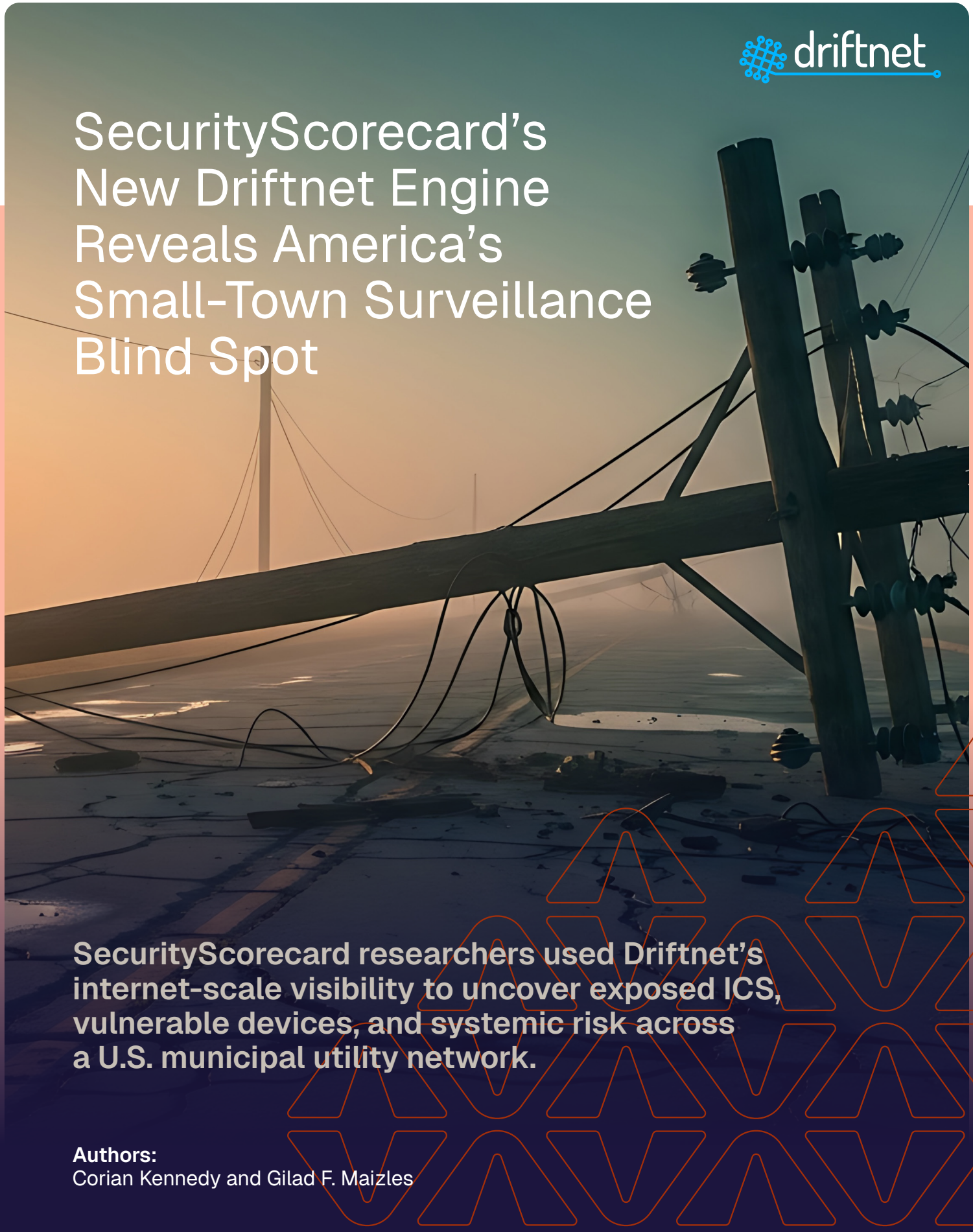
SecurityScorecard

REPORT



SecurityScorecard's New Driftnet Engine Reveals America's Small-Town Surveillance Blind Spot

SecurityScorecard researchers used Driftnet's internet-scale visibility to uncover exposed ICS, vulnerable devices, and systemic risk across a U.S. municipal utility network.

Authors:
Corian Kennedy and Gilad F. Maizles

Turning Internet-Scale Visibility Into Actionable Intelligence

Executive Summary

SecurityScorecard researchers used Driftnet's internet-scale discovery capabilities to analyze the network footprint of a small U.S. municipal utility provider that also operates as the town's internet service provider (ISP). The investigation identified widespread exposure across internet-facing systems, including vulnerable surveillance equipment, exposed Industrial Control Systems (ICS), weak encryption configurations, and End-of-Life (EoL) Windows devices.

The utility provider operates its own Autonomous System (AS), meaning internet connectivity and critical infrastructure services exist within the same broader operational environment. This convergence creates a concentrated point of failure where disruption to one service can affect others across the community.

Over a six-month period, Driftnet identified 1,498 services across 692 IP addresses. Of those, 446 IPs (64%) exhibited at least one technical issue that increased exposure risk. SecurityScorecard's Driftnet engine identifies 150% more internet-facing services than previous scanning methodologies, uncovering exposures traditional approaches miss. Findings included:

- **30 instances of Dahua and Hikvision surveillance equipment inside the entire footprint of the utilities AS.** Banned internet protocol (IP) cameras could enable Man-in-the-Middle (MitM) attacks, Distributed Denial of Service (DDoS) attacks, malware-based campaigns, and more.
- **Exposed ICS, SCADA, and OT-related services** directly reachable from the internet. At least three /24 clusters hosting ICS or IOT services and consumer devices on the same broadcast domain.
- **Weak or misconfigured encryption across 382 IP addresses**, in addition to cleartext FTP and HTTP and unrecognized Certificate Authorities.
- **EoL Windows hosts reachable via Server Message Block (SMB) and NetBIOS.** A relic from the past, rarely ever makes an appearance outside of OT environments.
- **25 Known Exploited Vulnerabilities (KEVs)** identified across internet-facing services.
- **Convergence of a utility and ISP creates a single point of failure.** Power delivery and internet reside on the same AS. Incidents on one impacts the other.

The research also identified multiple network segments where consumer-grade devices, surveillance systems, and ICS-related technologies operated within the same local network environment. This lack of segmentation increases the likelihood that compromise of a lower-security system could enable lateral movement toward operational infrastructure.

Inside America's Small-Town Infrastructure Exposure Problem

In many small U.S. towns, a single utility network supplies both electricity and high-speed internet to the community. In one such town — whose identity we have withheld to protect their security — the same network serving tens of thousands of residents shows dozens of exposures that increase risk to both the infrastructure and the people who depend on it, according to new research from SecurityScorecard.

The town's utilities provider runs its own fiber, its own AS, and its own peering with the global internet. It's the ISP and it's the power company. This convergence creates a concentrated point of failure, where a disruption could impact both connectivity and power delivery across the region. The lack of segmentation and external dependencies increases the likelihood of cascading outages and limits the ability to contain incidents.

This investigation draws on intelligence from SecurityScorecard's recent acquisition of Driftnet, revealing previously unreported exposure paths and systemic weaknesses that increase the risk of a material incident.

In this demonstration of Driftnet's capabilities and data collection, we pulled data associated with the entity and found 1,498 unique services across 692 unique IP addresses, over the period of six months. Observational data was expanded to include all parameters, covering software, firmware, and hardware vendor and series specifications and classification. We also cover severity of vulnerabilities, detectable versions, and configurations of internet-facing software.

Out of 1,498 detected services, Driftnet's comprehensive attack surface visibility enabled us to reveal several alarming exposures, from banned internet protocol (IP) cameras that could enable Man-in-the-Middle (MitM) or malware attacks, to clusters of exposed ICS, SCADA, and other OT-specific technologies sitting alongside misconfigured services. There is an overarching theme of limited visibility into exposure, insufficient implementation of security controls around critical assets, and blind spots across the wider attack surface.

This is not a problem unique to this one small town, but this town stood out in our analysis, because out of 700 static IP addresses detected in their footprint, 446 IPs (64%) presented at least one technical issue that could expose the network to anything from covert espionage to a destructive attack that may cost lives.

When the entire municipal and private infrastructure depends on the same AS, intranet segmentation and concrete security policies are no longer a nice-to-have, but rather a high priority goal. Maintaining them may very well be the difference between a localized security incident and a town-wide shutdown or worse. Below are the main findings of our report, derived directly from Driftnet's attack surface detection engine.

What Driftnet Revealed Across the Attack Surface

Banned IP Cameras And Surveillance Equipment: A Multi-Layered Threat

Within the footprint of the utilities provider, 30 unique instances of Dahua or Hikvision cameras and DVR surveillance equipment have been reported on Driftnet. Both vendors are Chinese state-owned surveillance tech giants, and as of 2020 are effectively banned in the U.S. due to security risks. (The ban was initially limited to government contracts under the National Defense Authorization Act (NDAA) 899 compliance requirement, but later the Federal Communications Commission (FCC) expanded the restrictions.)

Most IP cameras are not designed with strong cybersecurity controls in mind and often ship with minimal built-in protections. Driftnet's scanners currently track over 257,000 instances of vulnerable IP cameras around the world (see the query here). As for the banned vendors themselves, Driftnet detects more than 156,000 instances of vulnerable Dahua or Hikvision devices (not only cameras) worldwide. But vulnerabilities only represent a potential window for entry and not the intention behind the intrusion.

In our examination into the town's utility provider, these devices present a multi-layered threat. A hacked camera of this kind is a visual surveillance tool in the hands of a threat actor. It is also an internet device capable of listening and sending data within the boundaries of the town's AS. This means attackers may leverage it for Man-in-the-Middle (MitM) attacks or Distributed Denial of Service (DDoS) attacks by simply leveraging its native capabilities, such as listening to or generating network traffic.

IP cameras are also equipped with small CPUs, which are capable of running lightweight web servers and commonly used for their interface panel. This makes them a potential candidate for a localized deployment of lightweight malware and perhaps even Command and Control (C2) servers.

We have seen this kind of campaign occur with several botnets and Operational Relay Box (ORB) networks in the past, such as the China-nexus LapDogs ORB, which SecurityScorecard's STRIKE research revealed last year, among others.

Each of these characteristics makes IP cameras an attractive target for threat actors. However, they are rarely the end goal. In many cases, they serve as an entry point into the internal environments of critical infrastructure, enabling deeper access for disruption, surveillance, or espionage within Operational Technology (OT) systems.

ICS/OT Systems Exposure: The Bad, The Worse, And The Ugly Truth

ICS and Supervisory Control and Data Acquisition (SCADA) — both part of the broader classification of OT — represent high-risk targets due to their commonly rudimentary firmware architecture that leaves them susceptible to relatively simple attacks.

They are also a prime target for attackers due to the operational impact that can result from compromise. Look no further than the STUXNET attack on Natanz, Iran's enrichment facility, to see what attacks on these systems may lead to in sensitive environments.

Because of that very risk, critical infrastructure is heavily regulated (see the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Act of 2022 here) and requires reporting of incidents directly to the Cybersecurity and Infrastructure Security Agency (CISA). CISA's advisories for OT serving critical infrastructure environments and SP 800-82 Rev. 3 guidelines for industrial OTs both recommend preventing ICS, SCADA, and other OT-specific technologies from being exposed directly to the internet.

In the case of the U.S. town this research covers, Driftnet detected 13 unique instances where services associated with said technologies were directly exposed, and not even sitting behind a firewall or router to provide and enforce basic security policies.

This OT exposure already represents a significant level of risk. However, the risk increases when you look at how these systems sit next to each other on the same network. By grouping the entire footprint of the utilities AS into ranges and /24 subnets, we found more than one instance where a mix of systems and services should have never shared the same subnet environment.

On one address, a host answers on port 25565 with a private Minecraft server, while a Hikvision camera runs on port 8310. Just a few clicks away on another IP within this range, a MACH-ProWebSys building controller runs BACnet service on UDP port 47808. This combination highlights the absence of effective network segmentation between consumer, surveillance, and operational systems: A banned camera, a sensitive control system, and tens of other services. Same broadcast domain. Same ARP table.

These systems are all operating as if they are part of the same internal network. They can see and communicate with each other directly, without the protections typically applied to external traffic. This setup creates additional attack paths that would not exist if these systems were properly segmented, allowing a compromise in one system to more easily spread to others — including critical infrastructure.

Across the footprint, we were able to detect three different /24 clusters hosting both exposed ICS/OT-related services alongside vulnerable or misconfigured services and devices, two of which also include a Hikvision and a Dahua IP camera or DVR. If a malicious threat actor compromises the camera, the attacker doesn't have to bypass a perimeter firewall to reach the PLC. There's no perimeter to bypass. The pivot is a Layer 2 walk.

We also observed a large amount of End-of-Life (EoL) Microsoft Windows terminals, detected via exposed SMB and NetBIOS services, which are deprecated communication protocols. Driftnet detected over 140 enabled and active services across the AS. While not necessarily OT, EoL Windows terminals are commonly found in such environments and used as physical terminals to control industrial devices. They are also frequently used as terminals for medical devices such as MRI machines or X-ray scanners.

If these terminals connect to an industrial machine or medical equipment, a compromise could have severe consequences affecting public safety and health. Exposing them directly to the wide internet — especially without a firewall or router to mask them — significantly increases risk of compromise.

Old, Outdated Or EoL Devices: A Hacker's Treasure Trove

Shifting our view to the wider footprint of the utilities provider, Driftnet's scans detected significant security risks characterized by widespread exposure of vulnerable services and misconfigured devices.

Across all findings, weak, permissive, or expired encryption configurations are a primary concern, with 382 unique IP addresses exhibiting encryption misconfigurations. Driftnet observed the use of cleartext protocols including FTP and HTTP without TLS, which leaves data vulnerable to interception, eavesdropping, or tampering. It also surfaced unrecognized certificate authorities or flat out self-signed certificates, which are both untrustworthy. This is particularly prevalent in VPN & Remote Access (67 IPs) and the aforementioned IP Cameras and Surveillance (37 IPs) categories.

The Driftnet data also identifies unmitigated vulnerabilities across 121 IPs, with 25 instances of KEVs, primarily concentrated in Web Servers and Applications. This risk is compounded by the presence of exposed smart home and small office devices, including 25 Internet of Things (IoT) devices and embedded devices as well as 21 media and entertainment systems (such as smart TVs and streaming devices).

The combination of known exploits and poor encryption on these consumer-grade and small office devices creates a broad attack surface for this town.

When Exposure Becomes Systemic Risk

How Internet-Scale Visibility Exposes Hidden Infrastructure Risk

This case goes beyond individual risk factors for each device and service — it effectively reverts the premise of "defense in depth" on its head. When the entire perimeter and ecosystem surrounding the critical infrastructure is vulnerable, it creates conditions for sustained, multi-stage compromise across entities.

A capable threat actor will exploit the weaknesses, slowly compromising endpoints surrounding the OT, setting traps, establishing footholds and redundancies, intercepting communications, collecting credentials, and studying the entire ecosystem for potential future exploitation. By the time impact occurs, there will be very little left to do to effectively stop them.

This is why organizations need to secure and continuously monitor externally exposed systems — not just their core infrastructure and "Crown Jewels." Without a threat-informed approach to monitoring and remediation, isolated exposures can evolve into systemic risk across the broader supply chain.

The Complexity of Internet-Exposed Infrastructure

This is the part most reporting misses. This utilities provider runs its own AS. So do several other cities and towns. So does most every state that has a municipal broadband authority. They peer directly. They originate their own routes. There is no upstream provider to escalate to and no network operations center (NOC) at Comcast or AT&T to call when something goes wrong.

In many cases, responsibility is highly concentrated. The disclosure path, the remediation path, the crisis contact, the network operator, and (in many cases) the person who runs the power grid are the same human being, often working out of the same building. The same individual or small team manages network operations, incident response, and critical infrastructure systems.

When an exposed programmable logic controller (PLC) appears in this environment, the challenge is not identifying who to contact — it is whether the responsible party has the capacity, incentive, or support to act quickly.

Inside The Methodology

Driftnet observes more than 4.1 billion IP addresses globally. The utility sample analyzed over six months for this research serves as a proof of concept, not a complete view of the problem. The broader risk becomes clear when applying the same methodology across all municipal broadband networks in the United States.

By using Driftnet's rich variety of data points, including geolocation, open source registration or tacit ownership indications given by scanned services, it is possible to narrow the search to specific municipalities across the country and assess their individual security posture and susceptibility to cyber attacks.

Based on the patterns observed in this case study, similar exposures are likely present across this broader set. The remaining question is not whether these risks exist, but how widespread and severe they are.

From Exposure Discovery to Threat-Informed Defense

One town is an isolated case. The same pattern across hundreds of municipal utilities represents a systemic infrastructure risk — one that remains largely unmitigated.

The exposed cameras are not the root issue. Their presence is an indicator. They signal broader weaknesses across externally exposed systems, where critical assets such as ICS often sit nearby without adequate segmentation, monitoring, or escalation pathways. These conditions increase the likelihood of undetected exposure and delayed response.

Until now, this level of visibility has been difficult to achieve at scale. With the acquisition of Driftnet, SecurityScorecard can identify these exposures across the global internet in real time, uncovering hidden infrastructure risks that traditional approaches miss. The acquisition will bring Driftnet's high-fidelity internet discovery engine into SecurityScorecard's TITAN AI platform, giving Third-Party Risk Management teams, Security Operations, and threat hunting teams the real-time intelligence they need to find and fix risks before attackers exploit them.

This is the shift from isolated findings to actionable, systemic insight.

To learn how Driftnet-powered intelligence can help you identify and reduce exposure across your ecosystem, visit securityscorecard.com or request a demo.

Discover how SecurityScorecard can identify and reduce exposure across your system.

Explore Internet Intelligence at SecurityScorecard.

SecurityScorecard

Securing the world's supply chains