STEALTH CYBERSECURITY TACTICS

An Overview of Non-Attributable Data Networking and Communications Using the SecureCo Platform

EDITED BY DR. EDWARD AMOROSO
CEO & SENIOR ANALYST, TAG CYBER

TAG CYBER

secureco

STEALTH CYBERSECURITY TACTICS

AN OVERVIEW OF NON-ATTRIBUTABLE DATA NETWORKING
AND COMMUNICATIONS USING THE SECURECO PLATFORM

EDITED BY DR. EDWARD AMOROSO, CEO & SENIOR ANALYST, TAG CYBER

This book introduces and explains how non-attribution and obfuscation provide good risk mitigation of communication monitoring and network surveillance risks to organizations. The articles focus on various aspects of the issue and demonstrate use of the SecureCo solution in practical business settings to address this challenge.

CAN YOU HIDE YOUR BUSINESS FROM NETWORK MONITORING?

ED AMOROSO,
TAG CYBER

In 1979, the Director of the National Security Agency, Bobby Inman, was standing at a conference podium when a hand went up in the crowd. Admiral Inman acknowledged the question, which was essentially this: "Will the recent advances in public key cryptography from Diffie and Hellman make it harder for NSA to spy on citizens?" Such a familiar exchange from almost a half-a-century ago illustrates the persistent concern citizens have with network monitoring.

The earliest wiretaps showed up in New York City in 1895 when Mayor William Strong decided it would be acceptable to listen in on telephone conversations to catch criminals. (And yes, the date is correct: Bell got his patent in 1876.) Anyway, the idea obviously caught hold and throughout the twentieth century, the technique was used to bring down gangsters. The notorious John Gotti, for example, was brought down using Title III wiretaps in Manhattan.

These early examples have evolved into a collage of different approaches to monitoring targets, both individuals and groups, that want to avoid being monitored. Certainly, monitoring can advance the good of society by helping catch criminals and make citizens and businesses feel safe. But there is also the nefarious monitoring, which highlights the need for good solutions to prevent unwanted data collection.

Consider, for example, that businesses operating across global infrastructure often encounter countries that have long-standing policies and reputations for unrestricted monitoring. When this occurs, the business must determine whether to accept this risk or to implement a security solution that creates a more reasonable environment for them without unacceptable levels of surveillance.

In recent years, this concept of network monitoring has expanded, like the rest of society, into a more data-oriented internet context. Communications have shifted from circuit-switched phones to global zero-trust data networks, and this has prompted network monitoring agents, both good and bad, to adjust the technology being used. The unifying themes are twofold: networks are harder to monitor, but monitoring tools are also much better.

The social implications of hiding from network monitoring can be debated. Take the popular Tor browser, for example. While it can be used by oppressed individuals and groups trying to share important information with the world, it can also be used to sell drugs on the dark web. The double-edged sword nature of non-attribution must be acknowledged (especially in the context of the general public) and should factor into any discussion on the topic.

Nevertheless, the contention raised here is that businesses have under-used the technique, which can be deployed to prevent nefarious, illegal, and unethical monitoring of their corporate communications. The good news is that great technology and services exist for modern businesses to deploy and use, and we believe that for many applications, this would be an excellent decision.

This is the first of a series of commissioned articles that address this topic from several different perspectives. In the first article, TAG Cyber analyst John Masserini draws on his decades of experience as a chief information security officer to outline many of the risks that emerge from monitored communications. John explains how network activity monitoring is assisted by sloppy security such as running older mobile device software.

In the second article, TAG Cyber analyst Chris Wilder draws on his extensive experience in the US Department of Defense (DoD), as well as the private sector, to explain some of the methods used by governments to monitor networks and also to evade such monitoring. Chris shows how detailed processes and procedures pervade the government space and are often driven by legal concerns to ensure that nothing is being done improperly.

In the third article, TAG Cyber analyst Ed Amoroso provides a textbook introduction to the best current methods for achieving non-attribution and obfuscation in a network. The discussion draws heavily on the method known as onion routing, but readers will not have to possess a computer science background to follow the discussion. The goal is to help practitioners understand how network traffic can be better hidden, especially in business.

Finally, the team from commercial cyber security vendor SecureCo offers an overview of their solution. The SecureCo platform is designed to support non-attribution and obfuscation for business and government customers. The article explains the technique and offers practical case studies for how business customers are using the tool to avoid being monitored by nefarious actors.

The final article suggests an action plan for organizations that might choose to deploy this important network security control. Practical guidance is offered on how the SecureCo platform can be reviewed, tested, and deployed to determine if the security protection is suitable for the local environment. The goal is to help readers find ways to reduce their network monitoring and surveillance risks.

– I.–

THE HAZARDS OF EXPOSURE TO NETWORK MONITORING

JOHN MASSERINI,
TAG CYBER

The design decision in the 1960s to support connectionless processing for TCP/IP changed the nature of how communications might be monitored by governments or malicious actors. In traditional telephony, the endpoints are defined by a circuit-switched connection, but with the advent of the internet, source and destination addresses would be controlled by participants, rather than through some centralized authority such as a telephone company.

As a result, new methods emerged for both legitimate and illegitimate collection and interpretation of communications for targeted individuals, groups, and entities. As it is generally accepted that most people follow familiar, pre-determined routes throughout their day, by leveraging cell phone tracking techniques, malicious actors can quickly identify such routes and plan accordingly.

Whether for potential kidnapping or for subverting specific wireless network points, the ability of an adversary to predict someone's location, identity, and activity at any given time has significant implications. Additionally, the ability of an adversary to monitor network traffic can provide insights into the systems and applications the target uses, as well as basic data elements like passwords or multifactor authentication codes sent electronically.

Such new approaches are collectively referred to as traffic monitoring and they depend on deployed collection and processing tools that offer sufficient coverage and insight to achieve the monitoring objective. Citizens and businesses must be aware of this monitoring and surveillance risk because it presents a real and immediate threat to the protection of sensitive data and the assurance of critical operations.

In this article, we outline the risks that emerge for citizens and organizations where illegitimate monitoring of their communications might be occurring. Such risks could stem from data collection and review by hackers, criminal groups, hacktivists, or adversary governments using network analysis as the basis for their data theft. Understanding the risks requires investigation of the types of monitoring that would be deployed in practice.

1.1 Traffic Monitoring

Most infrastructure-centric communications companies, both telephony and internet service providers (ISPs), have legitimate traffic monitoring needs. Whether for problem resolution or capacity planning, the ability to monitor communications traffic is essential to providing the level of service most users are accustomed to. Unfortunately, the abuse of this necessary function is what causes substantial concern to privacy advocates.

It is customary to find static traffic pathways for most legacy communications providers. This approach, leftover from the days of switched POTS (plain old telephone service) networks, ensures a predictable, highly efficient path through the network's switching infrastructure. Additionally, such predictable networking ensures the existence of tap points throughout the network, which are necessary to support government wiretapping requirements.

While ISPs have been excluded from wiretapping requirements, they still have the need to monitor traffic for outage resolution and quality of service (QoS) for customers. In fact, the explosion of video conferencing during the pandemic caused many ISPs to rethink QoS metrics and routing protocols to ensure that, almost virtually overnight, the millions of new work-from-home employees could rely on video conferencing platforms.

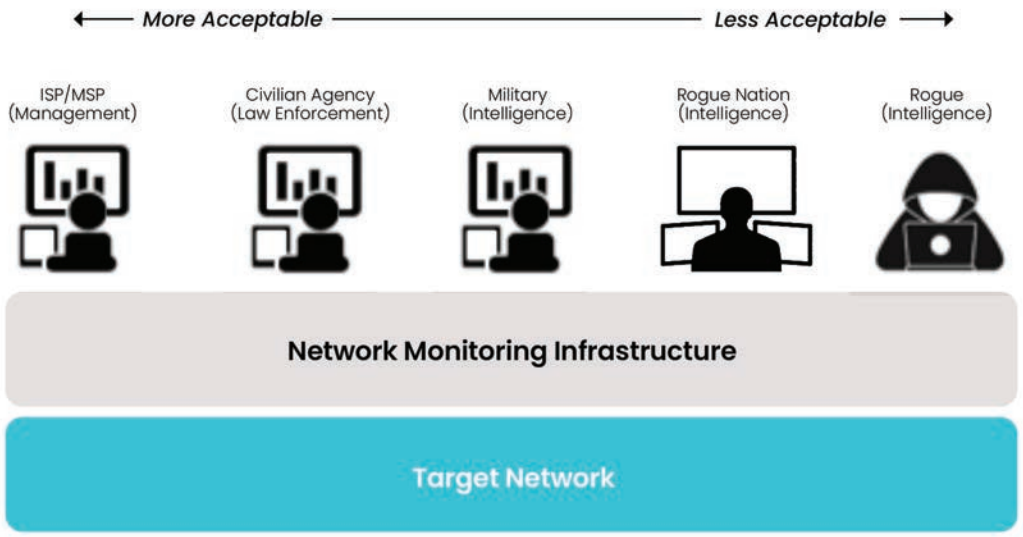

Figure 1.1-1. Network Traffic Monitoring Landscape

As 5G becomes more ingrained within the mobile providers, the lines between ISPs and phone companies become ever more blurred. The relentless push to move more services to the edge will invariably alter the network monitoring landscape, and further blur the line between network monitoring and activity monitoring. To ensure the highest level

The truth is that while ransomware and malware get the headlines, the foundation for their success to attackers often has to do with network and activity monitoring and the ability to capture and decode user traffic

of throughput, 5G networking architectures move infrastructure, which is currently buried deep within the operational technology networks, as close to the edge of the network as possible. This helps to ensure that the latency seen in existing networks is minimized as much as possible.

However, the risks associated with deploying this new architecture, which is based on NFVi (Network Function Virtualization infrastructure) must also take into consideration the cloud and software risks that accompany deploying a virtual infrastructure that bridges multiple networks. Additionally, attacks on the edge distribution platforms as well as network slicing attacks are making network obfuscation increasingly important for those concerned with the risks around confidentiality and privacy.

Secure communication also becomes ever more critical as we connect an increasing number of internet of things (IoT) devices to the public internet. This can include devices such as an obscure SCADA RTU/PLC device managing a natural gas pipeline, or a high-end connected sports car. In each case, the risks are real and substantial. An attacker gaining access to a SCADA device could easily adjust the pipeline pressures to cause an explosion, or they could cause the sports car to speed excessively, run red lights, or fail to negotiate a sharp bend in the road. Regardless of the endpoint, there will be heavy reliance on a trusted communication channel to protect the neighborhood above the pipeline or the passengers of the car.

ACTIVITY MONITORING

The use of activity monitoring on a targeted network is well documented in the press. In many countries around the world, restrictive governments have implemented technology that monitors and limits what their constituents can access on the internet. While the Great Firewall of China is the most notorious example, many countries have enacted similar technical or regulatory restrictions.

An additional network monitoring use case involves the malicious targeting of key enterprise personnel in an effort to gain information about access credentials, personal information, and methods used to impersonate said individuals for access into critical infrastructures. Protecting employees in an unmanaged/lightly managed remote work scenario is a challenge that's come front and center since the peak of the pandemic. It should come as no surprise that enterprises were hit by ransomware more in the first six months of 2021 than in all of 2020. Not only did these attacks cause significant system outages and downtime across virtually all industries, but as the ransomware evolved, hundreds of millions of customer records were also exfiltrated.

Employees are now forced to use their personal devices to conduct business (sometimes using endpoints of questionable security) over networks of questionable stability and risk profiles. The truth is that while

ransomware and malware get the headlines, the foundation for their success to attackers often has to do with network and activity monitoring and the ability to capture and decode user traffic.

SECRECY AND PRIVACY CONCERNS

The issue of personal privacy was never more apparent than during the onset of the COVID-19 pandemic. During this time, some governments mandated carriers to correlate cellular location data to track the spread of the virus. While this and other forms of government tracking are obviously controversial, there remains great interest in African and APAC regions to track mobile device users and limit secured or private communication channels.

As was widely reported by Amnesty International, software from the **NSO Group,** an Israeli group known for surreptitious tracking of criminals and terrorists, was widely reported to be found on dozens of mobile devices of those people close to an investigative journalist who was murdered in **2021.** Such tracking can easily extend beyond targeting bad actors to the targeting of anyone.

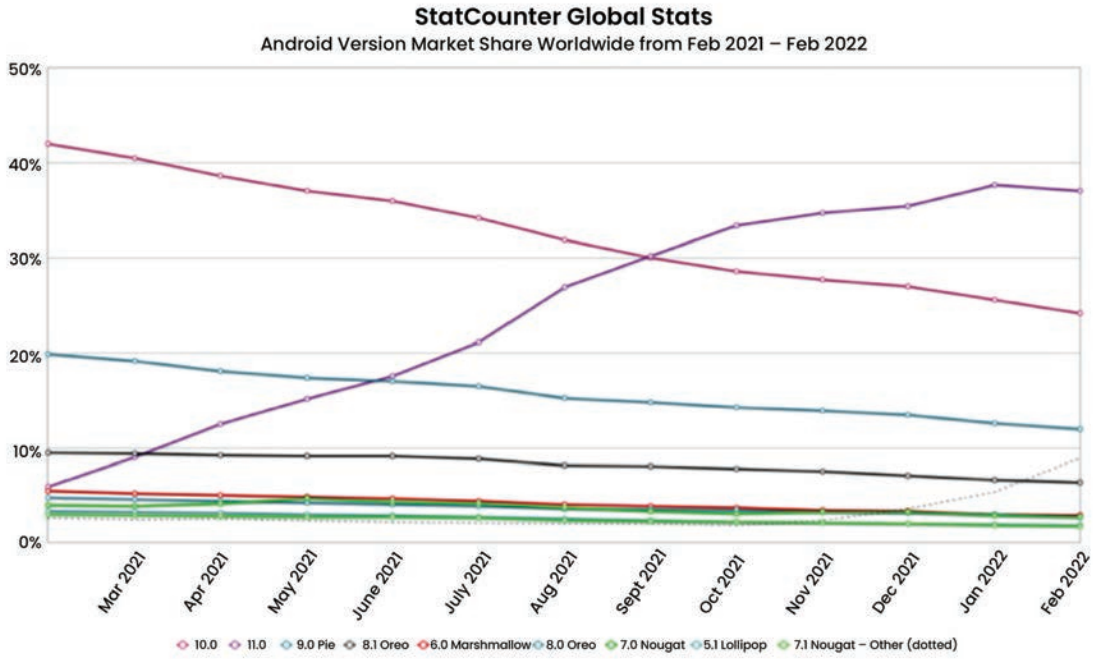

Figure 1.3-1. Android Market Share

The interception of consumer communications is often assisted by older technology. Nearly 32% of all Android devices are running older operating systems—which implies significant vulnerabilities and known weaknesses. Android malware is the most prevalent of all mobile devices, from Matryosh botnet DDoS malware to the recent FluBot malware, capable of capturing private user communications and data from the infected **device.**

The necessity to presume that endpoints are breached, but yet still provide a secure form of communications, is critical to the ongoing

evolution of business and technology. This also serves as the basis for the use of network monitoring mitigation methods such as non-attribution and obfuscation.

CONTINUITY CONCERNS

In November 2021, the largest ever recorded DDoS attack occurred, originating from over 10,000 sources from 10 different countries, resulting in a massive 3.47 Tbps attack. This was followed by two additional DDoS attacks in December, each of which was around 2.5 Tbps.

These attacks (in these cases, using UDP reflection) are relatively easy to execute with full botnets dedicated to providing DDoS-as-a-Service. The majority of enterprises, especially those in the small and medium business space, are not equipped to handle attacks of this magnitude. Most hosted or cloud-based web application firewalls and content delivery networks cannot contain a sustained multi-Tbps flood of traffic.

When we consider these recent DDoS attacks, it becomes clear that legacy incident management processes will no longer satisfy modern business requirements. Enterprise architectures must be more distributed and should implement mesh arrangements to enable leveraging of machine learning to rapidly adjust traffic routes to provide network paths to critical systems and services. We are long past the days when legacy, manually updated network routing resolution is sufficient for most companies.

NETWORK SECURITY IMPLICATIONS

As with any technological advancement, trying to shoehorn new concepts into legacy practices rarely works as effectively as expected. When we take a step back and look at the multi-cloud/multi-infrastructure environments most enterprises exist in now, trying to secure new cloud- and service-based applications with networking concepts born in the 1970s is akin to putting a Lamborghini emblem on a Yugo and expecting it to perform differently.

In today's enterprise, new approaches to network security are needed to safeguard the radically new everything-as-a-service application model. Two promising methods involve non-attribution, which helps reduce the likelihood that monitored traffic can be traced to the source, and obfuscation which provides a similar function to avoid the ability of an adversary to gain intelligence by tracking activity, network traffic, and day-to-day usage.

– II.–

THE NETWORK SURVEILLANCE THREAT: GOVERNMENT DEFENSE STRATEGIES

CHRISTOPHER R. WILDER, TAG CYBER

Every government knows that its ability to collect information through signals intelligence (SIGINT) has changed considerably. Where circuit-switched and satellite communications once reigned supreme in global network infrastructure, individuals and organizations now utilize IP-based networks, including the public internet, managed by service providers and mobile operators.

Monitoring such communications is now performed through traffic and activity monitoring using distributed collection. The means for mitigating such action cuts in two ways. That is, while one's own government might be exposed, such monitoring also allows defense, military, intelligence, and even civilian agencies to reduce their risk. Such best practices have typically not found their way into commercial use, but this is beginning to occur.

This article explains how government surveillance typically happens along with the most effective strategies deployed to avoid the consequences of such monitoring or surveillance. We offer a description of such a strategy at a broad level so that readers can interpret and tailor the approaches to their local situation. All methods presume that the target IP-based solutions are traversing the public internet, military networks, service provider networks, and mobile infrastructure.

It should be emphasized that significant risk has emerged for surveillance from hostile adversaries, as well as from governments and organizations performing such monitoring action routinely. Businesses, governments, and citizens are thus urged to take the time to learn how this is done—and the sections below are intended to support this objective.

MONITORING IP NETWORKS

In partnership with internet and telecommunications providers, US intelligence agencies have turned the domestic internet backbone into a collection point for the surveillance of bad actors and those who wish to harm the country. Initial collection programs focused on human-to-human communications, like email, photos, social media,

It must be understood, however, that encryption does not obfuscate the source of encrypted traffic and high-level analysis of traffic and routing flows can be done in the presence of encryption.

encrypted messaging services, and file transfers. Today, many intelligence organizations use data obfuscation to evade detection and firewalls when exfiltrating data from adversaries and bad actor networks.

Intelligence agencies install filters, back doors into the software, encryption-breaking keys, and secret court orders to gather data from foreign and domestic sources. The number of connected devices and the shift from a centralized workforce to a distributed one has allowed these agencies to expand their surveillance efforts to command and control assets (C2) and machine-to-machine communications. Using obfuscation, governments have been able to exfiltrate data from adversary and bad actor networks, often completely evading firewalls and detection tools.

The result is that governments have significant capability to monitor IP networks and the devices that live on these networks. This is true across the board, including for smaller countries with less funding for military teams, which means that our national competitors and adversaries can monitor the US, with all of the threats and vulnerabilities that entails. Developing an effective monitoring program does not require significant funding, so it is considered a valuable tool for national cyber offense and defense.

OFFENSIVE MONITORING MINDSET

By taking a "live-on-the-network" approach, the US DoD/intelligence community (IC) and other intelligence agencies can be proactive to protect and control information access. The military, intelligence agencies, and operations, including those responsible for the movement of personnel, material, and C2, have a low tolerance for adversarial monitoring and the threat of disruption or interference. They are highly motivated to deter committed and aggressive adversaries. The exploitation of cyber vulnerabilities undermines DoD's ability to operate and threatens national security and economic competitiveness.

Cryptographic-based technologies are at the core of protecting and sharing sensitive information across the government, and this has always been at the core of government avoidance of the monitoring threat. It must be understood, however, that encryption does not obfuscate the source of encrypted traffic and high-level analysis of traffic and routing flows can be done in the presence of encryption. Data owners and cloud providers deploy various methods and schemes to preserve the privacy of their data, but each encryption scheme has its vulnerabilities and poses a potential threat for data leakage. A holistic approach is needed to protect sensitive data; one that includes not just threat reduction, but countermeasures to prevent future leaks.

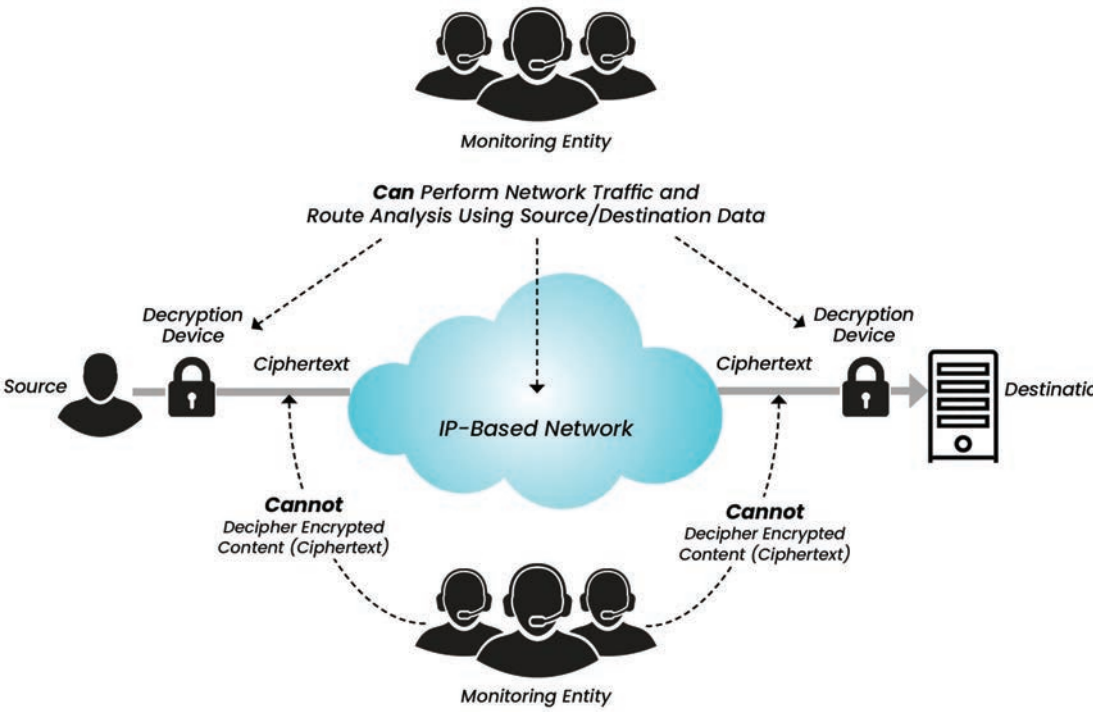

Figure 2.2-1. Traffic Monitoring in the Presence of Encryption

Throughout its lifecycle, the confidentiality and integrity of data (i.e., create, transmit, process, and store) is critical to maintaining overall trust in government systems. Continual modernization and strengthening of current communications and data integrity must keep ahead of adversaries' advances. The US government has begun to use advanced data deception and obfuscation techniques to ensure its personnel in the field remain uncompromised.

An effective offensive security posture requires a combination of human tradecraft, secure infrastructure policies, practices, and a strategy for responding to and mitigating risks before they happen.

SURVEILLANCE WITHIN GOVERNMENT

Government surveillance evokes the image of federal agents in the back of a van listening to people's private phone conversations or tracking their whereabouts. More commonly, the government uses digital or physical surveillance methods to identify and track bad actors and terrorists, break up counterfeit or money laundering organizations, and expose disinformation campaigns from hundreds of miles away.

Today's surveillance programs work to ensure real-time situational awareness when responding to public threats and collecting evidence in the event of an incident. Surveillance programs are not always nefarious, but organizations must also defend against these tactics to ensure the integrity of their sensitive information. Below are a few insights into how the intelligence community builds its surveillance programs.

ESTABLISH THE GOALS, METHODS, AND OBJECTIVES UP FRONT

Each initiative, system, or program must have specific goals and methods defined, whether offensive or defensive surveillance. These programs must be regularly reviewed with all stakeholders and have clearly defined goals. There is no argument that the IC indexes and stores information across all communications and internet activity that passes through a collection site. These agencies develop the insight to detect anomalous events and suspicious activity and enhance their SIGINT or open-source intelligence (OSINT) capabilities.

DATA COLLECTION AND STORAGE

All surveillance programs that involve data collection or transport should have clearly defined protocols for securing and transporting information to stakeholders. They must adhere to documented procedures and security controls for data collection.

DATA TRANSFER

Organizations should not transfer sensitive surveillance data unless it is necessary. However, if there is a need to move sensitive data, actions must adhere to agreed-upon methods such as data obfuscation, deception, sharing agreements, or smart contracts.

FOCUSED PLAN TO DEFEND "THE FORT"

From a defense perspective, there are four strategic focuses the DoD and IC have adopted to protect themselves. The US government is going through a transformation to ensure its infrastructure, workforce, endpoints, and sensitive data are protected as they defend against adversarial cyber bad actors. The IC and DoD are following several best practices; below are just some of the approaches they are taking:

- **Focus 1: Establish a Resilient Cyber Defense Posture –** Build a cyber-resilient defense posture that combines human tradecraft, architecture and engineering, and the delivery of new technologies and capabilities to support current information and communication platforms.
- **Focus 2: Build a Secure and Defensible Information Environment –** The DoD and IC are migrating to eliminate silos and share information across IT infrastructures, services, and intelligence capabilities. Because determined nation-state hackers consistently barrage the DoD/IC, it must maintain a high level of operational awareness. The DoD/IC can increase mission effectiveness and improve cyber defense efforts by sharing information amongst various agencies.
- **Focus 3: Practice Cyber Hygiene for Systems and Data Protection –** Cyber hygiene exists to create a secure environment that impedes the bad actor's ability to gain access, establish a presence, infiltrate

The use of technology to accomplish these objectives, including the deployment of techniques such as obfuscation and non-attribution will help operational teams achieve the desired reduction in risk of network monitoring and other offensive measures from an adversary.

deeper into the network, and attack or exfiltrate data. Understanding where to interrupt the intrusion to protect the data is critical to designing capabilities that harden and defend against an attack.

- **Focus 4: Strengthen Data Defenses –** Shoring up the confidentiality and integrity of information throughout its lifecycle (i.e., create, transmit, process, and store) is critical to maintaining end-user trust in DoD/IC systems. The use of multiple tools and technologies, including public key infrastructure, data obfuscation, and other cryptographic-based technologies, is already building a foundation for protecting and sharing information within DoD, the IC, its partners, and other agencies.

CONCLUSION

Implementing the above strategic imperatives requires a significant transformation within the DoD and IC. New processes, policies, and especially data protection technologies are already helping with discrete actions, information sharing, and reducing the data silos within the DoD and IC.

Executing these next steps will require a commitment to continued and increased cooperation and collaboration across the cyber community, including the intelligence, counterintelligence, and security partners, alignment of cybersecurity and defense strategies, plans, projects, and initiatives across DoD, and a DoD organizational construct that will foster the accomplishment of these objectives.

The use of technology to accomplish these objectives, including the deployment of techniques such as obfuscation and non-attribution will help operational teams achieve the desired reduction in risk of network monitoring and other offensive measures from an adversary.

– III.–

SECURITY APPLICATIONS OF NON-ATTRIBUTION AND OBFUSCATION FOR ENTERPRISE

ED AMOROSO,
TAG CYBER

Two strategies have emerged for avoidance of the risks of monitored communications. Each of the strategies (discussed below) has emerged in the context of complementary attempts by governments to use diplomacy to develop agreements on what can and cannot be monitored. As should be obvious to readers, such negotiations have not been successful at stopping governments and malicious actors from performing traffic and activity monitoring.

In response, government teams and related groups such as defense contractors and security vendors have identified non-attribution and obfuscation as being especially useful to avoid monitoring risks. While these methods have not yet found their way into conventional industrial deployments, they are being implemented in commercial platforms which will offer companies the opportunity to benefit from the control.

In this article, we explain non-attribution and obfuscation, and how they can be implemented in practice to significantly reduce the risks of monitored communications. The goal is to highlight how these methods work, not because practitioners will have to implement them directly, but rather to assist them in the review and selection of new commercial platforms that include these methods as components of their enterprise protection functionality.

WHAT IS NON-ATTRIBUTION?

The purpose of non-attribution is to ensure that access by users to some resource cannot be determined by network data. This includes assurance that source IP addresses cannot be linked to the originating device. Users such as businesses, government agencies, and even individuals might demand this requirement.

- **Accessed Resource –** Non-attribution prevents determination of the source device by an accessed resource (e.g., device with destination IP address).
- **Unauthorized Third-Party –** Non-attribution prevents external observation by a third-party to either perform unauthorized traffic analysis or to accomplish a hacking goal.

Government teams and related groups such as defense contractors and security vendors have identified non-attribution and obfuscation as being especially useful to avoid monitoring risks.

- **Authorized Third-Party –** Non-attribution does, however, prevent the determination of sources by authorized third parties such as law enforcement.

Hackers achieve non-attribution (to avoid being caught) through a technique known as spoofing, where they simply adjust their source IP address to some presumably unsuspecting dupe user. This has the effect of stamping their packets with that dupe's IP address. Certainly, this provides strong non-attribution, but it also blinds the actual originating hacker to the response data, such as the Synack packets in a TCP/IP connection (see Figure 3.1-1).

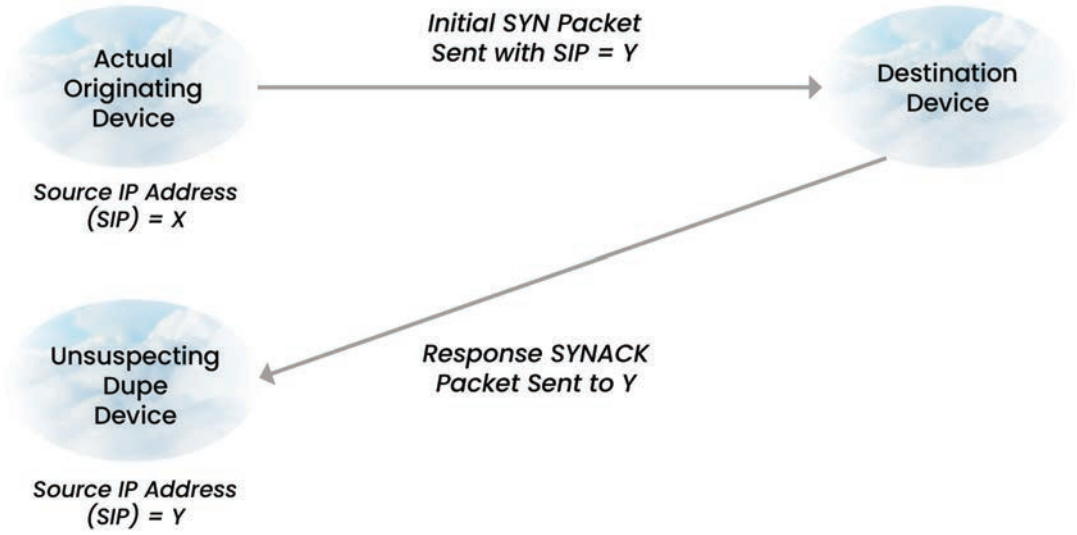

Figure 3.1-1. Concept of Non-Attribution via Address Spoofing Using IP

A preferred non-attribution approach would include this spoofing-type property but would also find some means for directing (or redirecting) the response data to the originator. This creates the technical challenge of determining how to hide the actual source while also exposing the actual source sufficiently to ensure that the originator can see the responses from the destination resource.

WHAT IS OBFUSCATION?

The purpose of obfuscation is to achieve the objective cited above; namely, to hide the details of an origination point, but to also preserve the capability for destination entities to respond to the source. This should also be done using a reliable mechanism versus hacking techniques such as guessing the details of a response (e.g., TCP sequence number prediction, as used by Kevin Mitnick in the 1990s).

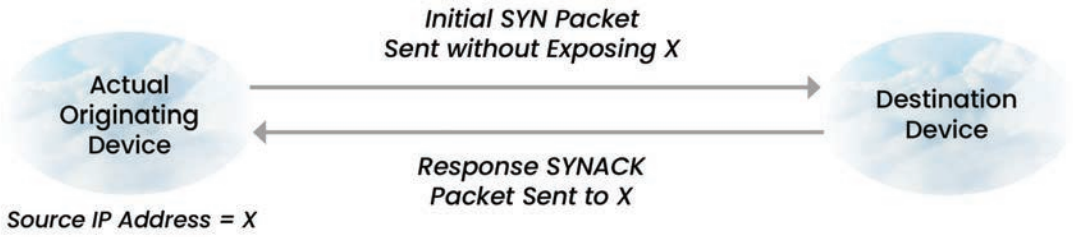

Figure 3.2-1. Illustrating the Goal of Non-Attributed Sessions Using IP

What is generally needed to achieve this objective is a scheme whereby the origination address is stored and remembered by some neutral intermediary which then hides this information from a destination point. This could be done by a centralized component, but that creates the possibility of the source data being coerced, leaked, or hacked. Instead, a scheme is required that provides both obfuscation and trust.

HOW ARE NON-ATTRIBUTION AND OBFUSCATION IMPLEMENTED?

The most common method for both non-attribution and obfuscation on the internet is the technique known as onion routing. Developed in conjunction with the goal to allow for anonymous internet surfing, the method creates a network that sits between a sender and receiver. The sender utilizes the onion network through an entry point, and the receiver notices requests from exit points.

Inside the onion-routed network is a series of intermediary nodes that collectively maintain sufficient information to pass requests from the entry to exit points, but that hide the details of the originator. Once the request leaves the onion network, the recipient only sees the exit point. This provides the type of capability exemplified by the popular Tor browser, which is used around the world for anonymous internet **browsing**.

The routing scheme in an onion network involves a stepwise unraveling. The source of the request first sends the "onion" to a router, which removes a layer of encryption to determine where it came from and where it should go next. It then sends the onion to the next router, which decrypts another layer to determine the next destination. This process continues until the last layer of encryption is removed the data is sent to the destination.

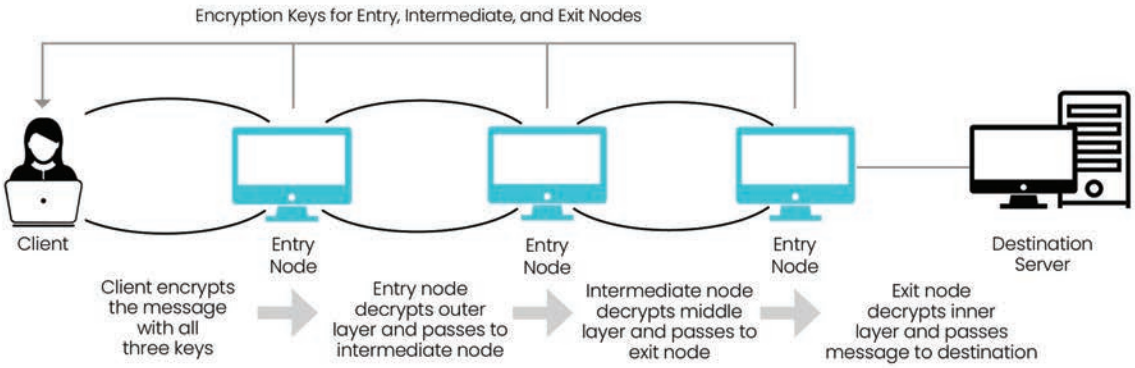

Figure 3.3-1. Onion Routing Scheme

This type of routing scheme results in an infrastructure-based solution for non-attribution and obfuscation. Specifically, a special network is placed between the client and destination to support the security objectives. Companies such as SecureCo are working to develop this type of capability to support business and government teams hoping to achieve this level of anonymity and security in their business communications.

Commercial development in onion routing, as with SecureCo, is spurred by the fact that while tools such as Tor have useful qualities, they are poor commercial solutions, generally with no QoS targets, an uncomfortable association with criminal activity, and often possessing many known vulnerabilities.

As a final note, it is worth mentioning that additional diverse tactics for obfuscation can be used to complement routing techniques. For example, engineers have long used dummy packets known as chaff which masquerade as encrypted data to defeat typical traffic analysis **methods**. This helps exemplify the types of engineering and design decisions that can be made to optimize non-attribution and obfuscation goals.

– IV.–

HOW DOES SECURECO'S PLATFORM PROTECT DATA NETWORKING?

ALEX HARRINGTON, SECURECO

The SecureCo data delivery platform for cloud or hybrid cloud environments creates a private subset of the internet for secure communications and data connections. Using an array of stealth techniques, including anonymization methods reclaimed from the dark web, SecureCo camouflages data-in-transit, making data blend inconspicuously with background noise and benign third-party traffic. Hackers cannot interfere with what they can't find.

The design purpose for the SecureCo offering stems from the growing risk of monitoring and surveillance from adversaries. The platform is designed to offer military-grade security with the flexibility of support and operations needed in the modern enterprise. The goal is to ensure that customers can continue to innovate and grow their business without the distraction of having to deal with unwanted traffic monitoring and associated threats to confidentiality and continuity.

In this article, we outline the salient aspects of the commercial SecureCo platform with emphasis on how it can be deployed into an enterprise network to address the risks of attribution and monitoring. A major goal is to address the threat of inappropriate behavioral traffic analysis, and this is addressed in the SecureCo offering through obfuscation measures that support secure networking and assurance of data-in-transit.

OVERVIEW OF PLATFORM FEATURES

To address the sophisticated nature of traffic monitoring threats, SecureCo has developed a software-defined transport protocol that combines multi-layered encryption, virtual circuit randomization, digital rendezvous, and decoy data-injection (chaffing) countermeasures to obfuscate client traffic as it traverses the internet. The platform includes support for various advanced security techniques, as outlined below.

- **Resilience –** The distributed mesh network architecture inherent in the SecureCo design provides redundant and region-spanning communications with rotating IP ranges and segments. This results in support for continuity, QoS, and DevSecOps agility. In addition, SecureCo supports a so-called moving target defense (MTD) which involves routing via random ephemeral circuits with a minimum of three direct routing hops.

- **Deception, Evasion, and Removal of Attribution –** Onion routing in the platform encloses data in multi-layer encryption, with one layer added for each hop, thus hiding sender/recipient attribution. Injection of decoy data (chaffing) is also used to disguise payload signatures and obscure data patterns. Finally, a virtual rendezvous system (patent No. 11,088,996) is employed to establish a connection without exposing endpoints.
- **Zero Trust and Additional Security Best Practices –** Zero trust is ascribed to network and application nodes to mitigate access breaches. FIPS-approved ECC and AES encryption algorithms are used for high performance, though modularity permits alternative algorithms (anticipating quantum resistance). In addition, core mechanisms and design principles already in place support least privileged access architecture (ZTNA).

SURVEILLANCE THREATS

The SecureCo architecture is designed to address activity monitoring threats by a surveillance entity. As illustrated in Figure 4.2-1, normal use of virtual private network (VPN) endpoints creates a surveillance exposure. Similarly, even with tunnels, there are signatures that can be recognized by a third party (e.g., existence or non-existence of communications). These threats require a solution that creates a means for enhanced privacy on the internet.

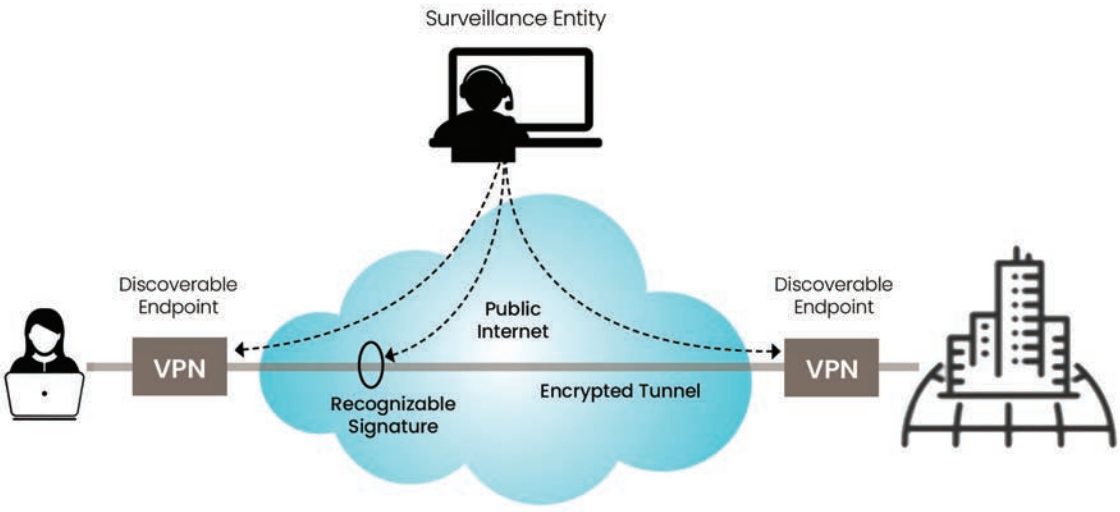

Figure 4.2-1. Surveillance Threats to VPN Usage

Implicit in this threat model is that the surveillance entity is performing unwanted, inappropriate, or even illegal monitoring of traffic and user activity. Where such monitoring is required or considered part of societal safety, it is reasonable for such entities (usually government) to coordinate with service providers, businesses, and users to ensure that sufficient means is available to obtain information about criminals and other bad actors.

Rather than relying on a point-to-point virtual tunnel across the internet, SecureCo instead creates a decentralized mesh network that includes many properties supporting non-attribution and obfuscation to reduce the unwanted monitoring risk.

SECURECO ARCHITECTURE

The SecureCo architecture is easily depicted in the context of the existing VPN threat model expressed above. The idea is that rather than relying on a point-to-point virtual tunnel across the internet, SecureCo instead creates a decentralized mesh network that includes many properties supporting non-attribution and obfuscation to reduce the unwanted monitoring risk.

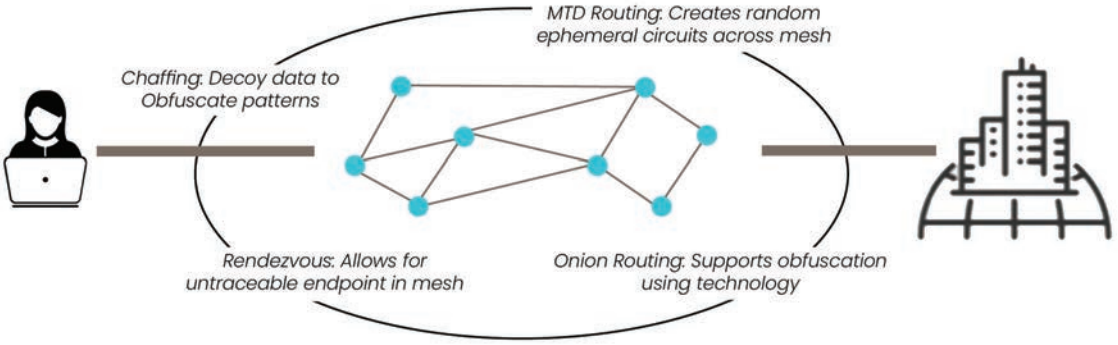

Figure 4.3-1. SecureCo Platform Deployment

It should be evident from the diagram that the secure mesh requires a special routing protocol that is multi-path and multi-region. In addition, the endpoints must be obfuscated using rendezvous points that have some commonality with how Tor entry and exit nodes are implemented. In addition, a randomization method is used to route using moving targets (see below) to implement ephemeral circuits between endpoints across the mesh.

BENEFITS OF THE PLATFORM

The resiliency benefits of routing over a mesh versus a point-to-point connection are well documented. SecureCo utilizes a technique known as random ephemeral MTD routing, which makes the transmission harder to find, increasing the burden of network compromise for a threat actor. The platform's redundant network is resistant to attack, providing mitigation by automatically reestablishing communication paths to exclude compromised nodes. As the outer layer of protection, SecureCo serves as a leading edge for denial-of-service defense.

SecureCo's patented virtual rendezvous redefines how connections are established. Instead of the traditional session establishment from source (point A) to destination (point B) endpoints, points A and B negotiate a random location or rendezvous (point C) in which to make the connection. This approach protects endpoints by cloaking or misattributing their actual IP addressing.

BENEFITS OF THE PLATFORM

The resiliency benefits of routing over a mesh versus a point-to-point connection are well documented. SecureCo utilizes a technique known as random ephemeral MTD routing, which makes the transmission harder to find, increasing the burden of network compromise for a threat actor. The platform's redundant network is resistant to attack, providing mitigation by automatically reestablishing communication paths to exclude compromised nodes. As the outer layer of protection, SecureCo serves as a leading edge for denial-of-service defense.

To remove source/destination data attribution, SecureCo's routing protocol leverages technology elements also found in Tor (The Onion Router) open-source privacy network. Tor has proven to be effective at preserving anonymity, though its association with criminal activity and certain key vulnerabilities have made Tor undesirable for commercial use. In contrast, SecureCo's implementation of onion routing de-attribution provides an elevated security posture by enabling identity suppression for operators seeking concealment of their network activity or location.

An additional security risk is discovery of attributable data-in-transit, which can lead hackers to vulnerable endpoints, resulting in disruption or penetration. Hackers who seek to intercept data from high-value targets over open networks or access points are thwarted if the target's data is anonymized. SecureCo provides anonymity assurances based on rigorous mathematical algorithms that consistently inform the scale, sustained bandwidth demand, and deployment architecture of the network.

Chaffing is another critical capability, since even anonymized and secure data can be intercepted or blocked if it can be distinguished from ambient "normal" internet traffic. The injection of secondary data into the transmission itself makes it much harder to detect a signature pattern, permitting secure streams to blend in as benign and pass undetected to hostile observers. In addition, injection of decoy data makes the ebb and flow of communications harder to observe, flattening out operational security spikes.

USE CASE EXAMPLES

SecureCo's sophisticated mesh network solution delivers hyper-secure and anonymous communications, providing digital low probability of intercept/detection across untrusted network environments. SecureCo's ability to obfuscate data routing and attribution makes the solution appropriate for a range of government, industrial, and commercial applications, as outlined in the list below:

- **Secure Remote Access & Mobility –** Our mesh-network-routed, software-defined tunnel provides a supplementary protective layer for TLS or replacement for VPNs. Easy integration while adding obfuscation, resilience, and security.

Now, nation state adversaries are targeting enterprise, non-nation-state threat actors have increased in sophistication and aggression, and the ability to observe network activity from the outside exposes attack vectors.

- **Critical Infrastructure –** Protects the resilience and integrity of SCADA and OT systems by anonymizing and hiding data flow using multi-path and multi-layered encryption. Shields infrastructure from interference, disruption, and ransom attacks reducing potential downtime or outages.
- **Private or Clandestine Communications –** Conceals data channels to avoid disruption, preventing leakage of identity and geolocation of interlocutors, and thwarting data capture or tampering. Allows critical communication flows to evade and penetrate into global regions many other solutions cannot.
- **IoT and Embedded Systems –** Protects low security endpoints and prevents intrusion by unauthorized devices. Small software footprint operates on low-power, inexpensive, and disposable hardware.
- **Protection of Ultrasensitive Data Flow –** Added privacy and confidentiality for sensitive IP, healthcare PII, financial information, or any data flows for which interruption or tampering is very costly (e.g., supply chain).

ONGOING TRENDS IN NON-ATTRIBUTION

First adopted in military and intelligence contexts, where the nation state adversaries have traditionally been the most sophisticated and aggressive, the stakes are literally life and death, and protecting identity and anonymization have first order benefits. However, now, nation state adversaries are targeting enterprise, non-nation-state threat actors have increased in sophistication and aggression, and the ability to observe network activity from the outside exposes attack vectors.

Even when concealing personal identities is less critical (e.g., machine to machine communications), removing attribution from data-in-transit purposefully conceals the identity of the sending and receiving network assets (effectively anonymizing them), which can help reduce targetability and diminish attack surface.

Furthermore, the ability to find, identify, observe, capture, reroute, block, or otherwise interfere with data-in-transit supporting critical operating or business activities can lead to catastrophic downtime or even worse, data and network breaches. The SecureCo team is witnessing commercial adoption in a number of areas: critical infrastructure, industrial controls, financial services, and healthcare.

– V.–

HOW CAN ENTERPRISE PUT SECURECO INTO PRACTICE?

ERIC SACKOWITZ,
SECURECO

The SecureCo platform can serve as a replacement or added layer of protection over current or legacy systems, providing depth and diversity of defense. It is built from the ground up to support multiple types of implementations, architectures, and use cases. Such layered protection encompasses everything from network and multi-site campus implementations to application-specific integrations, IoT, and secure mobility and remote access.

In this article, we outline some considerations to address when deploying the SecureCo platform to a live network environment. We focus on practical integration methods, along with guidance on security compliance. A high-level action plan is proposed to deploy SecureCo into an environment that requires non-attribution and obfuscation to avoid unwanted traffic monitoring and network surveillance, and the risks associated with these activities.

INTEGRATING SECURECO INTO A SECURITY PROGRAM

Network reconnaissance and traffic analysis are typically overlooked in security plans because adversaries perform these actions without the victim organization's awareness. When a downstream attack occurs, it's nearly impossible for the victim organization to replay and then understand their inadvertent exposures and leaks that revealed the actual cyber attack vectors.

Preventive measures are optimal for network and business well-being but are hard to assess from an efficacy or return on investment (ROI) point of view. For example, it is impossible to determine how many attacks would have succeeded without preventive measures. As a result, more focus is typically placed on reactive measures, such as detect and respond, which minimize damage from intrusions. Though it may not prevent damage, the direct feedback from the detection and response measures can still provide an ROI.

INTEGRATING SECURECO INTO A COMPLIANCE PROGRAM

Regardless of industry, cyber security controls and minimum requirements for most compliance frameworks, whether governed by NIST or other regulatory bodies, overlap significantly. The Venn diagram focuses on key areas of internal security policies and controls, data integrity, redundancy, accountability, authorization, access, and quality assurance. Encryption

is at the heart of most cyber compliance programs, including data storage, transmission, and access which extends to physical, virtual, and application resources. Unfortunately, the minimum regulatory policies have yet to catch up to the heightened cyber defense posture necessary to thwart current and evolving threats.

SecureCo integrates into an existing compliance framework and exceeds policy and regulatory controls for most industries. In the more heavily regulated and pivotal industries, like medical, pharmaceutical, financial, legal, law enforcement, and critical infrastructure, SecureCo provides extra layers of benefits unique to supporting those operations. For example, patient data in clinical trials requires anonymizing PII, along with the demands of HIPPA and COPA. Similar requirements exist for GDPR, CCPA, and PCI in financial transactions.

PILLARS OF ZERO TRUST SUPPORT

The same large companies that have been part of the past problems are now claiming to have new solutions for zero trust, and yet are not addressing all of the fundamental requirements of a modern cyber security stack. That stack should minimally focus on three primary pillars:

- **Operational Security –** This involves stealth networking and obfuscation.
- **Least Privileged Access –** This includes support for zero trust network access or least privileged access.
- **Monitoring –** This is comprised of behavior monitoring with detect and respond solutions.

SecureCo has the first two of these requirements covered and is integrates with the third. This does not negate the fact that all enterprises should have good cyber hygiene within their IT organization, which includes password management, two-factor authentication on applications, inventory management, and employee use policies and enforcement.

ACTION PLAN FOR ENTERPRISE

The action plan for the enterprise should be based on a comprehensive risk assessment—one that answers the following questions:

- **Outage –** What is the cost of breach or downtime?
- **Threat –** Do we place a high premium on privacy, identity, or data?
- **Communications –** Do we see a growing reliance on data communications?
- **Applications –** Do we develop applications or provide services that contain sensitive/critical data or command and control capabilities to their operation or consumers of their technology?

- **Regulation –** Does regulation impose security requirements and/or greater costs to remediate breaches?
- **Posture –** What is our cybersecurity posture today and what gaps might exist with regards to the primary pillars and cyber hygiene mentioned above?

Also, there should be a budget check focused on what the organization now spends on cyber security. For example, the SecureCo CONNECT solution can replace certain existing infrastructure (e.g., VPN) to minimize budget impact. This allows enterprise teams to ensure that their budget allocation is commensurate with the current increased threat levels.

SecureCo can help enterprises assess and recommend a response/action plan, which will likely include more than just SecureCo solutions. The team also operates a partner network that can assist. Additionally, SecureCo has a flexible Pilot Program that allows customers to trial SecureCo CONNECT for up to 60 days.

ABOUT TAG CYBER

TAG Cyber is a trusted cyber security research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 100 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth Research as a Service (RaaS), market analysis, consulting, and personalized content based on hundreds of engagements with clients and non-clients alike—all from a former practitioner's perspective.

ABOUT SECURECO

SecureCo creates the most secure internet connections possible, addressing a critical gap in existing cyber security solutions. Our patented stealth technology protects networks and transmissions from interference and disruption, powering resilient data links, secure applications, and end user privacy. SecureCo offers a next generation replacement or augmentation for legacy VPNs while extending zero trust principles to data transport, cloaking data exchange, services, and assets to reduce network attack surface and targetability. Trusted by some of the most demanding cyber security customers in the world, we deliver high performance, exceptionally secure data transit for military, intelligence, industrial and commercial applications.

IMPORTANT INFORMATION ABOUT THIS DOCUMENT

Contributors: Edward Amoroso, John Masserini, Christopher R, Wilder, Alex Harrington, Eric Sackowitz.

Publisher: TAG Cyber LLC. ("TAG Cyber"), TAG Cyber, LLC, 45 Broadway, Suite 1250, New York, NY 10006.

Inquiries: Please contact Lester Goodman, (lgoodman@tag-cyber.com), if you'd like to discuss this report. We will respond promptly.

Citations: This paper can be cited by accredited press and analysts but must be cited in context, displaying the author's name, author's title, and "TAG Cyber". Non-press and non-analysts must receive prior written permission from TAG Cyber for any citations.

Disclosures: This paper was commissioned by SecureCo Inc.. TAG Cyber provides research, analysis, and advisory services to many cybersecurity firms mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.

Disclaimer: The information presented in this document is for informational purposes only and may contain technical inaccuracies, omissions, and typographical errors. TAG Cyber disclaims all warranties as to the accuracy, completeness, or adequacy of such information and shall have no liability for errors, omissions, or inadequacies in such information. This document consists of the opinions of TAG Cyber's analysts and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice.

TAG Cyber may provide forecasts and forward-looking statements as directional indicators and not as precise predictions of future events. While our forecasts and forward-looking statements represent our current judgment and opinion on what the future holds, they are subject to risks and uncertainties that could cause actual results to differ materially. You are cautioned not to place undue reliance on these forecasts and forward-looking statements, which reflect our opinions only as of the date of publication for this document. Please keep in mind that we are not obligating ourselves to revise or publicly release the results of any revision to these forecasts and forward-looking statements considering new information or future events.

Copyright © 2022 TAG Cyber LLC. This report may not be reproduced, distributed or shared without TAG Cyber's written permission. The material in this report is composed of the opinions of the TAG Cyber analysts and is not to be interpreted as consisting of factual assertions. All warranties regarding the correctness, usefulness, accuracy or completeness of this report are disclaimed herein.