ZERO TRUST CAN IMPROVE YOUR SECURITY POSTURE

So how do you implement it?

Zero Trust is on a lot of peoples' minds these days. You might be tempted to think it's just a buzz phrase, but at the core is a really important concept that can help your defensive posture where data is concerned: assume that your IT environment is already compromised and apply a healthy level of mistrust to any user or device attempting to access data or services.

Zero Trust isn't really an industry standard, but it is the following:

The US Department of Defense (US DoD) points out that Zero Trust is a **philosophical** shift in the way that we secure our IT resources and data environment.

Zero Trust is not a codified industry standard but rather a **framework** that has been captured in reference architectures (such as the US DoD) and other explanatory documents (NIST, analyst papers).

Businesses are driven to consider and implement a Zero Trust approach to cybersecurity because of a number of factors, including increased user **mobility**, distributed **remote work forces, cloud architectures**, and legacy **perimeter security tools** that are easy for threat actors to attack and overcome.

> *A ZT APPROACH IS PRIMARILY FOCUSED ON DATA AND SERVICE PROTECTION*
>
> *US NIST SP 800-207*

HAVE YOU CONSIDERED THESE POINTS?

Understanding these facts is the first part of your Zero Trust journey.

Border and perimeter security isn't enough
Many enterprises still rely heavily on protecting the borders and perimeters around their IT environment. The thought is that keeping threat actors and hackers on the other side of your virtual wall ultimately keeps your environment and resources safe. That's simply **not true**.

Assume you're already sustaining a breach
This is one of the prime tenets of Zero Trust. It hits at the detrimental outcome of complacency and a false sense of security, which encourages lax protections and plenty of weaknesses for threat actors to exploit.

Zero Trust is comprehensive
Zero Trust is many things. Implementing it affects everything from your corporate culture to your network, the devices and resources connected to your network, and the users who depend on this entire infrastructure to get work done. No platform can provide you with total coverage of Zero Trust protection across all these different aspects of the IT infrastructure.

You can't implement everything at once
Because Zero Trust affects so many different parts of the infrastructure, often referred to as "pillars" of Zero Trust, you have to decide where to start your Zero Trust journey. Different vendors suggest different stepping off points, which usually centers on their offers. Let's walk through the reasons we feel that data security is an ideal starting point.

> *"CYBERSECURITY ARCHITECTURE WILL BECOME DATA-CENTRIC"*
>
> *US DEPARTMENT OF DEFENSE REFERENCE ARCHITECTURE*

WHAT IF YOU COULD?

This isn't wishful thinking—you can actually achieve these accomplishments very quickly, all while adopting a Zero Trust approach to cybersecurity:

Protect private and sensitive information even if it falls into the wrong hands.

Implement data security that greatly exceeds regulatory demands.

Work with sensitive data without having to de-protect or compromise that information.

WHAT THREAT ACTORS AND HACKERS WANT

Have you ever considered what these bad actors really want when they carry out attacks on your business? They're actually targeting very specific things, but sometimes we confuse what they're after with the stepping stones they use to get to their ultimate goal.

In testimony before a US Congressional subcommittee in 2018 about terrorism and illicit finance, participants explained very clearly what hackers really want. Their goals inevitably are to:

Breach defenses to get into a data environment, leveraging stepping stones such as the network and other IT resources along the way.

Steal highly valuable data, whether that data may be peoples' sensitive PII or the company's IP.

Leverage, monetize, and potentially even weaponize stolen information for financial gain and to assist in further compromising people and businesses.

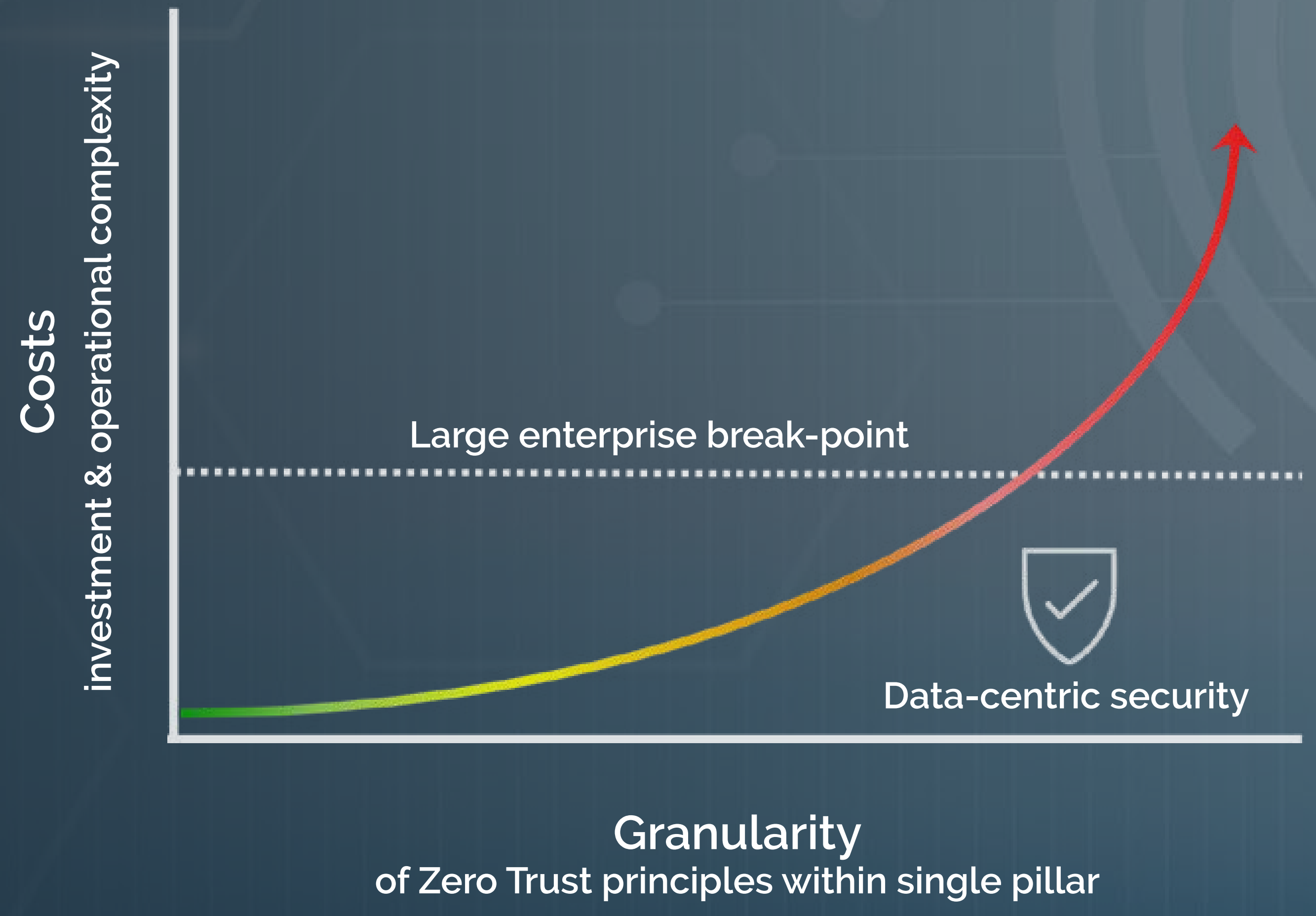
As the US NIST agency explains in their special publication about Zero Trust (SP 800-207), a main focus of Zero Trust is the protection of data and the IT services that house that data.

> *DATA IS THE TARGET OF ALL THREAT ACTORS*

HOW ZERO TRUST & DATA-CENTRIC SECURITY MAKE A DIFFERENCE

Zero Trust forces you to rethink cybersecurity so that ultimately your data and resources are better protected. Data-centric security methods such as tokenization are the best way to protect data. It is highly granular (you can protect down to a specific data element), easier to implement (turning months of implementation time into days or weeks), and ultimately more cost effective.

We've helped customers cut their expenditures significantly while achieving a stronger and more granular level of data security simply by starting with data protection. Costs can go up precipitously when trying to achieve ZT with strategies like micro-segmentation of the network across very large enterprises. Costs for data-centric security don't follow that exponential curve. The following illustration shows the cost-to-benefit reality of data-centric security.



CYBERSECURITY IS AS MUCH A BUSINESS DECISION AS IT IS A TECHNICAL ONE.

HERE'S WHAT YOU NEED TO KNOW ABOUT ZERO TRUST

You might be asking yourself, do I really need to figure out yet another cybersecurity methodology to implement? The short answer is yes, you do. All you need to do is look at the growing number of cyberattacks, especially the ones hitting major enterprises and supply chains in order to cause major chaos and disruption, to realize that current defensive strategies aren't enough. This is the reason that understanding Zero Trust—and implementing some or all of the recommended guidelines—might be the difference between an incident and a full-on heavily publicized breach.

Aspects of Zero Trust

Remember, Zero Trust is not a standard, so no governing body has determined a "right" way to implement it. Many organizations, however, have published papers and guidelines on the subject. As mentioned previously, the US DoD and US NIST have both issued publications on the topic, and these reference documents are great for background information on and implementation details for your Zero Trust initiative. Here's how they both define Zero Trust:

- The acceptance of the fact that breaches cannot be prevented 100% of the time, so assume that you have been breached or that an attack is underway.
- This acceptance should change your defensive posture dramatically toward skepticism about any user or device trying to access information or a service. Have zero trust (ah, there's where the name comes from) in any request, 100% of the time.
- Extend no trust simply based on location within your IT environment—just because a laptop is on your internal network doesn't mean it should inherently have any access to any information, data, or service.
- Buying into the first two points, you should then continually assess all transactions and requests for information, data, and services within your IT and data environments.
- Subsequently, restrict access to explicitly expressed and proven need for that information, data, or service.
- When you grant access after successful challenge, provide the bare minimum privilege and re-challenge when more privilege is requested.

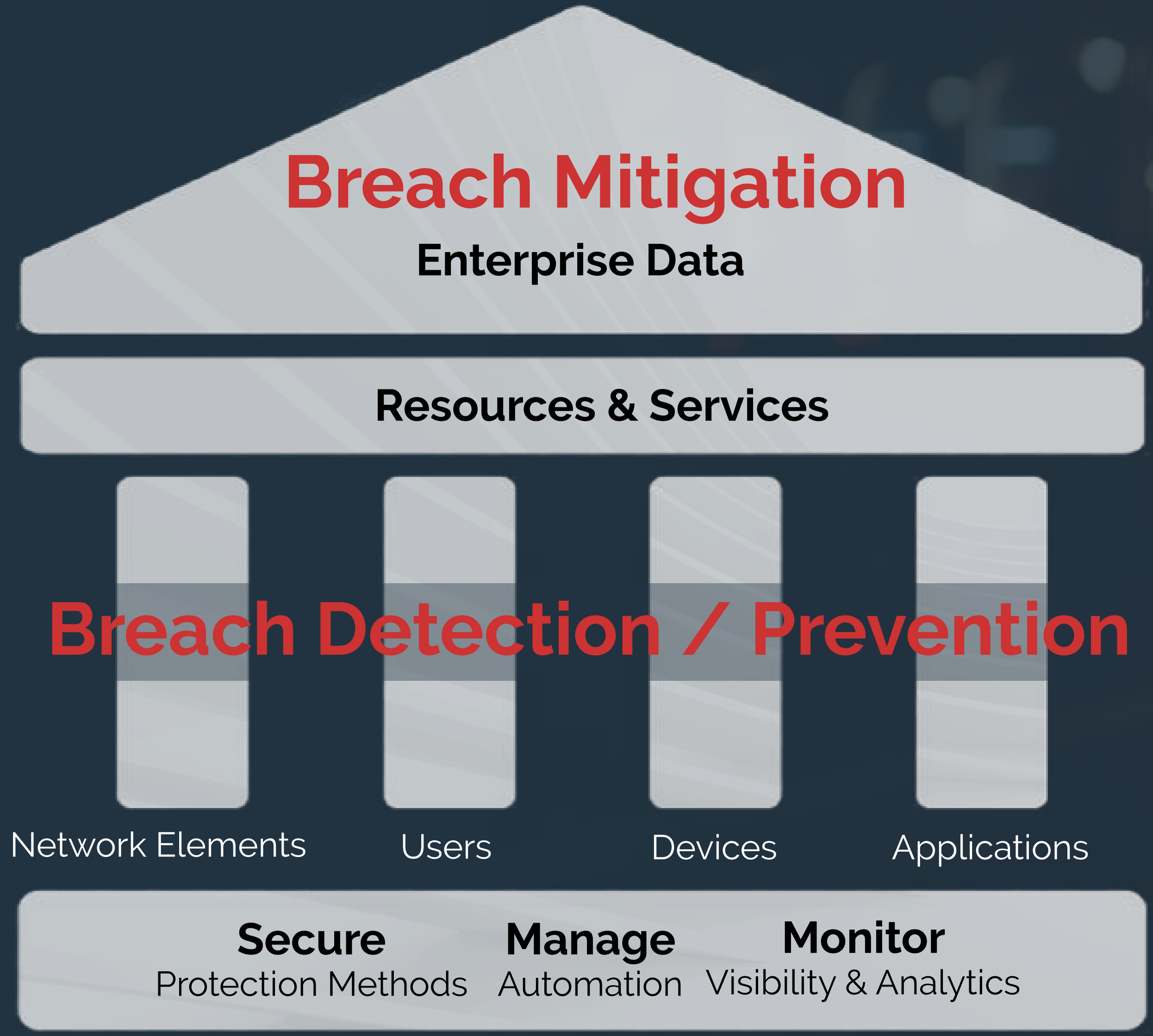
Pillars of Zero Trust

In the US DoD's reference architecture, the authors provide a very thorough walkthrough of the different parts of an IT infrastructure and the different protection mechanisms which help to implement Zero Trust within that area. The reference architecture centers around seven "pillars" of Zero Trust:

- Network elements, meaning the infrastructure creating connectivity within your IT infrastructure.
- Users who leverage the network to access information, data, and/or services to get work done.
- Devices including workstations, laptops, and even tablets and mobile devices.
- Applications, either directed by users or through automation, that work with information, data, and service to carry out business-specific workflows.
- Data, which includes all information that users interact via various business applications and which is the centerpiece of every organization.
- Automation resources to carry out workflows with little or no user intervention.
- Monitoring and analytics tools and functions to assess and analyze systems and data.

Data isn't a Pillar of Zero Trust

The problem with the pillar structure is that it places data as a coequal part of your entire IT infrastructure. We don't see it that way. Keep in mind the testimony referenced earlier and any breach report you've heard of—threat actors are after sensitive information and data. Everything else is just a means or a conduit to get to that data. If we refactor the pillar view just a bit to reflect the predominance of data, it might look a little like this:



Data is Where You Start

All of this leads to a very simple point. If you are looking for a place to start your Zero Trust journey, which means an investment in time, money, and effort, look to what all the threat actors are after. You want to protect the data first and foremost, so that's where you start.

In this representation, the pillars are supporting the crowning part of the structure, which is data. Perhaps it's just a bit of semantic manipulation, but we don't think so. Even the US DoD says that Zero Trust is a philosophical shift in thinking. We're suggesting that the philosophy is more applicable if you view data as the most important part of the entire structure.

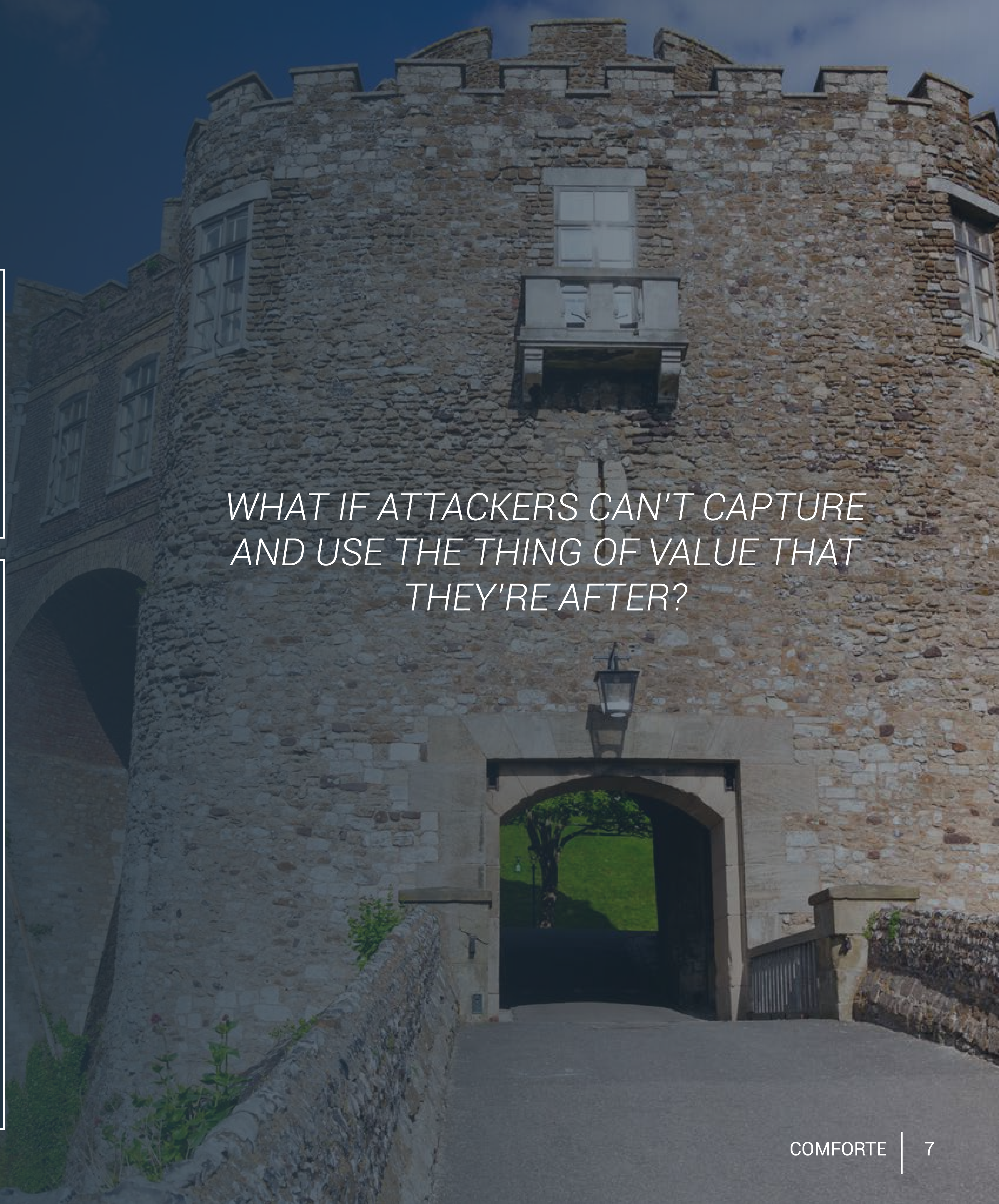
HERE’S HOW DATA-CENTRIC SECURITY HELPS ACHIEVE ZERO TRUST

Data-centric security means protecting your data—applying the protection methods direction to the data itself—rather than the borders and environment around that data. If data is what threat actors are really after, then the logical starting place for any Zero Trust implementation would be your enterprise data, which could be compromised, monetized, and weaponized in a way that would negatively affect your organization. But what can you do with data that would thwart bad actors who get their hands on it?

Let’s look at an analogy to show the power of protecting the thing of value instead of the environment around it. Think of a castle. Medieval castles had multiple layers of security implemented around them.

Just as with your IT infrastructure, castles had borders and guarded perimeters to try to keep unwanted people out, from walls and moats to drawbridges and inner keeps and towers. If attackers could get through all the defenses and to the throne room to capture the king and queen, then it was game over, right? But what if the king and queen escaped through a secret passage? The attackers wouldn’t get the ultimate prize, and so the attack wasn’t a success. This is what data-centric security does to your data—turning the sensitive data elements into innocuous representational elements that make the data incomprehensible, so threat actors can’t leverage it for nefarious purposes. Yes, hackers get to the data, but that information is of no use to them.

The ultimate point of Zero Trust is to assume an attack is underway and to negate any detrimental effects of threat actors getting to your enterprise data. Like whisking the king and queen away, data-centric security helps you achieve Zero Trust by making any sensitive information incomprehensible (and uncompromised) unless a very specific, validated request for that information exists.



WHAT IF ATTACKERS CAN’T CAPTURE AND USE THE THING OF VALUE THAT THEY’RE AFTER?

Comforte has a long and successful history in mission-critical applications and enterprise data security. Our data security platform can enable you to start with Zero Trust by protecting your enterprise data itself. Check out our capabilities and some success stories by going to

www.comforte.com