twosix
TECHNOLOGIES

CRACKS IN THE FOUNDATION OF ZERO TRUST

It’s Time to Build ZTA From the Ground Up

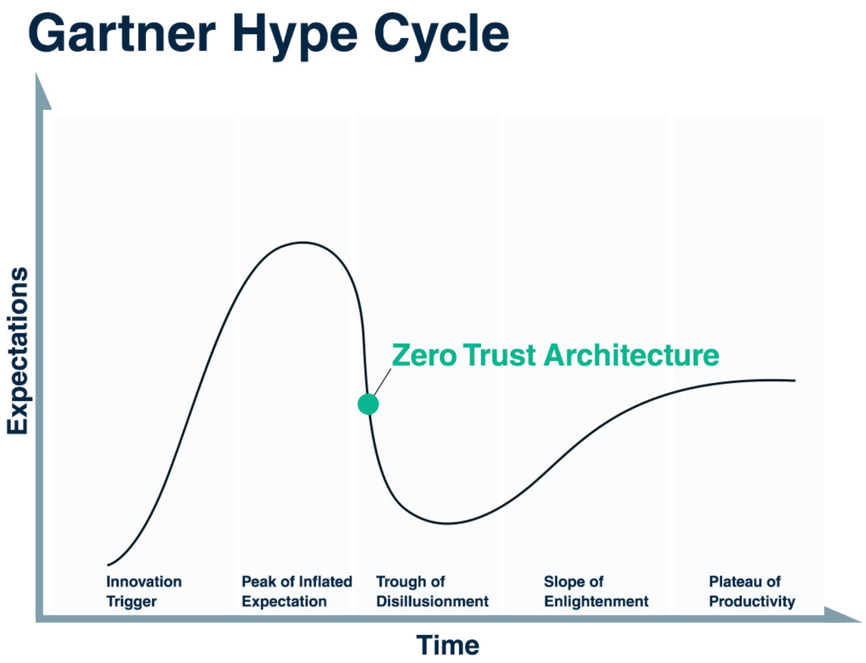
When nation-state cyber criminals strike, their attacks aren’t a minor inconvenience; they’re a major threat to national security.

Our most sensitive information is kept under digital lock and key — and foreign threats keep breaking in. **Microsoft** found that 40% of all attacks on U.S. critical infrastructures were nation-state motivated. With foreign threats in mind, it’s no wonder why the **Office of Management and Budget** released a federal plan to move the U.S. government towards implementing zero trust architecture (ZTA). It’s one that demands entities move at a breakneck pace.

> On the topic of deploying zero trust across enterprise systems by 2027, **Department of Defense (DoD) CIO John Sherman** stated, "The adversary capability we're facing leaves us no choice but to move at that level of pace."

However, government organizations face a major challenge in trying to implement zero trust: managing legacy systems. The **Center for Strategic & International Studies** reports that "technology debt" is one of the greatest barriers to ZTA, with a majority of the $90B federal budget for IT being spent on legacy maintenance.

As a result, organizations are left with few options but to "patchwork" together solutions for zero trust. In other words, security teams must combine zero trust tools in an effort to achieve a strong foundation of ZTA. Here's the problem: Many of these component solutions are not built to deliver comprehensive zero trust — leading to significant (and dangerous) cracks.



Cracks in the Foundation of Zero Trust

Zero trust is in the thick of what Gartner describes as the “trough of disillusionment.” We’re starting to see that some early solutions purporting to enable zero trust fail to deliver. For example, a “zero trust” tool might encrypt data for an organization but also pass secrets in clear text. — causing an ideological crisis in a sea of tools claiming to provide zero trust.

Government agencies, prime contractors, and technology vendors don’t just need a zero trust solution — they need a zero trust *engine* that has the power to implement the highest security standards for every interaction in every environment. That’s why we built TrustedKeep with “never trust, always verify” underpinnings at its core, meaning security teams can put an end to external and internal incidents like:

The 2013 National Security Agency (NSA) Leaks

The leak from NSA contractor Edward Snowden caused more than 1,000 high-priority intelligence targets to remove themselves from visibility, including those plotting directly against the U.S.

The 2023 Microsoft Hack

China-backed bad actors forged authentication tokens and gained access to several government email accounts, conducting espionage undetected for a month.

The 2023 Pentagon Leak

U.S. Airman Jack Texeira released countless classified documents about the Russia-Ukraine War on Discord, compromising missions overseas.

We’ll dive into the foundations of zero trust and what underlying capabilities are the key to implementing **comprehensive** zero trust architecture. Plus, we’ll share why TrustedKeep is the zero trust engine that can help:

Government agencies:

Set the right requirements for zero trust from the bottom up, targeting a strong end-to-end ZTA.

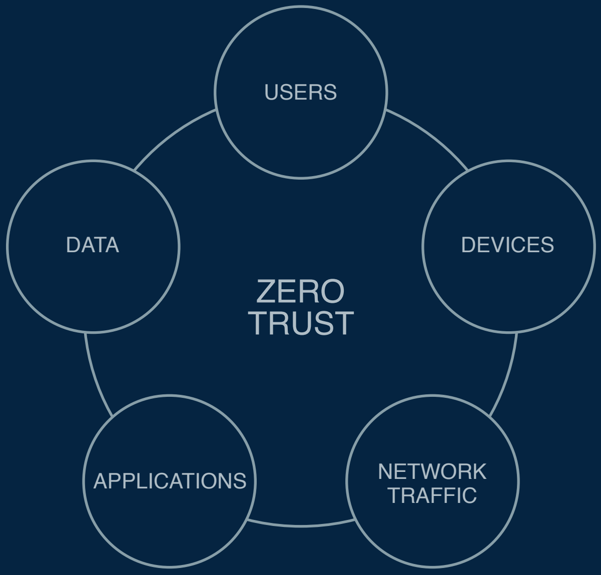
Prime contractors:

Deliver the best, secure zero trust solutions to your customers.

Technology providers:

Enable comprehensive zero trust for customers — fast, augmenting your capabilities without the need to completely rework or rehash your existing solutions.

What Is Zero Trust?



Zero trust is the cybersecurity gold standard. Several authoritative frameworks and entities have covered recommendations and standards for zero trust, including **NIST SP 800-207**, **CISA's Zero Trust Maturity Model**, **ISO/IEC 27001**, and the **Center for Strategic & International Studies**.

Zero trust architecture is the much-needed update to legacy, perimeter-based cybersecurity. Organizations can no longer rely on implicit trust to defend their networks. That means ZTA, at its core, must enable:

- **Strict separation of duties:** No admin should have access to keys and the data they protect.
- **Continuous authentication of identities:** No more "one-time" log-in processes.
- **Least privileged access in all environments:** Only those who absolutely *must* have access *should*.
- **Never trust, always verify:** No activity, whether it originated from outside or inside the perimeter, should be assumed to be trustworthy.

Without fulfilling those critical components, a "zero trust" program is not really zero trust at all. It's only a partial salve for larger security problems. Achieving the **needed** level of zero trust to protect our national security is about assuming all contacts and connections are potential threats until proven otherwise — and being able to do this at massive scale while maintaining performance.

What It Takes to Fill in the Zero Trust Cracks

Government organizations *must* move swiftly and efficiently to implement ZTA — or risk having the next Snowden on their hands. However, the current approach to zero trust is flawed because:

- **It's not up to the task.** These solutions only provide *elements* of zero trust, not the core of it. They cannot grant the holistic foundation of security required to implement real zero trust — and that leads to big national security breaches like Snowden, stolen capabilities like the J-20 and FC-31, and shut down critical infrastructure.
- **It affects performance.** Even if component solutions don't *break* existing architectures, they can seriously affect their performance — practically negating any small security benefit from implementing them.
- **It breaks existing architectures.** The fact is organizations have structures, connections, and workflows within them that they cannot transform with a snap of their fingers. Many solutions that help put zero trust practices into place would compromise the efficacy of these essential legacy architectures.

The Reality

Comprehensive zero trust *must* be built from the ground up, not cobbled together through patchwork solutions later. Subsequently, organizations must leverage tools that:

1. Implement a strict separation of duties for data access, policy administration, and control plane administration
2. Enable consistent policy enforcement across clouds and private data centers
3. Continuously authenticate users with strong identity management, PKI, and multi-factor authentication
4. Ensure that the policies being enforced are the right policies
5. Integrate well with existing capabilities to make them more secure, not more fragile

A strict separation of duties helps combat international threats — like Russia- or China-backed threat actors — by minimizing the ripple effect of a compromised or breached user. It also mitigates a growing threat to successfully implementing zero trust: insider threats.

Insider threats and nation-state bad actors are the heavy hitters in the current threat landscape. Organizations must extend the zero trust core tenet of “never trust, always verify” to even the administrators in charge of safeguarding and handling sensitive data to achieve a true foundation of zero trust.

But current approaches to zero trust are not only bogged down by legacy tools and solutions — they’re also bogged down by legacy *mentalities*.

Old habits die hard. Government agencies have been engaging in the same security practices and strategies for decades. That makes it a logistics nightmare for large organizations with a lot of history (and a *lot* of sensitive assets) to get the ball rolling quickly.

Federal entities are in need of a platform that can enforce zero trust without breaking legacy systems or compromising existing workflows. That’s a tall order for some solutions, but the right zero trust *engine* can get the job done.

> “We can say, ‘Assume breach,’ but people want to do the same things they’ve done in the past,” says **Kevin Bingham**, NSA Zero Trust Lead. “It’s just the way our programs are set up. It’s the way you were trained… That cultural change is hard.”

Now Enter: TrustedKeep

TrustedKeep was conceived and built to enable secure collaboration and dissemination of the government's most sensitive data long before the current ZTA hype drew in other solutions and motivated services to engage in zero trust rebranding.

In the wake of national disasters like 9/11, our plucky team of security pros knew there was a serious problem with getting intelligence where it needed to go — quickly and securely. Those incidents, plus a rapid influx of info-sharing with the cloud, inspired our experts at TrustedKeep to build a system that could meet the fundamental requirements of zero trust.

We operate on this critical source of truth: that **real** zero trust works like an engine, not an add-on.

A Zero Trust Engine Is What You Need

Our platform was built with zero trust in mind from the start — making it the engine you need to drive zero trust throughout your organization. The core value components of our engine are:

- A strict separation of duties
- Object-level encryption with unique keys
- Secure, on-premise key management
- The highest level of accreditation
- Unmatched operational track record since 2018

Strict Separation of Duties

TrustedKeep was purpose-built with a strict separation of duties in mind. Our platform has controls that prevent gateway administrators, policy administrators, and users from being the same person. This prevents the muddying of duties that often lead to intentional and accidental insider threats. Plus, no users are permitted to log into TrustedKMS — where all the data gets stored. Administrators can only access that data through APIs requiring PKIs and multiple identification factors to get in.

Object-Level Encryption

Very few zero trust solutions encrypt data to the object level. We built TrustedKeep with this goal from the beginning.

TrustedKeep protects each object equally. Why? Because it's essential that it be difficult to distinguish between data points that are being actively protected and data points that *aren't* being actively protected.

No other tools on the market encrypt data at this fine-grain level. We protect data to the most incremental level to throw potential threats off the scent of valuable information. And for use cases with more flexible security needs, TrustedKeep allows you to tailor your encryption approach to match your policies.

Key Management

TrustedKeep can produce billions of keys simultaneously, but we're not adding any secrets management tasks to your security team's plate.

Our tool contains a high-performance, distributable data store that's essentially event-based. For every piece of data that comes in through TrustedKeep, we harbor its metadata and encryption keys within that data store. These encryption keys never leave TrustedKeep's boundaries, and even authorized administrators cannot request access to or view them.

We manage these keys disparately from your data, where even administrators cannot get direct access to them. This helps mitigate the chances of a successful insider threat.

Accreditation

TrustedKeep is accredited to protect systems handling the most sensitive data our customers have. Our tool is ready-made to support hyper-sensitive workloads. The Intelligence Community (IC) and DoD trust us to protect classified information — and support workloads that no other tools are prepared to support yet.

We meet the strictest government standards for privacy and security. Therefore, we're equipped to scale out confidential workloads in other highly sensitive areas where there might be a significant risk of exposure.

Operational Track Record

Our platform has been running without downtime for *years*. In that time, we've encrypted and helped transfer some of the most high-level classifieds in the federal sector. Since 2018, our tool has ensured countless classified workloads are secured to the nth degree as they move to and from users, data centers, servers, and ephemeral environments like the cloud.

TrustedKeep Turbo-Charges ZTA Projects

Bad actors are only getting bolder. Your organization needs a zero trust engine that works across all environments and systems — or it risks being the next source of a national security disaster.

TrustedKeep was created with the underpinnings of zero trust in mind from the start. That’s why we safeguard some of the most highly classified information in the federal sector and have the power to prevent future Snowdens and Operation Auroras from happening.

It’s time to turbo-charge your ZTA projects and keep sensitive assets locked down air-tight. With TrustedKeep, you won’t be signing up for the hype. You’ll get the real thing.

Ready to turn your zero trust goals into a reality?
Get in touch with us at **trustedkeep@twosixtech.com**.