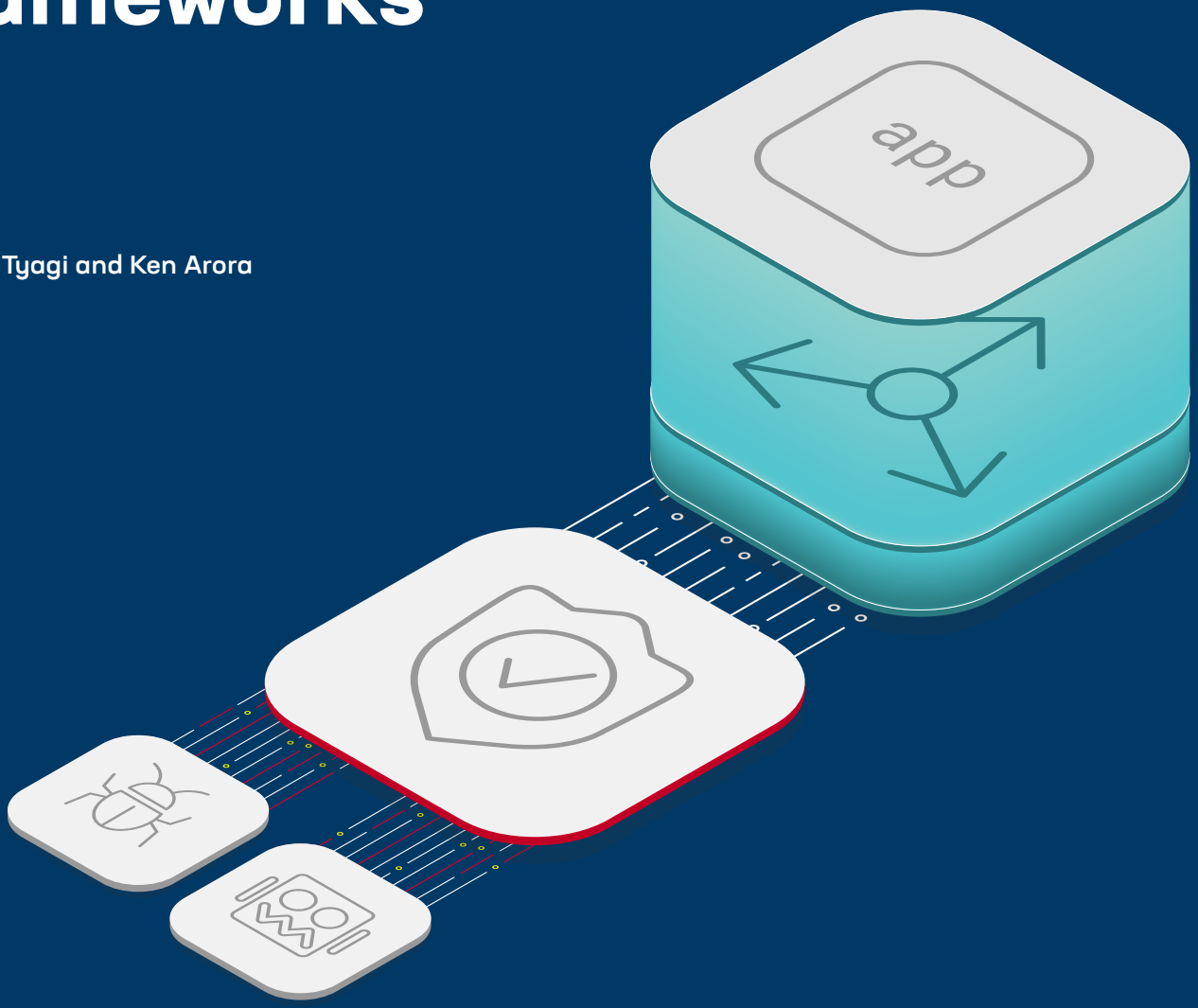
Benefits of Zero Trust Adoption Through the Lens of MITRE ATT&CK and D3FEND Frameworks

By: Mudit Tyagi and Ken Arora



Cyberattackers operate by scanning their target organizations' networks and applications—their *digital attack surface*—to craft multi-step attacks using multiple techniques and procedures that exploit discovered and zero-day vulnerabilities. In this paper, we consider several classes of threats that enterprises must defend against and highlight the use of zero trust principles to increase the chances of containing damage from adversaries' activities. We then take a brief look at attackers' tactics, techniques, and procedures, which are codified in the MITRE ATT&CK framework. Finally, we discuss the MITRE D3FEND framework and map it to zero trust principles.

What is the Attack Surface?

In its Computer Security Resource Center (CSRC) glossary, the National Institute of Standards and Technology (NIST) offers an abstract definition of "attack surface" as "the set of points on the boundary of a system, a system element, or an environment where an attacker can try to enter, cause an effect on, or extract data from, that system, system element, or environment."

Another way to think of "attack surface" is to consider all known and unknown vulnerabilities that lurk on various components of the digital environment. A non-exhaustive list of such components would include:

- Physical and virtual network, compute, and storage assets
- Hypervisors, virtual machines, container orchestration systems, service meshes
- Software that runs on these assets, such as firmware, operating systems, database management software, application software
- Container image repositories, VM image repositories, code repositories
- Internal and external APIs, microservice endpoints, application portals
- Services external to the local environment, but consumed locally, such as identity validation services, time servers, and remote data storage
- Identity stores, user account databases, business data stores

Understanding Threat Classes

To minimize risk to business, organizations must defend their own digital assets and intellectual property as well as the privacy of their customers and employees, while also conforming to all regulatory compliance requirements. They must do so while simultaneously ensuring that business workflows and digital experiences continue to be available and reliable. The solution to this challenge is to adhere to zero trust principles: use least privilege, explicitly verify, continuously assess, and assume breach.[1] By doing so, organizations can address a number of different threat classes, as discussed in the following sections.

DATA THREATS

Data is the life blood of modern digital enterprises; therefore, attackers have strong financial motivations for going after an organization's data. Once stolen, the data can be sold in the dark web and used by other parties to carry out further harm to the data owner. An organization can also fall prey to ransomware, where attackers make the organization's data unavailable, either by encrypting the data in place or removing it entirely from the organization's infrastructure. The attackers can then demand payment—a "ransom"—from the victim in exchange for restoring the data. A third class of data attack, used by actors who simply wish to do harm, is to subtly corrupt the data, thereby disrupting business processes and the digital experiences that depend on it.

Leakage

Data leakage, or data breach, occurs when an adversary gains access to confidential information without the consent of the owner. In addition to the intellectual property impact, these attacks often cause brand damage and loss of trust. The law requires breached organizations to report any data loss that contains personally identifiable information. Phishing techniques, exploiting vulnerabilities in public facing applications, and using supply-chain compromise are all popular methods for infiltrating the digital environment where data is stored.

A notable recent example is the SolarWinds supply chain attack,[2] which adversaries used to penetrate thousands of corporations and government organizations. This initial access provided a springboard for subsequent attack exploitation steps by establishing a persistent presence in the digital infrastructure, thus enabling lateral movement across multiple victim applications and networks. Ultimately, these tactics led to the attacker's end goals—to compromise credentials/passwords and exfiltrate the victim's data.

[1] https://www.f5.com/services/resources/white-papers/why-zero-trust-matters-for-more-than-just-access
[2] https://en.wikipedia.org/wiki/2020_United_States_federal_government_data_breach

Ransomware

Another form of attack against data is “ransomware” attacks, in which hackers deploy malware to either disrupt or entirely block key business processes. Most commonly, crucial business data is encrypted or removed, thus disrupting critical workflows. In some cases, data in the identity authentication data store is also encrypted or removed, effectively locking legitimate users out of the system entirely. Only upon receipt of the “ransom” do the attackers restore access to the system or decrypt the data. In May 2021, a ransomware attack crippled Colonial Pipeline,[3] which carries gasoline and jet fuel to the southeastern United States.

Silent Data Corruption

Some adversaries use a more nuanced approach in their data attacks. Rather than exfiltrate the data or make it unavailable, these sophisticated attackers make a small number of carefully targeted changes to the in-situ data of the victim organization—with the payoff being delivered through the application’s normal externally facing workflows. Examples include increasing the fraction of airline seats that are to be sold at a discount, manipulating an inventory supply database to make it appear that more or fewer items are for sale, or adding a special discount code on an e-tail site. These “stealth” changes, which are often hard to detect until the damage is done, take advantage of the victim’s own business workflows to extract value for the attacker.

INFRASTRUCTURE RESOURCE THREATS

Hackers launch attacks that consume resources in the network and compute infrastructure such that business processes come to a standstill or function inefficiently. The goals of such attacks vary from damaging the target organization’s brand to extorting payment to achieving a specific business outcome, such as making online ticket sales unavailable. Additionally, advanced attackers often use this type of attack as a smoke screen while carrying out other steps of a simultaneous, more sophisticated attack.

DDoS

Attackers use botnets to direct attack traffic toward the target’s resources to launch distributed denial of service (DDoS) attacks. Volumetric DDoS attacks flood the target’s network with traffic, consuming all available bandwidth. Protocol DDoS attacks send specialized traffic to fill up connection tables on stateful networking devices—such as firewalls—so that legitimate connections are dropped. Application DDoS attacks consume resources on the servers with illegitimate requests.

[3] https://en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack

CPU Stealing

Attackers can gain unauthorized access to compute resources to perform computations on behalf of the attacker, the results of which are reported back to a command-and-control server. This is most often done to run crypto-mining code in the background, unbeknownst to the owner of the computer. Phishing and drive-by downloads are typical methods used to deploy crypto-mining code on computers. Hackers use the MITRE ATT&CK lateral movement tactic to grow their stolen CPU capacity and persistence tactic to sustain their ability to run unauthorized computations.

BUSINESS THREATS

Actors with malicious intent cause harm to organizations by abusing a desired workflow or user experience. These threats can lead to revenue loss, a tarnished brand, and higher operational costs for dealing with fraud.

Business Resource Exhaustion

Hackers, motivated by personal profit, use legitimate business processes to harm organizations. For example, they may use automation to purchase a substantial number of tickets for a popular event, making it impossible for others to buy, and then sell them at a higher price.

Business Intelligence

Business information can be scraped from an organization's public website or stolen from internal systems, and then used in ways that are detrimental to the organization. As an example, a competitor may scrape price information and lower their own prices to lure customers away.

Brand Attacks

Hackers can modify the content of a public facing website and deface it to embarrass an organization. They can also alter the content to deliver incorrect information to website users.

Commerce Fraud

Fraudsters find ways to commit financial transactions on behalf of other users so that they benefit from the transactions. They use stolen credentials to take over an account or trick unsuspecting users into going to a site that looks like one they normally use and give up their account credentials. This kind of fraud is typically done on ecommerce sites or financial institution portals. During the COVID era, many fraudsters engaged in unemployment fraud, where they filed fraudulent unemployment claims using stolen identities and directed the benefits to themselves.[4]

[4] https://www.f5.com/company/blog/unemployment-fraud-covid-19

MITRE ATT&CK Framework

A persistent adversary who launches a threat against an organization is patient, organized, and highly skilled. To cause harm, the attacker must achieve several tactical goals, such as gathering intelligence, gaining initial access, establishing a beachhead, stealing information, exfiltrating data, and more. The MITRE ATT&CK framework[5] lists tactical goals, techniques to achieve the tactical goals, and procedures to implement those techniques. Defenders can use this framework to dissect any attack into its set of tactics, techniques, and procedures (TTPs), which can be found on the MITRE ATT&CK framework site. We note that for each tactic and its associated techniques, adhering to principles of zero trust across the digital environment reduces the probability of the attacker's success and increases the probability of early detection of their activity, as represented in Figure 1.

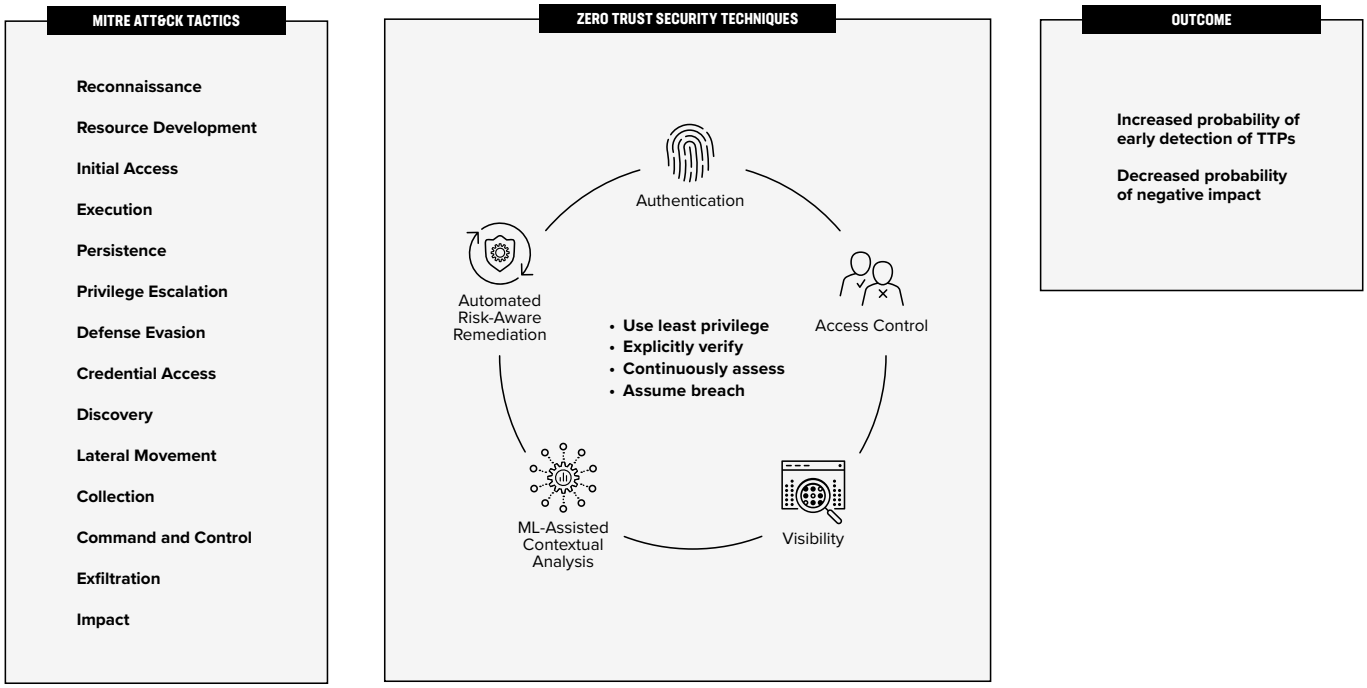


Figure 1: Zero trust security techniques based on zero trust principles thwart TTPs[6]

[5] https://attack.mitre.org/matrices/enterprise/
[6] https://attack.mitre.org/tactics/enterprise/

MITRE D3FEND Framework follows Zero Trust Principles

The D3FEND framework offers a countermeasures knowledge base and knowledge graph that "contains semantically rigorous types and relations that define both the key concepts in the cybersecurity countermeasure domain and the relations necessary to link those concepts to each other."[7] This framework helps security practitioners consider what capabilities are needed to defend against threats relevant to their digital environment.

Further, it is possible to think of security risk in terms of preparedness against the various TTPs enumerated in the MITRE ATT&CK framework by taking stock of the ability to execute relevant countermeasures listed in the D3FEND framework. The connective tissue between the two frameworks is the "digital artifact" abstraction. When attackers employ a set of TTPs to conduct their attack, their activity produces observable digital artifacts. The D3FEND framework helps practitioners specifically note how to look for digital artifacts produced by the adversary's activity and helps to build an actionable defensive plan.

We note that categories of MITRE D3FEND countermeasures neatly map to zero trust security techniques based on the zero trust principles as seen in Figure 2.

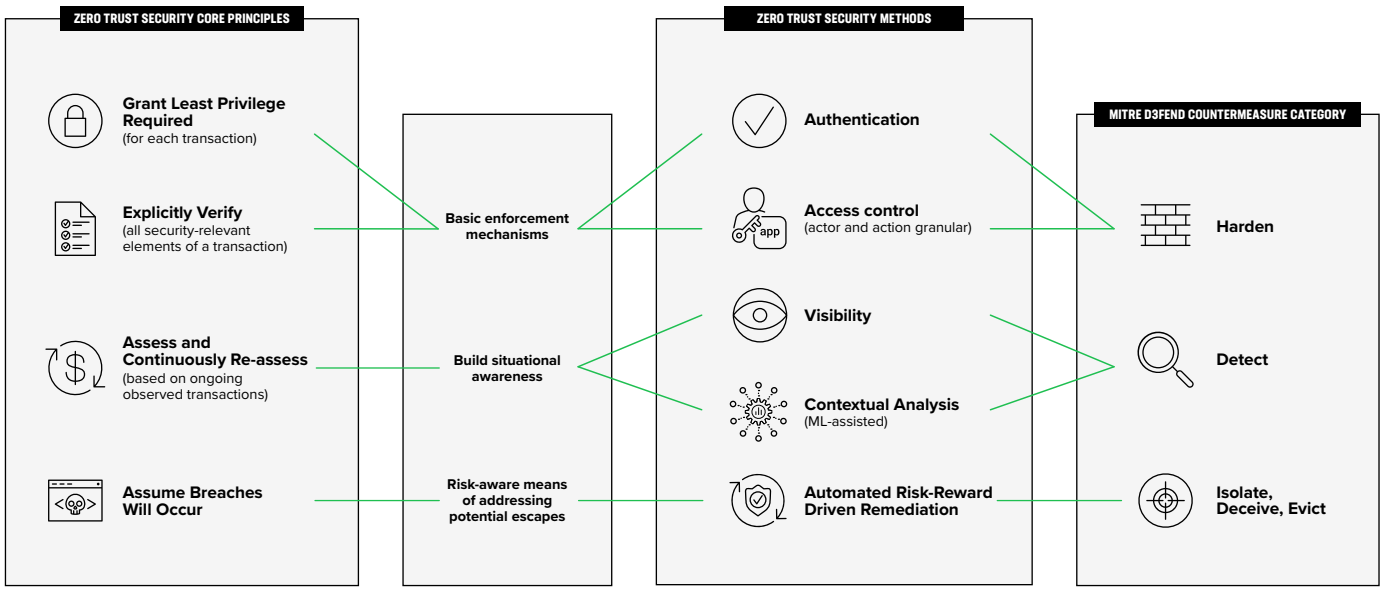


Figure 2: Mapping between zero trust security techniques and MITRE D3FEND countermeasure categories

[7] https://d3fend.mitre.org/about

Conclusion

Today's applications and digital experiences are being driven by the business desire for richer engagement across a wider variety of target customers, including both human and smart devices, in the broader context of an ecosystem of interconnected digital enterprises catering to an increasing mobile workforce and customer base. Simultaneously, the requirement for ever-increasing business agility and efficiency has caused application architectures to leverage open-source and SaaS components to a much greater degree. Consequently, the core application today is dependent on a deeper and less controlled infrastructure than ever before. Modern business requirements have driven increased application architecture complexity, resulting in the exposure of a broader and more dynamic threat surface, which is being exploited by sophisticated adversaries that are better funded and more motivated than ever before.

The MITRE ATT&CK framework offers an organized nomenclature for tactics, techniques, and procedures that bad actors use to compose complex attacks. The MITRE D3FEND framework specifies a knowledge graph of countermeasures that organizations can use to detect observable digital artifacts produced by the TTPs used in an attack. MITRE D3FEND countermeasures can be associated with various principles of zero trust, and adherence to these principles makes the specific mechanism of implementing the countermeasure more effective.

DC 08.2022 | RPRT-OCTO-934308834