Rethinking your defenses

What to know about nation-state adversaries like Salt Typhoon and how to defend against them

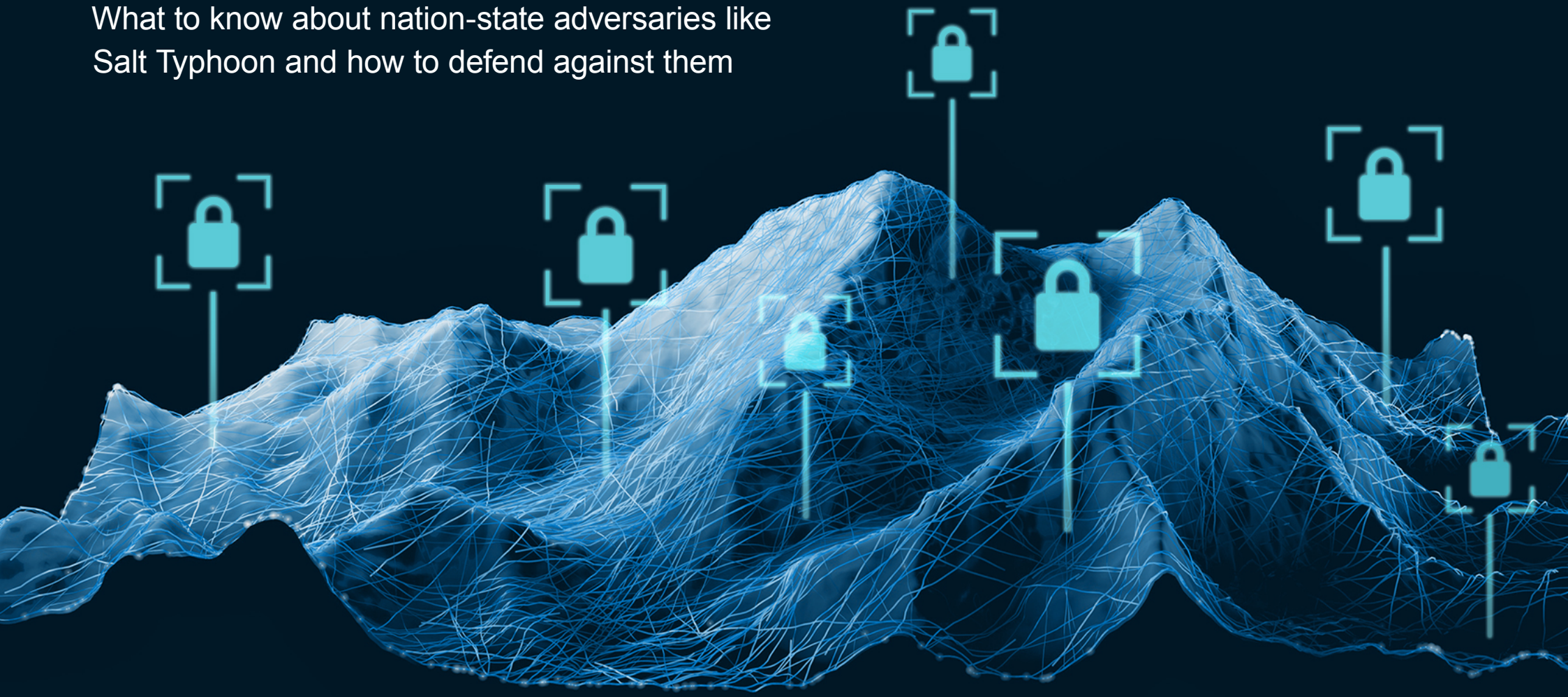


Table of contents

Advanced threats are expanding their target lists 3

Top challenges in defending against advanced threats 4

How advanced adversaries operate 6

How your current environment may increase risks 7

Rethinking infrastructure to reduce exposure 8

Preparedness is your best defense 9

Advanced threats are expanding their target lists

Ransomware attacks are well known to most enterprises, but nation-state adversaries don't always get the same attention. These bad actors bring fundamentally different capabilities and intentions to the table.

Threats such as Salt Typhoon are well-organized, well-funded, and patient. Their intent is to get inside your network, linger, gather information over time, and potentially cause harm. However, just because Salt Typhoon isn't making headlines the way it did at its onset doesn't mean the threat has eased. The group remains active and stealthy.

Salt Typhoon conducts espionage as a long-game of information theft of intellectual property for strategic global advantage. The goals of the threat differ from those of financially motivated threat actors, who rely on ransomware and extortion for criminal gain. As a result, nation-state adversaries such as Salt Typhoon warrant heightened awareness and focused diligence that extend far beyond typical cybersecurity measures.

Salt Typhoon is affiliated with the People's Republic of China. It's focused on espionage as its primary objective. Active since at least 2019, the group is responsible for numerous network infrastructure compromises and widespread intrusion activity against several major U.S. telecommunications companies.

Top challenges in defending against advanced threats

Defending against adversaries such as Salt Typhoon can be challenging for enterprises. The characteristics that make nation-state actors and other advanced persistent threats (APTs) successful are the same ones that also make them difficult to counter. Challenges include:

1 Unsupported equipment creates persistent exposure

Many environments still use equipment that manufacturers no longer support. When a device no longer receives security updates, these vulnerabilities can accumulate without remediation. APTs find and exploit these gaps as entry points.

2 Attackers move slowly to evade detection

Advanced adversaries are incredibly patient. They move slowly and are careful not to show their tactics or capabilities while maintaining presence in a network. This strategy makes it challenging to identify threats quickly. Proactive threat hunting and the ability to detect subtle variations in normal activity are key to uncovering these threats.

3 Internet-facing systems are a primary entry point

Attackers rely heavily on exploiting internet-facing appliances for initial access. These systems live at the boundary of your network. When running unsupported software, they provide adversaries a well-established path to entry.

4 Advanced threats leverage weaknesses throughout the supply chain

Attacks against vendors, partners, upstream and downstream suppliers are all potential vectors used to gain access to organizations through trusted connections.

Case study:

Telecom leader closes vulnerability entry points across thousands of devices with GDT

The challenge:

A telecommunications leader with a highly distributed U.S. infrastructure was looking to address end-of-life and end-of-support (EOL/EOS) devices while accelerating modernization. Internal teams lacked the capacity and specialized expertise to execute at the required scale and speed.

The solution:

GDT delivered a two-phase program that combined EOL/EOS device replacement and IOS firmware upgrades. Devices were preconfigured, validated, and hardened at GDT's staging facilities prior to deployment. This allowed for execution within four-hour maintenance windows across live production environments without operational disruptions.

The result:

- Approximately 1,000 EOL devices replaced annually
- Reduced attack surface through remediation of known vulnerabilities
- Faster modernization with minimized downtime
- Stronger security posture with consistent patching and firmware updates
- Reduced burden on internal teams, freeing capacity for higher-value work

Read the full case study

How advanced adversaries operate

Understanding how Salt Typhoon and similar groups operate can help you build stronger defenses. Adversaries are focused on a diligent, patient, stealthy, and organized approach to attacks. The profile of these advanced adversaries includes:

Focus

Crosshairs aimed at specific industries and organizations. For example, telecom providers and service providers are prime targets.

Diligence

They have near-infinite resources focused on objectives that contribute to long-range strategies.

Patience

They are willing to move very slowly to avoid revealing tactics and evade detection. This approach allows them to maintain presence over long periods of time.

Infrastructure and network solutions

GDT architects, manages, and supports resilient, scalable IT environments tailored to meet regulatory demands and support secure, reliable network and data access.

Living off the land

Salt Typhoon may use tactics similar to other types of threats, such as stealing credentials or exploiting public-facing vulnerabilities, but it also uses a “living off the land approach.” Instead of introducing unfamiliar tools that might trigger detection, it uses tools, protocols, and utilities that already exist in your environment. This strategy makes the activity harder to detect within normal operations.

Common tactics

Salt Typhoon uses coordinated and multilayer attacks, such as the following:

- Credential use and expansion
- Configuration exfiltration
- Infrastructure pivoting
- Configuration modification
- Packet capture
- Use of present operational tools in addition to custom-built utilities such as JumbledPath
- Defense evasion

Advanced adversaries don’t just break in to achieve financial objectives; they move laterally, quietly, and carefully. They expand credentials and repurpose the same tools your teams use every day.

How your current environment may increase risks

Many enterprise environments weren't designed for a threat like Salt Typhoon. The infrastructure decisions made years ago — reasonable at the time — can now create conditions that advanced adversaries actively exploit.

Unsupported equipment

Equipment that is no longer supported by its manufacturer can serve as the perfect entry point for attacks on your network. When patches and updates no longer arrive, known vulnerabilities become the entry points that bad actors exploit.

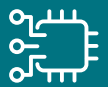
Legacy architectures and complex protocols

Legacy architectures often use complex protocols, tunnels, and overlays that accumulate over years of gradual change. This complexity creates a strong advantage for attacks. Ambiguity about what normal looks like can make anomalous behavior harder to identify and investigate. A network built on a legacy of workarounds and deprecated protocols provides these adversaries with plenty of places to hide.

Unpredictable traffic paths

Without predictable traffic paths, establishing a baseline for normal network behavior is more difficult. When teams can't clearly define how traffic should move between important systems, unexpected pivots, route detours, and configuration changes are much harder to detect.

These conditions allow attackers to remain in your environment without triggering alerts. And the longer an adversary remains undetected and the more information they gather, the greater the exposure to potential risks.



With advanced adversaries such as Salt Typhoon, a network that is more observable, segmented, and controllable helps teams validate that protections are working and identify potential anomalies sooner.

Rethinking infrastructure to reduce exposure

Rethinking network design is increasingly important in protecting against advanced threats. Architectural choices that reduce complexity and increase visibility help minimize the conditions that adversaries, such as Salt Typhoon, thrive on.

Micro-segmentation limits lateral movement

Micro-segmented paths make lateral movements across your environment more difficult. Enforcing boundaries between critical domains raises the cost of what an attacker must do after gaining that initial access. Instead of moving freely across your network using stolen credentials and existing tools, the adversary hits friction at every boundary you set.

With carrier-grade architecture, locator-based routing, and segment ID chains, micro-segmented paths can be enforced between critical domains. That makes lateral movement and infrastructure pivoting much harder for bad actors to execute.

Increased visibility supports faster detection

When security teams can view traffic behavior more clearly and compare it to a known baseline, they can more easily spot subtle variances. Deterministic, intent-driven paths that are easy to verify and monitor mean unexpected route changes or traffic detours are quickly visible, rather than blending into background noise.

Troubleshooting also becomes easier and quicker. For example, inspecting a packet header to confirm routing intent is much more efficient than tracing an MPLS label-switched path across a complex, multilayer topology.

Deterministic routing improves monitoring and validation

Deterministic routing improves monitoring and validation by making expected behavior explicit. When a team knows exactly how traffic should flow between systems, changes from that expectation are clearer. This makes the repurposed tools and unexpected traffic that living off the land supports easier to spot

A network environment that is more observable and controllable helps to reduce risk around an attacker's success.

Standardizing modern security controls, rather than operating with a patchwork of legacy tunnels and deprecated protocols, eliminates the favorite hiding spots that advanced persistent threats seek to exploit. The goal is a network fabric that is easier to harden, observe, and validate against long-game intrusions.

Preparedness is your best defense

Defending against nation-state and advanced attacks requires a comprehensive approach. You need the ability to identify vulnerabilities and potential exposures, protect against them, and detect when attacks are occurring so you can respond quickly.

GDT enables clients to defend against advanced attackers through a comprehensive approach.

In-depth, advisory-led assessments

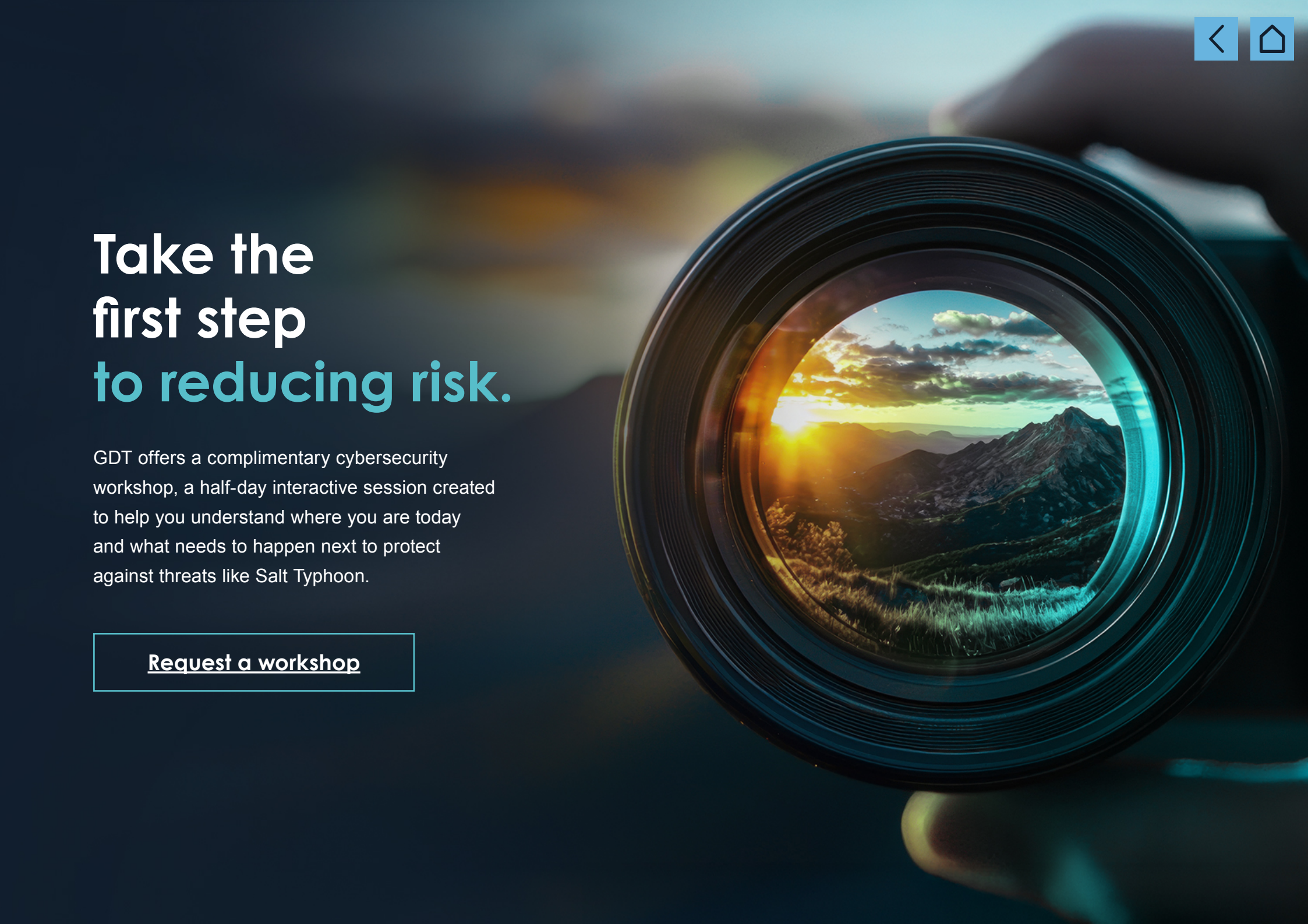
GDT helps you build a solid foundation through an in-depth, comprehensive assessment. This engagement supports you in understanding where your environment is today, identifying your largest exposures, and determining your next best actions.

A modular approach to prioritize highest-impact actions

Our approach is modular, which means your organization doesn't have to complete an extensive study before acting. The modular model allows you to start addressing the highest-priority exposures immediately while broader assessment work continues.

Ongoing testing, validation, and support to stay ahead of new threats

Adversaries are continuously adapting to avoid detection. Testing and validation of defenses and detection processes are critical in keeping pace with evolving threats. We provide ongoing support to help you stay ahead of new threats, so your defense remains strong in the future.



Take the first step to reducing risk.

GDT offers a complimentary cybersecurity workshop, a half-day interactive session created to help you understand where you are today and what needs to happen next to protect against threats like Salt Typhoon.

Request a workshop