COMCAST
BUSINESS

2025
Comcast Business Cybersecurity Threat Report

Table of Contents

Foreword

By Noopur Davis

Executive Vice President, Chief Information Security and Product Privacy Officer, Comcast

The cybersecurity environment we face in 2025 is unlike any that has come before. Threats are growing in scale, stealthiness, and sophistication. But this is also a transformative time for cyber defense, with advances in AI, automation, and industry collaboration opening new opportunities to innovate.

Technology is a defining factor in this landscape. Artificial intelligence (AI), in particular, is reshaping the cyber battlefield by introducing not only new risks, but also powerful tools for defenders to outpace their adversaries. Yet even with these advances, one reality remains unchanged: people make the difference. Skilled professionals are essential to interpret subtle signals, investigate anomalies, and make rapid decisions when an incident unfolds. People, paired with advanced technology, are what ultimately determines resilience.

At Comcast, we are in a unique position to see what many others cannot. Our visibility spans across vast residential and business networks, giving us early insights into the trends and tactics shaping today's threat landscape. This perspective strengthens our defenses and directly informs the services we deliver through Comcast Business. By combining multi-layered security solutions with deep security operations center (SOC) expertise, we help organizations simplify complexity, extend their capabilities, and respond with confidence in a high-stakes environment.

This cybersecurity threat report is the product of that commitment. It distills learnings from billions of real-world events, advanced analytics, and cross-industry intelligence to provide decision-makers with actionable insights on where to focus their defenses. The goal is not just to inform, but to empower leaders with a clear view of current risks and opportunities, so they can focus effort where it matters most and build stronger, more resilient organizations.

My call to you is simple: use the insights in this report to strengthen defenses, rethink risk, and embrace partnerships. Cybersecurity is a collective effort. By working together, we can not only stay ahead of the threats but also harness innovation to protect what matters most.

Executive Summary

In 2025, enterprise leaders find themselves operating in a global threat landscape characterized by accelerating scale and sophistication.

As adversaries weaponize artificial intelligence, double down on exploiting human trust, and adopt more sophisticated evasion tactics, the traditional calculus for managing enterprise risk is being fundamentally rewritten. Business and technology leaders are now tasked with defending an expanding attack surface against threats that are greater in volume and attackers that are more adept at blending in with normal business activity.

This report draws from the analysis of 34.6 billion cybersecurity events Comcast Business detected from June 1, 2024 through May 31, 2025 across its cybersecurity customers. It provides data-driven intelligence on how the tactics used by cyber adversaries are evolving, alongside the advanced strategies and technologies organizations can deploy to counter them. Ultimately, this report equips leaders with the intelligence needed to better assess organizational exposure, anticipate adversary evolution, and proactively adapt defenses.

The numbers presented throughout the report represent the collective and anonymized data of customers leveraging Comcast Business security offerings, including distributed denial of service (DDoS) mitigation, endpoint detection and response (EDR), vulnerability scanning and exposure management, managed detection and response (MDR), and other services. Our internal data, mapped to the MITRE ATT&CK® framework, is complemented by industry research, insights from our vendor partners, and the expertise of Comcast's security product, threat intelligence, and operations teams.[1] This comprehensive perspective provides a well-rounded analysis of the direct threats we see, the trends shaping the cybersecurity landscape, and the business and risk implications for enterprise leaders.

[1] ©2025 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.

Agentic AI, large language models (LLMs), proxy-based infrastructures, and other technologies are expanding the attack surface in new ways. AI is lowering the barrier to entry for attackers, and enterprise adoption of AI and shadow AI use by employees creates new blind spots in identity and access management (IAM). Proxy abuse and attacker-controlled infrastructure further amplify risk by disguising malicious traffic.

Our analysis reveals adversaries that are smarter, faster, and more resourceful than ever, mounting high-volume phishing and drive-by compromise campaigns, exploiting "living-off-the-land" (LOTL) techniques, and deploying increasingly sophisticated DDoS attacks. Fortunately, defenders are hard at work, too. They're innovating new tools to prevent and respond to attacks—and combining the power of technology with human expertise to weed out intruders who may be hiding in plain sight. The role of people remains central to cybersecurity, from expert analysts who uncover weak signals in vast streams of data to employees whose awareness and vigilance, or lack thereof, can either stop attacks before they escalate or represent the weakest link in defense.

Organizations must adopt a multi-layered, adaptive security strategy that blends preventative and responsive measures. Prevention remains critical—strong patch and vulnerability management, secure email and web gateways, posture management, and phishing-resistant multifactor authentication (MFA) can block many threats before they reach users. But since some intrusions will inevitably get through, success also requires advanced detection, behavioral analytics, AI-driven automation, and expert-led threat hunting to contain them quickly. Aligning these capabilities to the organization's most critical business risks, and reinforcing them with a culture of resilience, helps leaders reduce exposure and adapt defenses with confidence.

Threats are becoming smarter, faster, and harder to detect.

Security teams and end-users face mounting pressure.

Security strategy must be tied to business impact.

What the Threat Landscape Is Telling Us

Threat Volume and Velocity Continue to Grow

Attacks are growing in volume, speed, scale, and stealth, with Comcast Business detecting 34.6 billion cybersecurity events over a 12-month period. Attackers blend high-volume, automated threats with "low-and-slow" tactics that evade traditional detection, intensifying pressure on defenders.

> **Business impact:** Without automated response, higher alert volumes stretch resources, increasing response times, breach risk, and associated costs.

AI is an Enabler as Well as a Risk Multiplier

The cybersecurity AI landscape is quickly evolving on three key fronts.

Front 1: Threat actors are leveraging generative AI (LLMs) to craft more convincing phishing lures and malware at scale, lowering the skill barrier and increasing the efficacy of attacks.

Front 2: Enterprise adoption of LLMs and employee use of "shadow AI" broaden the attack surface, while AI agents raise new concerns about non-human identity (NHI) management and digital trust.

Front 3: Defenders are deploying AI and machine learning (ML) to scale anomaly detection and automate responses.

> **Business impact:** AI has tremendous business value but can also be a liability. It must be governed and secured while being strategically leveraged.

Human Factors and Fatigue Stymie Security Efforts

Security teams are under intense pressure, facing burnout from alert overload as well as budget and staffing constraints. Meanwhile, end-users remain a primary target and are often the weakest link, as a single-clicked phishing email or misused password can allow an attacker to bypass perimeter security tools.

> **Business impact:** Human error continues to drive breach exposure and increase workloads for security teams. Investing in security culture and tooling is no longer optional.

Multi-Layered and Adaptive Defense Is Critical

Many threats exploit basic security lapses like unpatched systems and weak credentials, highlighting why best practices and user education remain crucial. As attackers employ more advanced methods to bypass the perimeter, organizations must evolve their prevention, detection, and response capabilities, and root out early-stage compromises with active threat hunting.

> **Business impact:** Basic cyber hygiene mistakes and over-reliance on perimeter security can lead to high-impact breaches. A holistic approach must pair employee education and advanced technology with mature processes and skilled people.

It's Time to Rethink Enterprise Risk

Faced with this complex and rapidly evolving threat landscape, organizations must align cybersecurity investments to critical business risks, prioritize exposures, and use a new AI-driven risk calculus to make smarter decisions about accepting, mitigating, or transferring risks.

> **Business impact:** Cybersecurity is no longer just IT's challenge. It is a board-level business continuity, resilience, and reputational challenge.

Key Data Findings

The high-level trends shaping the 2025 threat landscape come into sharper focus when examined through the lens of our cybersecurity solution data. Comcast Business's analysis of 34.6 billion cyber events reveals significant patterns, illuminating not just the sheer volume of potential threats, but the specific tactics and techniques that define how modern attacks unfold.

34.6 billion cybersecurity events analyzed, including:

19.5B
Resource development events related to botnet activity

9.7B
Drive-by compromise events attempting to install malware

4.7B
Phishing events attempting to compromise credentials or deliver malware

44K
DDoS attacks attempting to test or overwhelm defenses

Early-stage Threats Put Pressure on the Perimeter

Comcast Business detected and blocked billions of phishing (4.7 billion) and drive-by compromise (9.7 billion) events aimed at bypassing perimeter defenses. In our analysis, drive-by compromise emerged as the top technique used to attempt to gain initial access. This low-effort approach for attackers requires no user interaction beyond simply visiting a compromised or malicious website.

Attackers Invest in Resource Development

While many pre-attack activities, such as purchasing domains, acquiring Secure Sockets Layer (SSL) certificates, and setting up social media accounts, are invisible to security tools because they happen outside the network, others, like botnet usage, can be observed. Comcast Business detected 19.5 billion events attributed to attackers using botnets to probe our customers' networks, a sub-technique within the MITRE ATT&CK® resource development tactic. The massive scale of botnet events detected suggests that attackers are investing heavily in setup before the first malicious packet is sent.

Resourceful Adversaries Are Living off the Land

Once inside a network, attackers are increasingly employing LOTL techniques by conscripting trusted system tools and files to move laterally, escalate privileges, and exfiltrate data without tripping traditional defenses. This approach minimizes the attacker's footprint and extends dwell time by evading signature-based detection.

DDoS Tactics Evolve with Short Bursts and Carpet Bombing

Comcast Business detected 44,069 DDoS events, with attackers using high-velocity, short-burst assaults as a form of reconnaissance and stress-testing of defenses. These quick hit-and-run bursts may last only seconds, probing for weaknesses before larger onslaughts are unleashed. In parallel, "carpet bombing" DDoS campaigns—spreading attack traffic across many target IPs or subnets simultaneously—overwhelm networks in a stealthier manner.

Proxy Abuse and Attacker Hideouts

Threat actors abuse compromised proxy networks, botnets, and legitimate cloud services to hide their infrastructure. Across its combined residential and business customers, Comcast's threat intelligence team has identified groupings of tens of thousands of infected or co-opted devices that are quietly forwarding traffic for outsiders. Commonly referred to as "residential proxies," these can use any compromised personal or business device including routers, IP cameras, and other Internet of Things (IoT) devices. Once compromised, the devices' IP addresses are often sold or rented to attackers. The Comcast threat intelligence team has visibility into these threats, even though they often originate from devices that are outside of Comcast ownership and management.

Security Fundamentals: Back to Basics

Our data shows that attackers continue to exploit basic lapses, particularly around unpatched software, open ports, misconfigurations, and credential hygiene. Access to valid accounts via compromised credentials was among the most commonly observed post-compromise techniques, underscoring the importance of enforcing strong password policies, MFA, and timely deprovisioning of stale or unused accounts.

The 2025 Cybersecurity Prism: Building Enterprise Resilience with Layered Security

In 2025, cybersecurity is inseparable from business resilience. A successful breach is not just a technological event. It can disrupt operations, impact revenue, and damage reputation. Multi-layered defense, therefore, is no longer simply an IT best practice. It is a cornerstone of organizational resilience.

Resilient security anticipates that some defenses will fail. By layering protection across the network, cloud, endpoints, and people, businesses can detect and contain threats more quickly, minimizing downtime and recovery costs. This approach hardens operations while enabling faster recovery when incidents occur.

Technology alone is not enough. AI-powered monitoring and automated response provide speed, but skilled analysts and threat hunters are critical to interpret signals, prioritize risks, and act decisively. The combination of human expertise and adaptive technology ensures attacks do not spiral into crises.

For business leaders, the lesson is clear: cybersecurity is a board-level concern. Investing in adaptive, multi-layered defenses builds resilience, protects customer trust, and helps the enterprise keep moving forward in an uncertain environment.

How Comcast Business Helps Enable Enterprise Resilience through Cybersecurity

Comcast Business provides scalable, multi-layered security solutions to counter modern threats. This year's report shows attackers are striking earlier and faster with sophisticated evasion tools, demanding a coordinated defense across the entire attack chain and enterprise. Our comprehensive portfolio integrates advanced capabilities into customers' infrastructure, including network firewalls, intrusion prevention, vulnerability and exposure management, cloud security, and sophisticated detection and response solutions such as Endpoint Detection and Response (EDR), Network Detection and Response (NDR), and Managed Detection and Response (MDR). These work in tandem with Secure Access Service Edge (SASE) frameworks, zero trust architectures, and targeted security such as DDoS mitigation.

By combining these technologies with around-the-clock monitoring, threat intelligence, and a team of skilled analysts, Comcast Business helps organizations detect, prevent, and respond to threats with speed and precision.

Bringing the Data to Life

To provide clarity and an actionable structure, this report maps our security log data against the MITRE ATT&CK® framework and provides parenthetical links to tactics, techniques, and sub-techniques mentioned. This industry-standard model helps technology leaders visualize the entire attack lifecycle, establish a common language for discussing threats, and directly link adversary behaviors to proven mitigations and security controls. To help illustrate the lifecycle of a modern cyberattack, we've organized the narrative into four stages. While these are not official MITRE ATT&CK® stages, this structure helps leaders see not just what individual techniques look like, but also highlights the interconnected nature of techniques as bad actors attempt to execute an end-to-end attack:

01.

Identifying Targets & Testing Defenses

The initial phase where adversaries perform reconnaissance, develop resources, and attempt to compromise defenses.

02.

Establishing a Foothold

The critical post-compromise stage where attackers execute code, establish persistence, and escalate privileges.

03.

Digging Deeper & Expanding Reach

The dangerous phase of lateral movement, credential harvesting, and defense evasion as attackers burrow deeper into a network.

04.

Playing Out the Endgame

The final stage where attackers establish command and control, exfiltrate data, and deploy their ultimate payload, whether that's destroying data, stealing it, or holding it for ransom.

Interspersed throughout the MITRE-based narrative are insights on the broader trends shaping the threat landscape—such as the rise of LOTL techniques that abuse legitimate system tools, the pervasive use of proxy networks to mask malicious activity, and the role of AI as both a defensive accelerator and a risk multiplier. Together, these insights illustrate how adversaries are evolving and how defenses must adapt in an increasingly high-stakes, AI-driven environment.

To bring these threats and defensive actions to life, we have included SOC case studies. These illustrative examples are based on anonymized, real-world events with additional details added by Comcast Business SOC analysts to better demonstrate some typical techniques and behaviors of an attack. They provide an inside look at how multi-stage attacks can unfold and how a combination of advanced technology and human expertise can interrupt the attack chain and mitigate business impact.

Attack Stage 1

Identifying Targets & Testing Defenses

This initial stage covers the early steps in an attack, where adversaries identify weaknesses and attempt to gain entry.

MITRE Tactics Covered:

Reconnaissance | TA0043
Resource Development | TA0042
Initial Access | TA0001

Reconnaissance is Constant

Just like with physical crimes, cyber adversaries often begin by quietly casing the perimeter. Every day, threat actors (from low-level cyber criminals to nation-state backed groups) probe common entry points such as firewalls, web servers, remote access ports, virtual private network (VPN) gateways, and IoT devices, seeking any crack in the enterprise perimeter. This "background noise" is largely automated and commoditized, as botnets and scan-as-a-service tools continually sweep the internet. That automation has supercharged reconnaissance, with Fortinet recording a 16.7% year-over-year surge in automated global scanning, peaking at a velocity of 36,000 scans per second.[2]

While you cannot eliminate reconnaissance activity, you can harden and minimize the attack surface, institute robust vulnerability and patch management, and monitor for early warnings (e.g., ingesting threat intelligence on known scanner IPs and blocking aggressive probing can preempt attacks).

16.7%

YoY surge in automated global scanning

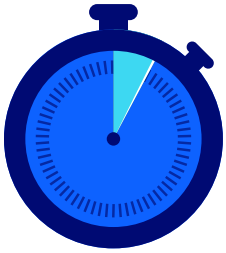
Source: Fortinet, 2025 Global Threat Landscape Report

[2] Fortinet, 2025 Global Threat Landscape Report

DDoS Short Bursts as Reconnaissance

Comcast Business detected an increase in short-duration (less than 5 minutes) DDoS attacks that threat actors can use as a reconnaissance tool to essentially jiggle the locks on network defenses. These hit-and-run DDoS attacks overwhelm defenses briefly and then stop before traditional mitigation can engage. For example, a threat actor might hit a web service with a 30-second burst of traffic to gauge DDoS detection triggers, then back off to see what happens. Attackers can learn valuable information about defense capabilities without causing too much of a stir, revealing how quickly a target mitigates, what threshold causes a response, and which parts of the infrastructure are less secure. These short-burst attacks confirm that reconnaissance isn't limited to quiet scanning—sometimes it's loud and brash, meant to test defenses.

Comcast Business detected increased use of short-burst DDoS attacks, with some lasting less than 10 seconds.



405 events
in less than 5 minutes

56 events
in less than 10 seconds

As New Vulnerabilities Proliferate, Patch Management Remains a Cornerstone of Proactive Cyber Defense

Patching may not always grab headlines, but—coupled with security posture and system configuration hardening—it can reduce one of the most common paths attackers use to compromise organizations. Yet, fully closing the patch gap is challenging because it is difficult to identify software dependencies that rely on the prior version, and dependency updates must be tested in advance. The sheer volume of Common Vulnerabilities and Exposures (CVEs), the complexity of enterprise IT environments, and downtime considerations can all slow mitigation. This is why a risk-based approach to vulnerability management, coupled with continuous testing, is crucial.

The Scale of Common Vulnerabilities and Exposures Continues to Climb

Tracking the growth of CVEs from 2020 through 2024.

2020	2021	2022	2023	2024
18,375	20,161	25,059	28,961	40,077

Source: CVE.org data

Resource Development

Before attackers make an intrusion attempt, they spend time building and positioning their assets. Resource development techniques include acquiring or compromising tools like domains, servers, SSL certificates, and proxy IPs as well as setting up social media accounts and developing custom malware for use in future attacks. This preparatory stage has become highly commoditized and supercharged by automation, fueling a higher volume of attacks as criminals no longer need advanced skills or expensive infrastructure to launch campaigns.

Comcast Business detected 19.5 billion resource development events tied to botnet activity, where adversaries harness compromised machines to probe customer networks for weaknesses. This activity reflects how much effort attackers put into staging their campaigns before ever sending a malicious payload. The scale suggests that botnets are a core element of industrialized attack preparation, giving adversaries the ability to scan, test, and refine their approaches at massive scale.

Outside botnets, we detected especially high alert volume across the following techniques: acquire infrastructure (T1583), compromise infrastructure (T1584), and develop capabilities (T1587). These alerts indicate the benefit of managed detection and response for blocking attacks earlier in the attack chain and taking a more proactive defensive stance by interrupting threat actors in the set-up phase.

Acquire/Compromise Infrastructure (T1583 & T1584)

Threat actors acquire domains, cloud servers, and hacked websites to use as launchpads. Some use Virtual Private Servers (VPS) hosted by bulletproof hosting services[3] that resist takedown requests, while others simply compromise legitimate sites to host malware. A key trend is the use of Initial Access Brokers (IABs), who sell network access on criminal marketplaces. This allows attackers, like ransomware operators, to bypass the time-consuming and sophisticated reconnaissance phase by purchasing a ready-made foothold.

Develop Capabilities (T1587)

The development of malware and exploits has also evolved, with attackers often buying tools instead of creating them. They can purchase malware “root kits,” use open-source tools, or subscribe to malware-as-a-service offerings. Additionally, AI has become a force multiplier for capability development. In 2024, we saw the emergence of tools like WormGPT (an AI model tuned for malware coding) marketed on dark web forums. Generative AI can now fill skill gaps for criminals, helping them write effective malicious code or create polymorphic malware that changes to evade detection.

[3] Bulletproof hosting is a general reference to web hosting services that ignore or evade law enforcement requests.

Initial Access

Once attackers conduct prep work, they shift their energies to attempting to access their target environments. This often begins with social engineering in the form of phishing. This technique has long been used to trick users into revealing valid credentials to threat actors but is undergoing a shift as security education programs make users more wary of entering credentials when prompted. Increasingly, phishing messages are being used to set up another initial access technique: drive-by compromise. An innocent looking link in an email, text, or chat leads to a compromised or malicious website, where attackers use malware to gain a foothold within the user's device.

Top Initial Access Methods Detected

Drive-by Compromise (T1189)

Visiting a compromised or malicious website can automatically infect a user's system with malicious code without any further action.

Phishing (T1566)

Deceptive messages are used to trick victims into revealing credentials, clicking malicious links, or deploying malware.

Phishing (T1566) as a primary vector

"Click This" remains at the top of the hacker's playbook, and for good reason. Phishing continues to be rampant across email, text (smishing), voice (vishing) and, increasingly, workplace collaboration tools (such as Microsoft Quick Assist), as adversaries look to trick users into either giving up credentials or executing malware.[4]

Key Takeaway

Threat actors are escalating phishing campaigns with new AI-driven tactics.[5] Generative AI helps churn out convincing phishing messages at unprecedented speed and scale, while AI-based voice cloning has given rise to more convincing vishing schemes where victims hear familiar voices, like those of a CEO or loved one, to deceive them. Attackers even deploy deepfake images and video in these social engineering ploys. Whatever the channel, phishing continues to adapt and thrive. AI tools are only helping increase the realism, speed, and scale of phishing attempts, making this vector more formidable than ever.

4.72B

phishing events detected by Comcast Business

[4] Microsoft, Threat actors misusing Quick Assist in social engineering attacks leading to ransomware
[5] Federal Bureau of Investigation, Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud

Drive-by Compromise (T1189)

Drive-by compromise emerged as a prevalent initial access vector in our data set, with nearly 9.8 billion events blocked. In a drive-by attack, a user visits a compromised or malicious website that then automatically triggers malware download or exploit code (often via malvertising or fake prompts). Notable examples are SocGholish[6] (injects fake browser update dialogs into legitimate but compromised websites) and ClickFix[7] (produces fake error messages or security alerts, often displayed as pop-up windows, that can trigger infostealer installation). The massive scale of our detections indicates that attackers find drive-by attacks attractive for targeting broad user populations.

These attacks can deliver malware that opens the door to larger-scale compromises if not caught and contained. Defending against drive-by attacks requires layered web security: updated browsers, Domain Name System (DNS) filtering, web proxy scanning, and isolating or shielding untrusted web content. User education helps, but given these attacks are often invisible to the user, technical controls are the front line. Encouragingly, many drive-by attempts are noisy and can be readily detected by security tools. The case study below, from the Comcast Business SOC, illustrates one such detection.

9.7B

drive-by compromise events blocked by Comcast Business in one year

[6] SocGholish is a JavaScript-based loader malware that has been used since at least 2017.
[7] ClickFix attacks are a sophisticated form of social engineering, leveraging the appearance of authenticity to manipulate users into executing malicious scripts.

SOC Casebook

Comcast Business Threat Hunting Team Contains Fake Browser Update Attempting to Establish a Foothold for Attackers

In this example, we see how a drive-by compromise using a fake update enabled attackers to establish persistence and command and control (C2) communication, as well as how rapid, managed SOC detection and containment cut off the attack before escalation or ransomware deployment.

A user browsing an infected news site encountered a pop-up urging a "critical browser update." Trusting the prompt, they downloaded and ran the installer, which was actually SocGholish, a JavaScript-based loader favored by ransomware crews. In MITRE terms, this represents a drive-by compromise (T1189) and user execution (T1204) sequence.

Once active on the employee's workstation, SocGholish decrypted its stage-one payload, planted a hidden scheduled task (T1053.005) for persistence (TA0003), and reached out over HTTPS to an attacker-controlled C2 server (T1071.001) to await further instructions that typically include Cobalt Strike beacons or ransomware.

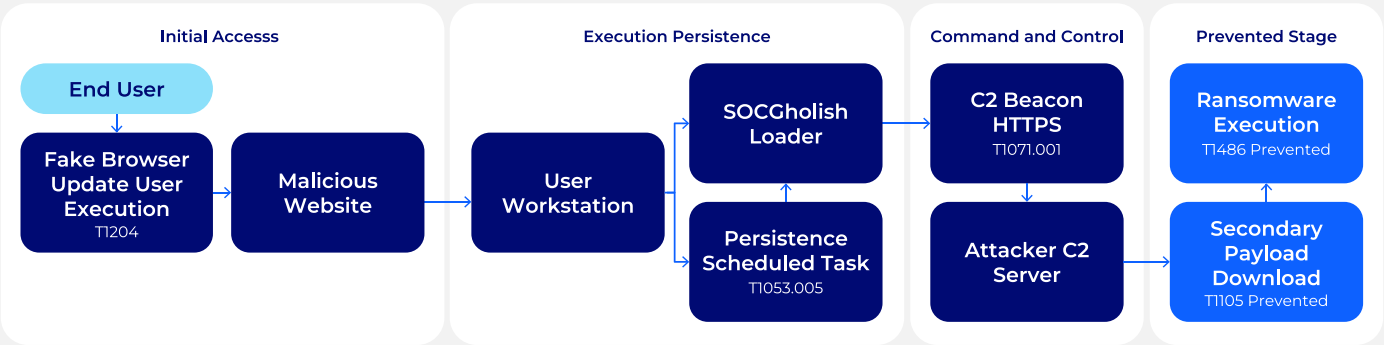
Comcast Business threat-hunting analytics flagged the new scheduled task, unfamiliar binary hash, and anomalous outbound beacon. The SOC remotely quarantined the workstation, blocked the C2 domain, and contacted the customer to reimage the device and reset credentials. Rapid containment severed the backdoor's command channel before it could pull secondary payloads, preventing potential privilege escalation, data theft, and encryption.

SOC Insights:

User-driven infections remain potent: Fake browser-update lure bypasses perimeter controls by exploiting user trust and normal download workflows.

Behavioral hunting closes the gap: Detecting a never-before-seen hash, sudden scheduled task creation, and quick HTTPS beaconing exposed SOCGholish before stage-two malware arrived.

Education plus layered security is essential: Continuous awareness, combined with endpoint detection and 24/7 SOC monitoring, provides security against aggressive malware.



The Human Element

In cybersecurity, technology sets the stage, but people determine the outcome. While security strategies increasingly emphasize AI, automation, and zero trust architectures, human behavior remains one of the most significant variables in both risk exposure and defense effectiveness. Every phase of the attack chain, from the first phishing click to impact, is shaped by human actions, oversights, and intuition.

In cybersecurity, technology sets the stage, but people determine the outcome.

Human-triggered exposures and IT misconfigurations play a role in a large amount of successful attack attempts. From phishing emails to poor credential hygiene, attackers continue to exploit natural human tendencies like urgency, curiosity, and trust.

Yet it's not just end-users at risk. The defenders themselves—security analysts, engineers, and IT teams—are overwhelmed. The global cybersecurity workforce gap has widened to 4.76 million professionals and 67% of organizations report a staffing shortage that puts them at risk, according to ISC2's 2024 Cybersecurity Workforce Study.[8] This chronic overload contributes to higher risk in subtle but serious ways. Alert fatigue can lead analysts to miss real threats buried in the noise. Repetitive tasks drain focus and morale. Turnover among experienced staff can leave organizations exposed at critical moments.

67%

of organizations report a shortage in cybersecurity staffing, leading to increased risk and burnout.

Source: ISC2

Key Takeaway

The challenge also reveals an opportunity: empowering people through smarter processes and technology. Leading organizations are investing in tools that augment human judgment, reducing burnout while sharpening response capabilities. AI-enabled MDR services, for example, are transforming the role of human analysts from triage engines to strategic threat hunters. Elsewhere, behavior-aware security platforms are adapting to individual user patterns, spotting anomalies like unusual login behavior or file movements that might escape traditional rule-based alerts. These tools can act as a second set of eyes, flagging human mistakes before they escalate into breaches.

[8] ISC2, 2024 ISC2 Cybersecurity Workforce Study

Attack Stage 2

Establishing a Foothold

This critical post-compromise stage details how attackers solidify their presence within a network to maintain access and expand their control.

MITRE Tactics Covered:

Execution | TA0002
Persistence | TA0003
Privilege Escalation | TA0004

Stealthy Execution Is the Norm

After penetrating a system, attackers tend to avoid noisy, obvious exploits. Rather than dropping known binaries, threat actors live off the land, enlisting tools such as, but not limited to, PowerShell, Windows Management Instrumentation (WMI), scripting languages, and other built-in Windows and Linux tools to run their code. By piggybacking on these trusted utilities—while also using fileless, in-memory malware—adversaries can execute their objectives while looking like routine IT work.

Our data reinforces this trend, with command and scripting interpreter (T1059) misuse ranked as the most detected post-compromise techniques we blocked. In practice, that means an attacker might launch scripts to start malicious processes under the guise of normal system activity. Security teams must therefore scrutinize even mundane processes. As IBM notes in its X-Force 2025 Threat Intelligence Index, nearly one in three attacks[9] now involves the use of valid accounts rather than malware, indicating that many intrusions execute entirely under the radar of traditional antivirus. The bottom line: once inside, attackers run quiet by default.

Top Techniques Used for Execution

Command and Scripting Interpreter (T1059): Built-in command and scripting tools are abused to execute malicious commands and scripts.

User Execution (T1204): Malicious code is executed by tricking a user into performing an action, such as opening a malicious file or clicking a link.

Windows Management Instrumentation (T1047): The native WMI framework is abused to execute malicious commands and payloads, enabling interaction with local and remote systems.

Exploitation for Client Execution (T1203): Malicious code is executed by exploiting software vulnerabilities in common client applications, such as web browsers or productivity software.

[9] IBM, IBM X-Force 2025 Threat Intelligence Index

Maintaining Footholds

With a beachhead established, attackers work to persist in the network, ensuring they survive reboots or initial incident response actions. Common persistence techniques include adding autorun keys in the registry, planting scripts in startup folders, abusing scheduled tasks, and even creating covert new user accounts. For example, an intruder might register a malicious service that quietly respawns their backdoor or schedule a nightly task to re-download malware. In server environments, attackers may install legitimate remote access software (like screen-sharing or remote monitoring tools) as their backdoor, knowing such software won't raise suspicions or be flagged by anti-malware defenses.

Key Takeaway

Defenders should monitor closely for unusual changes to systems, such as new services appearing, an admin account suddenly being created, or a device making unexpected outbound connections. These can all be early red flags of an ongoing intrusion.

Notable Persistence Techniques Observed

Event Triggered Execution (T1546): Malicious code is executed in response to specific system or user events, such as logons or application launches, to establish persistence or elevate privileges.

Boot or Logon Autostart Execution (T1037): System settings are configured to automatically run malicious programs during system boot or user logon to maintain persistent access.

Scheduled Task/Job (T1053): Task scheduling utilities are abused to automatically execute malicious code at predetermined times or intervals for persistence.

Create Account (T1136): New local, domain, or cloud accounts are created on victim systems to establish secondary, persistent access.

Once inside, attackers run quiet by default.

Escalating Privileges

With an initial foothold and persistence in place, attackers seek higher privileges. Gaining administrator or system-level rights allows them to access more data, disable security tools, and move through the network at will. Techniques can include exploiting known operating system (OS) vulnerabilities to run code as SYSTEM, abusing misconfigurations, and using credential dumping tools that steal admin passwords. Tools like Mimikatz, an open-source tool used by both attackers and penetration testers to extract credentials, remain a go-to for attackers to extract credentials.[10] Once they obtain a domain admin hash, for example, the threat actor can leapfrog through the network via pass-the-hash or lateral login, impersonating a high-privilege user. This creates a fast path to expanding control over many systems. Without robust defenses like credential vaulting and multi-factor authentication, an attacker with one stolen password can become an "administrator" of your entire environment.

The prevalence of these attempts highlights why organizations must closely monitor admin account activity and Windows Security Event logs. Even seemingly benign events, like a user suddenly being added to an admin group, should raise immediate scrutiny.

Top Privilege Escalation Techniques Detected

Exploitation of Privilege Escalation (T1608): Software vulnerabilities are exploited to execute code and gain elevated privileges on a system.

Valid Accounts (T1078): Existing legitimate accounts are abused to gain access to systems, bypass security controls, and move through a network.

Abuse Elevation Control Mechanism (T1548): Built-in system mechanisms that control user privileges, such as User Account Control (UAC), are circumvented to gain elevated permissions on a system.

Process Injection (T1055): Malicious code is injected into a legitimate process to execute under its security context, evading defenses and potentially elevating privileges.

AI Agents & Non-Human Identities: New Frontiers of Risk

As enterprises deploy their own AI agents and engage with autonomous systems being used by partners, suppliers, and customers, the attack surface is expanding in a new dimension: non-human identities (NHIs). From API keys and service accounts to the identities of the agents themselves, these digital credentials are proliferating at a massive scale. Unlike human users, these NHIs may operate without direct oversight, behave in less predictable ways, be granted overly broad permissions, and can be implemented and abandoned without clear ownership, creating significant blind spots for cyber defenders.

A compromised NHI serves as a powerful gateway for attackers, enabling them to access sensitive data, evade detection, and move laterally through networks with the legitimacy of a trusted system. This reality demands that technology leaders move beyond a simple block-or-allow security posture. Managing this new frontier of risk requires a nuanced calculus, where the business value of an AI-driven task is carefully weighed against the potential exposure.

The path forward involves extending robust, modern Identity and Access Management (IAM) controls to these digital workers. Security strategies must treat agents as powerful but untrusted users, enforcing the principle of least privilege and granting just-in-time (JIT) access only for the duration of a specific task. By implementing strong governance, continuous monitoring, and clear audit trails for every NHI, organizations can harness the power of automation while managing its inherent risks.

[10] Mimikatz is a well-known hacktool used to extract Windows passwords in plain-text from memory, perform pass-the-hash attacks, inject code into remote processes, generate golden tickets, and more.

SOC Casebook

Enumeration Red Flag Cuts the Attack Chain

This scenario involves a simulated intrusion test that underscores how account discovery and token-manipulation exploits mirror real-world ransomware and nation-state tactics.

Custom detection rules created by Comcast Business triggered on a burst of account discovery (T1087) commands—whoami /all, net user /domain, and LDAP queries. Within minutes, the same endpoint attempted a token-manipulation exploit to obtain NT AUTHORITY\SYSTEM privileges, matching the MITRE privilege escalation technique (T1068).

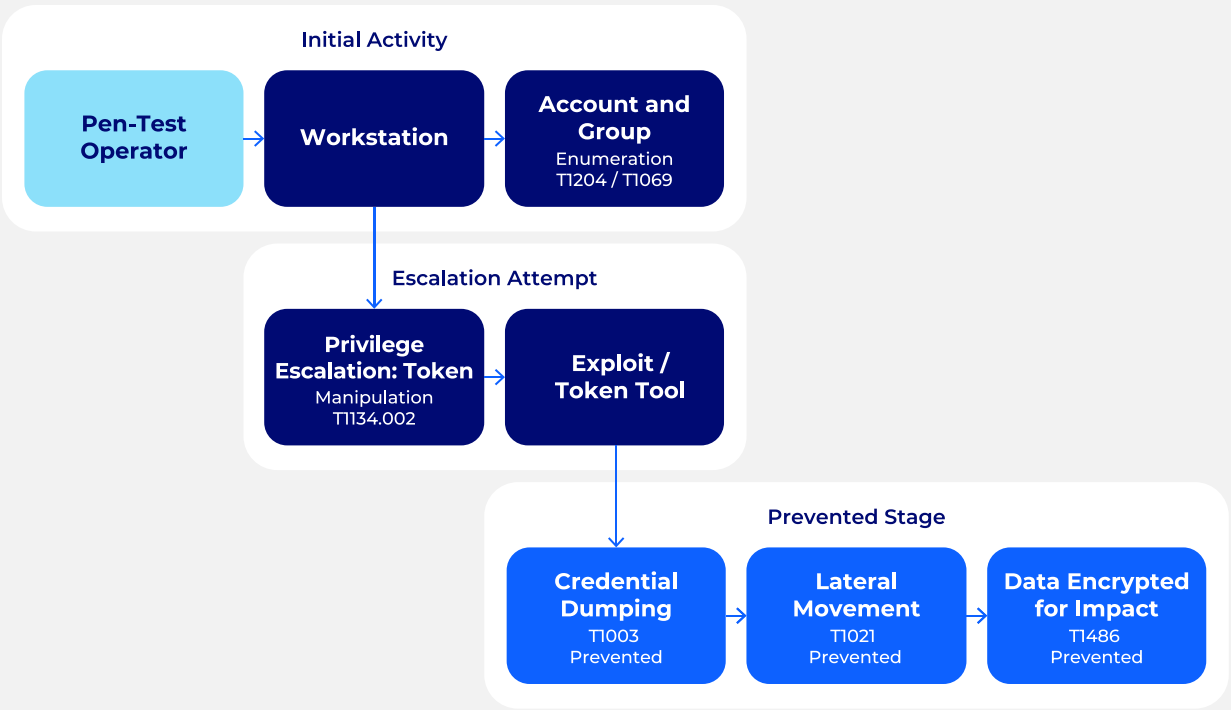
Although the activity stemmed from an authorized penetration-testing engagement, these steps mimic real ransomware and nation-state tradecraft. MDR analysts received the alert, investigated contextual evidence, and remotely quarantined the workstation. By isolating the host, the SOC cut the attack chain before credential dumping, lateral movement, or ransomware deployment could follow.

SOC Insights:

Early enumeration is a tell: Account and permission discovery often precede privilege escalation, so catching it will buy critical response time.

Custom EDR rules matter: Comcast Business detections surfaced the threat early, highlighting the value of tailored analytics, human investigation, and high-quality threat intelligence.

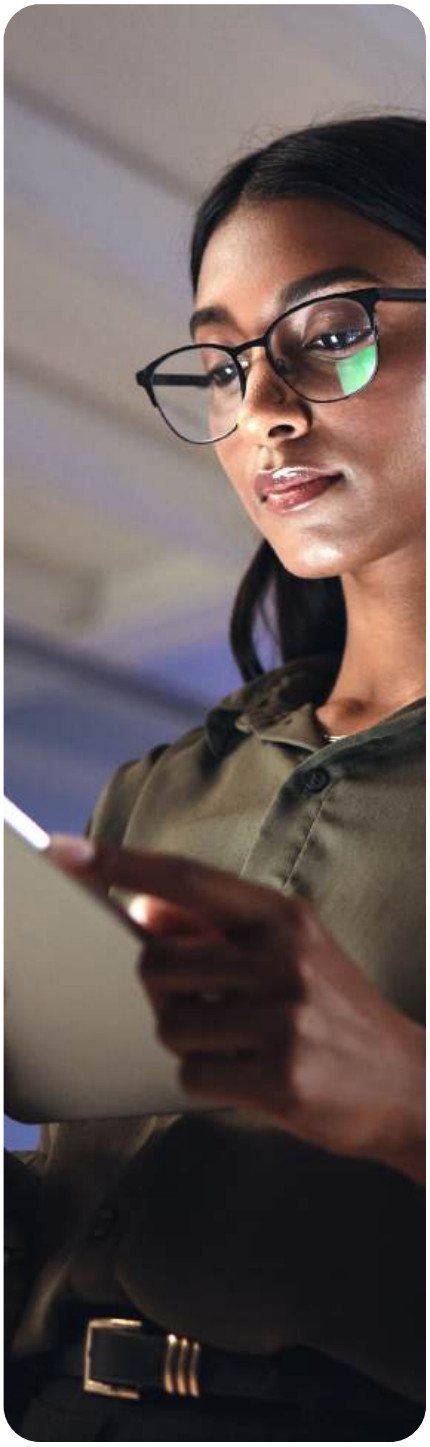
Layered services reduce risk: Combined EDR and MDR coverage compresses the window between intrusion, detection, and containment, which is essential against fast-moving adversaries.



Living Off the Land in Action

Today's attackers often prefer to live off the land inside victim networks. But what does that look like in practice? Intruders pivot to using whatever tools and access they can find on the system. Instead of downloading a custom port scanner that could raise a red flag, an attacker might use the operating system's own netstat and PowerShell to survey the network. Or they might use built-in Secure Shell (SSH) and Remote Desktop Protocol (RDP) to move from host to host. Some attackers even masquerade their malicious processes by renaming them to resemble harmless system processes. This blended strategy is highly effective at evading signature-based defenses.[11]

According to federal law enforcement,[12] cyber threat actors, including the People's Republic of China (PRC) and Russian Federation state-sponsored groups, often leverage Living off the Land Binary (LOLBin) techniques to compromise and maintain persistent access to critical infrastructure organizations.



Comcast Business MDR data reveals how diverse these stealth techniques are. We logged events in the past year tied to these key LOTL behaviors:

Windows Management Instrumentation (WMI) (T1047): The native WMI framework is abused to execute malicious commands and payloads, enabling interaction with local and remote systems.

Dynamic-Link Library (DLL) Injection (T1055.001): A legitimate process is forced to load a malicious DLL, allowing malicious code to run hidden within the trusted application.

Scheduled Task (T1053.005): The Windows Task Scheduler is abused to automatically execute malicious code at specific times or intervals for persistence.

Software Packing (T1027.002): Malicious executables are compressed or encrypted to conceal their contents and evade detection, unpacking the true payload in memory at runtime.

Key Takeaway

A large share of the alerts generated by these detections were later classified as benign or expected activity, which highlights the defensive challenge: malicious and legitimate operations sometimes look alike. Attackers are counting on that ambiguity to hide in plain sight. This is why advanced detection analytics and human-led threat hunting have become so important. An experienced analyst can spot subtleties, such as a PowerShell process running base64-encoded commands in an environment that normally never does. They can then connect the dots that an automated tool might miss. In short, living off the land is no longer an outlier technique, but the new normal for adversaries. Defenders must up their game in detection finesse.

[11] Office of Information Security, "Living Off the Land," 2024
[12] National Cyber Security Centre, "Identifying and Mitigating Living Off the Land Techniques," 2024

Salt Typhoon

Salt Typhoon is the code name for a Chinese state-sponsored threat actor that specializes in long-term, low-profile intrusions. This group made headlines after quietly infiltrating a U.S. Army National Guard network and remaining undetected for close to nine months (from March to December 2024).[13]

How did Salt Typhoon pull off such an extended breach? By masterfully living off the land. According to investigators, the group refrained from using any zero-day exploits or noisy malware. Instead, they exploited older known vulnerabilities and co-opted legitimate network tools to stay under the radar.

Salt Typhoon operatives specifically seek out assets that are unmanaged or poorly monitored, such as a forgotten IoT device or a legacy server lacking proper logging. They then use these assets as their footholds. In the National Guard case, they were able to compromise a VPN appliance and then move laterally through network segments without tripping alarms.

During their months-long residence inside the Guard's network, Salt Typhoon reportedly exfiltrated administrator credentials and even obtained detailed network diagrams, effectively mapping out the entire infrastructure for further exploitation. This incident has been a wake-up call for many in both government and industry. A threat actor with patience and expertise can burrow into critical systems for the better part of a year, all while appearing innocuous.

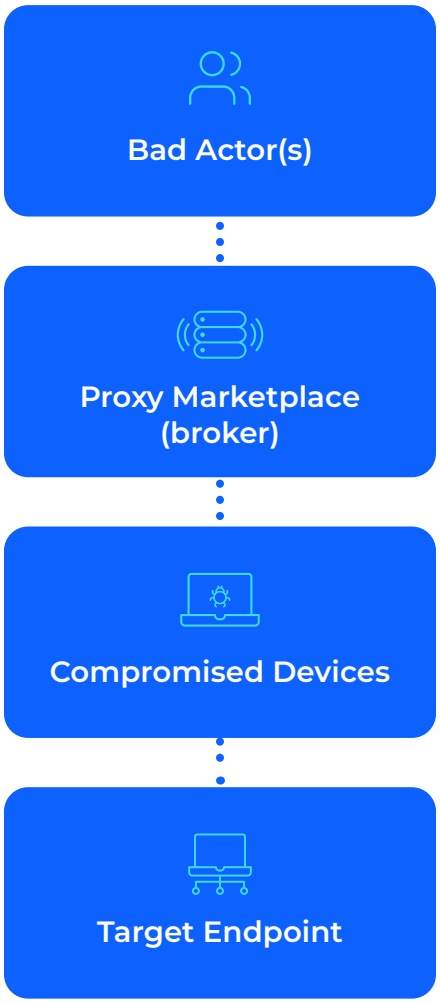
[13] Federal News Network, How Salt Typhoon breached the National Guard — and what it means for U.S. cybersecurity

The Hidden Threat: Proxy Abuse and Masked Adversaries

Attackers increasingly hide behind proxy relays to disguise where traffic truly originates. In practice, that often means co-opting internet-connected devices in homes and businesses—such as laptops, cameras, phones, and IoT equipment—so malicious requests appear to come from "ordinary" IPs instead of attacker infrastructure. Referred to as a "residential proxy" or "ResProxy," the tactic obfuscates the location of threat actors, diminishing defenders' abilities to trust what an IP address or apparent geography implies.

Research conducted by the Comcast Threat Research Lab (CTRL) using real-world network telemetry reveals that ResProxy abuse has become pervasive.[14] Across its combined residential and business customers, Comcast has identified large groupings (or "herds") of tens of thousands of infected or co-opted devices that are quietly forwarding traffic for outsiders.[15] This is infrastructure that can be used by threat actors to mask credential stuffing attempts, facilitate rapid C2 channel rotation, and even data exfiltration.

Comcast's research shows that in some cases, users may have no knowledge of the infection on their devices with the proxy service, while in other cases, they may actively know about it but not understand the implications. While the Comcast threat intelligence team has visibility into these emerging threats, they originate from devices that fall outside Comcast's ownership and management. However, where possible, Comcast is taking concrete steps to help combat this activity, such as informing device manufacturers of their susceptibility to residential proxy services.



[14] Comcast, Comcast's Proactive Cyber Defense Activities
[15] Comcast, ResProxies – What Hasn't Been Herd Yet

Business Impact of ResProxies

For enterprises, this threat is dual-faceted: it poses direct technical challenges (e.g., detection complexity, persistent evasion of block lists) and indirect reputational risks, as compromised infrastructure may unknowingly participate in malicious activity. Even if an organization never initiates malicious traffic, a compromised device on its network could relay phishing or fraud attempts, inviting uncomfortable questions from auditors, regulators, and customers.

Enterprises must proactively monitor and mitigate outbound proxy traffic anomalies, enforce stringent MFA protocols, and integrate DDoS mitigation and threat-hunting workflows to detect and deter adversary tactics that leverage compromised proxies.

Security tools cannot trust an IP's location because a connection that appears to come from within a specific geography might actually be an attacker from another part of the world operating in disguise. Critically, this also undermines the use of IP addresses as a key factor in establishing trust and verifying identity. That means that defenders need to shift their tactics, with a heavier focus on analyzing behavioral patterns. The rise of proxy abuse underscores the need for zero-trust assumptions about network traffic and more sophisticated threat hunting that can peel back the layers of attacker obfuscation.

Recommended Actions for Cybersecurity Leaders

- Establish baselines for outbound traffic and create alerts for destinations or bandwidth spikes that deviate from normal patterns, especially on IoT and guest segments.
- Block any uncommon ports, and for any exceptions, carefully inspect traffic classes that have no business reason to leave the network.
- Mandate MFA and unique passwords for every external service. Compromised credentials lose value when secondary factors are enforced.
- Deploy behavioral-based anomaly detection to flag connections that look normal at the IP layer but diverge from expected usage patterns, such as unusual timing, frequency, or command sequences.

Attack Stage 3

Digging Deeper & Expanding Reach

In this stage, attackers who have established access seek to spread to other systems, gather credentials, and avoid detection at all costs. It's where a single compromised host can snowball into a full domain takeover if not caught and contained.

MITRE Tactics Covered:

Defense Evasion | TA0005
Credential Access | TA0006
Discovery | TA0007
Lateral Movement | TA0008
Collection | TA0009

Quiet Lateral Movement

Attackers often perform internal discovery and lateral movement slowly to blend in with legitimate user activity and avoid detection. Rather than immediately exploiting stolen admin credentials, skilled attackers may lie low for weeks or months or choose off-hours to advance, masking the source of their access. By pacing their lateral movement, they stay below the radar of intrusion detection thresholds. For example, instead of a sudden mass pivot, an attacker might incrementally hop from system to system, performing internal reconnaissance and staging next steps until they find a high-value target. This patience can pay off. Unusual patterns can emerge in logs (e.g., a spike in authentication attempts or new users with administrative privileges appearing on crown jewel servers) but these may be subtle blips spread over time.

Key Takeaway

Security teams must remain vigilant for these faint signals of lateral spread. Network segmentation and zero trust access controls are critical defensive techniques to make it more difficult. Containing user and server networks into smaller zones makes it harder for intruders to roam freely. Likewise, monitoring East-West traffic between segments and baselining normal peer-to-peer communication helps expose anomalies. Implementing zero trust principles further limits lateral movement by continuously verifying identity and session context for each access request. In practice, that means even if an attacker gets in, they can't simply reuse one set of credentials everywhere without raising alarms or hitting access roadblocks.

Key Lateral Movement Techniques Observed by Comcast Business

Remote Services (T1021): Built-in remote connection protocols like RDP and SSH are used to log into other systems on a network to execute commands.

Valid Accounts (T1078): Compromised user, admin, or service account credentials are used to pivot and log into other systems across a network.

Credential Harvesting on Steroids

Once inside a network, threat actors operate under the maxim that "credentials are the keys to the kingdom." They may deploy tools like LaZagne[16] or built-in OS commands to dump passwords and hashes—for example, reg save commands to export Security Account Manager (SAM) hives,[17] or Volume Shadow Copy Service vssadmin to snapshot the New Technology Services Directory Information Tree (NTDS.dit) database.[18] Any account obtained, user or admin, becomes a steppingstone to the next. Common techniques include pass-the-hash[19] and pass-the-ticket[20] (using stolen hashed credentials or Kerberos tickets to authenticate on other systems without cracking passwords), as well as token impersonation[21] in cloud environments. In effect, a single captured password can spawn access to dozens of systems if permissions are not locked down.

Compromised credentials are widely traded on the dark web. In fact, IBM's 2024 X-Force Cloud Threat Landscape Report noted that gaining access via cloud credentials was the second most common initial attack vector in recent cloud incidents.[22] The phenomenon drives a vicious cycle: more breaches yield more stolen logins, which fuel further intrusions. The prevalence of info-stealer malware, which siphons passwords and session cookies en masse, has shifted credential theft into overdrive.

Key Takeaway

Multi-factor authentication is a must, though not a panacea, as adversaries now use MFA fatigue and adversary-in-the-middle[23] tricks (force communication between systems through an adversary-controlled system) to bypass it. Security detection rules should employ User and Entity Behavior Analytics (UEBA) machine learning techniques to identify potential issues like abnormal credential usage (e.g., unusual privilege escalation, an account authenticating to many endpoints, or access attempts at odd hours). While such detections are noisy and prone to false positives, they remain crucial when seen in the context of other techniques that sometimes signal illicit use. Finally, organizations should monitor criminal forums as a source of threat intelligence for their own leaked credentials and act quickly if any surface. In short, credential theft is the fuel powering modern breaches. Cutting off that fuel through hardened authentication and vigilant monitoring will blunt an intruder's ability to escalate.

Primary Credential Access Techniques Detected by Comcast Business

Valid Accounts (T1078): Existing legitimate accounts are abused to gain access to systems, bypass security controls, and move through a network.

OS Credential Dumping (T1003): Account credentials and password hashes are extracted from operating system memory or files like the Security Account Manager (SAM) database.

Brute Force (T1110): Passwords are systematically guessed, either online against a login service or offline against stolen password hashes, to gain account access.

Unsecured Credentials (T1552): Credentials stored in plaintext or other insecure locations, such as configuration files or the system registry, are searched for and stolen.

Credentials from Password Stores (T1555): Credentials are stolen by targeting and extracting them from dedicated password stores, such as web browsers or password managers.

Credential theft is the fuel powering modern breaches.

[16] LaZagne is a post-exploitation, open-source tool used to recover stored passwords on a system.

[17] Adversaries may attempt to extract credential material from the SAM database either through in-memory techniques or through the Windows Registry where the SAM database is stored.

[18] Adversaries may attempt to access or create a copy of the Active Directory domain database in order to steal credential information, as well as obtain other information about domain members such as devices, users, and access rights.

[19] Pass-The-Hash is a toolkit that allows an adversary to "pass" a password hash (without knowing the original password) to log in to systems.

[20] Pass the ticket is a method of authenticating to a system using Kerberos tickets without having access to an account's password.

[21] Adversaries may duplicate then impersonate another user's existing token to escalate privileges and bypass access controls.

[22] IBM, X-Force report reveals top cloud threats

[23] Adversaries may attempt to position themselves between two or more networked devices so they can collect information or perform additional actions.

Defense Evasion and Cover-up

Sophisticated adversaries treat evasion and cover-up as a core part of their operation, not an afterthought. By the time they're moving laterally or exfiltrating data, they are actively trying to erase or obfuscate any signs of their presence. Attackers commonly tamper with or shut down security tools as well as clear logs and artifacts that might reveal them.

Our data showed that a key technique in this phase is system binary proxy execution (T1218), where we recorded hundreds of events. Through this technique, adversaries attempt to hijack signed or otherwise trusted binaries, such as but not limited to Microsoft-signed files like rundll32.exe, regsvr32.exe, or wscript.exe to proxy their payloads and slip past application-allow-listing and EDR controls.[24] Other techniques included process and DLL injection (T1055.001)—used to attempt to bury malicious code inside benign processes—and software packing/obfuscation (T1027.002) to defeat static binary code analysis that examines the code without actually running it.

Common Defense Evasion Techniques

System Binary Proxy Execution (T1218): Trusted and signed system binaries are abused to proxy the execution of malicious code, bypassing application controls and other defenses.

Impair Defenses (T1562): Security tools, logging mechanisms, or other defensive controls are disabled or modified to hinder detection and allow malicious activity to go unnoticed.

Masquerading (T1036): Malicious files, tasks, or services are disguised to look legitimate by manipulating their names, locations, or other features to evade detection.

Obfuscated Files or Information (T1027): Files or information are encrypted, encoded, or compressed to make their malicious contents difficult for security tools to discover and analyze.

Subvert Trust Controls (T1553): Security controls that rely on trust, such as code signing or download warnings, are undermined to allow malicious programs to execute without alerts.

Key Takeaway

Cover-up behavior is expected in modern breaches. Security teams must deploy controls to make evasion harder (e.g. disable unnecessary scripting tools, enforce Windows Event Log retention and forwarding) and employ detection methods that focus on anomalies and attacker techniques.

[24] Adversaries may abuse these common files to execute malicious code or deliver malware—rundll32.exe, regsvr32.exe, wscript.exe.

SOC Casebook

Workplace Chat Tool Phished for Remote Takeover

A threat actor initiated external workplace chats posing as the customer's IT support, an example of the MITRE ATT&CK® initial access sub-technique called spearphishing via service (T1566.003). Several employees accepted the invites and followed instructions to "fix a security issue," downloading a legitimate-looking remote access tool from a public URL.

Launching the installer triggered user execution (T1204.002), after which the program silently registered itself as a service, granting the adversary interactive control over each workstation through external remote services (T1133). The attacker was now positioned to perform privilege escalation, harvest data, or deploy ransomware.

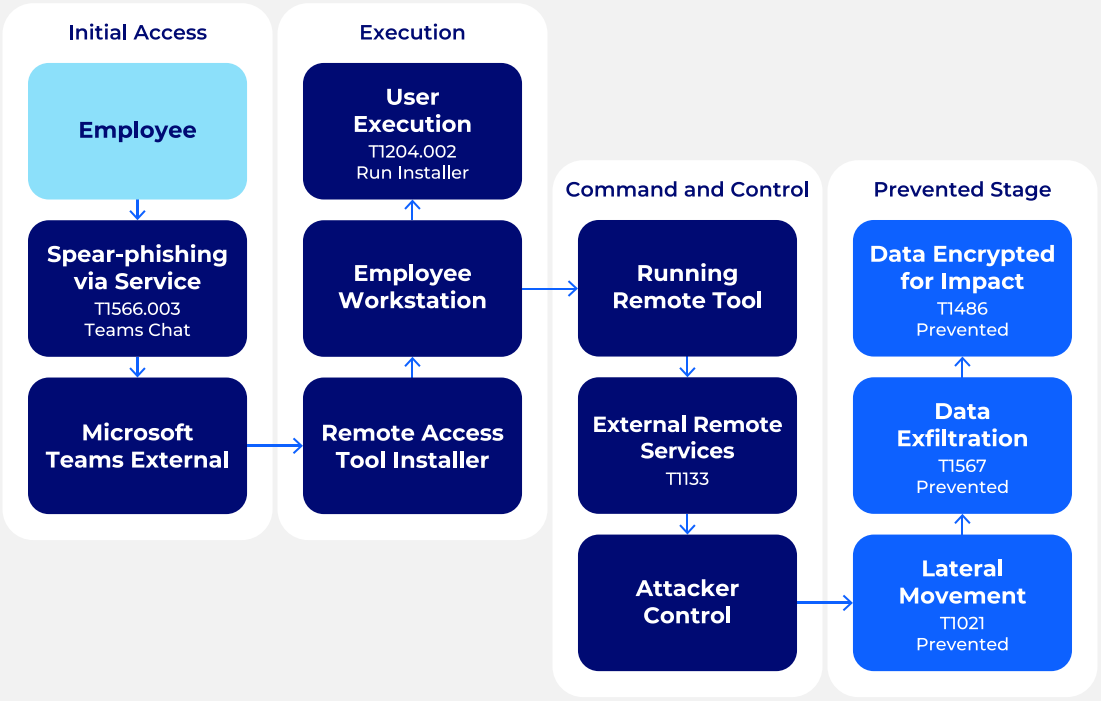
Comcast Business security analytics and SOC analysts correlated the sudden burst of external chat sessions with first-time downloads of remote-administration binaries across multiple hosts. Our analysts quarantined the compromised machines and disabled the affected accounts, contacting the customer to begin reimaging and resetting credentials. The swift response severed the attacker's live sessions, blocked lateral movement, and helped prevent potential data exfiltration or ransomware deployment.

SOC Insights:

Chat platforms are phishing venues: External chat invites can bypass email filters.

Legitimate tools are used for malicious activity: Off-the-shelf remote access software gives attackers hands-on control while evading basic malware defenses.

Rapid quarantine contains damage: Isolating endpoints and disabling accounts cut C2 channels, preventing escalation to data theft or ransomware.



MDR & EDR: Elevating Detection from Reactive to Proactive

In cybersecurity, time is often the most critical factor. Attackers attempt to blend in with legitimate activity not just to be stealthy but to buy the time needed to achieve their objectives. This is why detect-and-response tools, whose primary function is to shrink the window between initial compromise and decisive response, matter more in 2025 than ever before.

Once an attacker gains a foothold, the clock starts ticking. It can take mere minutes for an adversary to escalate privileges and move laterally across the network—a concept known as “breakout time.”

Our data includes detections across early post-compromise MITRE techniques and sub-techniques such as Windows Management Instrumentation (T1047), process injection (T1055), DLL injection (T1055.001), and Software Packing (T1027.002). Responses to these detections interrupt attackers before they have time to escalate privileges or move laterally, which are key steps on the path to compromising data.

Our analysis also reveals how MDR provides crucial opportunities to get ahead of the attacker’s timeline altogether. By combining threat intelligence with anomalous behavior detection, these tools can pick up signals that point to early-stage resource development techniques, including acquiring or compromising infrastructure (T1583, T1584) and developing malicious capabilities (T1587). This helps move response further to the left in the attack chain often disrupting threats before a foothold can be established.

But automated detection is only one part of the solution.

The Human Element: Threat Hunting at Scale

Continuous threat hunting provides active defense, unlike passive alerting. Skilled hunters proactively search networks, cloud, and endpoints for subtle indicators of compromise that evade automated tools. This is vital because our analysis shows that some of the most frequent alerts don’t necessarily indicate an attack, with benign alert rates hitting 96% for some alert types. The volume of these false alerts can cause significant analyst fatigue, thus underscoring the importance of proactive threat hunting.

Why It Matters for Enterprises

- Rapid triage and prioritization using AI-augmented analytics to separate signal from noise.
- Cross-kill-chain correlation to connect seemingly unrelated events and reveal coordinated attack campaigns.
- 24/7 monitoring helps prevent high-priority alerts being missed during off-hours or resource gaps.

Attack Stage 4

Playing Out the Endgame

In the final stage of an attack, adversaries attempt to take charge by establishing command and control (C2) channels to manipulate compromised systems, attempt to exfiltrate sensitive data, and execute impact actions (ransomware deployment, data destruction, fraud, etc.).

MITRE Tactics Covered:

Command and Control | TA0011
Exfiltration | TA0010
Impact | TA0040

Encrypted and Covert Command and Control Traffic

The endgame phase of an intrusion is defined by subtlety. Adversaries rarely send unencrypted instructions. Instead, they cloak outbound communication in trusted channels to avoid detection. Tactics such as domain fronting, DNS tunneling, and hijacking popular services (Slack, Discord, GitHub) allow attackers to make their C2 beacons appear indistinguishable from routine traffic.

These subtle C2 activities represent a key point in the battle between attackers and defenders. If attackers go unnoticed here, they are finally positioned to steal, compromise, or ransom an organization's data.

Over a six-month period, Comcast Business detected and blocked more than 708 million command and control attempts, including over 191 million attempts made through proxy-based channels, like those we explored earlier in the report. These detections underscore the scale at which attackers attempt to conceal their operations in plain sight, and the extent to which covert C2 has become the standard for modern intrusions.

Defending against this activity requires looking beyond simple indicators. Effective countermeasures include anomaly detection that flags unusual destinations (e.g., a host suddenly initiating encrypted traffic to a new geography), Transport Layer Security (TLS) inspection of encrypted traffic to surface hidden payloads, and continuous monitoring for outbound traffic irregularities. Together, these measures provide defenders with the best chance to detect and disrupt adversaries before data exfiltration and impact can take place.

708 Million C2 Attempts Blocked by Comcast Business

Phishing-linked C2: 497M
Adversaries repurpose phishing infrastructure for covert control.

Proxy-based C2: 191M
Beacons routed through residential proxies to mask origins.

Scanner-to-C2 transitions: 13M
Reconnaissance tools later serve as command relays.

Botnet C2: 2.0M
Distributed malware networks acting as control hubs.

Web attack C2: 2.0M
Exploits delivered via malicious sites with embedded C2.

Windows exploit C2: 1.7M
Post-exploit channels tied to Windows vulnerabilities.

Spam-source C2: 1.1M
Malicious traffic hidden within spam relay networks.

Mobile threat C2: 2.5K
Small but persistent presence of mobile malware calling back.

Data Exfiltration and Impact

After establishing command and control, adversaries often turn to exfiltration or direct impact. Data theft is rarely loud. Attackers favor slow and deliberate methods designed to fly under the radar. Rather than a single large transfer, stolen information is often broken into smaller packets, moved outside normal business hours, or tunneled through alternative protocols like DNS, File Transfer Protocol (FTP), or Simple Mail Transfer Protocol (SMTP). Comcast Business telemetry reflected this trend, with exfiltration over alternative protocols (T1048) appearing as one of the most frequently attempted late-stage techniques.

Impact actions follow closely behind. Palo Alto's Unit 42 reported that 86% of incidents they investigated in 2024 involved operational downtime, reputational damage, or both.[25] In other words, adversaries aren't only stealing data—they're disrupting business continuity as a means of creating leverage or sowing chaos.

The combined data makes clear that while the number of these late-stage detections is understandably much smaller than early-stage threats, they represent the most consequential moments of an attack chain. If exfiltration or destructive actions succeed, the result is often immediate business disruption, high recovery costs, and reputational harm.

Ransomware as an Endgame

Ransomware remains one of the most dominant impact payloads in 2025. Once footholds are secured and data is staged, attackers encrypt critical systems to halt operations and pressure victims into payment. Groups such as Cl0p[26] and Qilin[27] continue to refine their tradecraft, deploying ransomware at speed and scale across industries.

What makes ransomware especially challenging is the multi-pronged approach many groups now employ. Encryption is often paired with data theft, creating a "double extortion" model where sensitive files are stolen before systems are locked down. Even if victims refuse to pay for decryption, they may still face threats of public leaks or exposure of confidential information. The result is that ransomware incidents extend well beyond technical disruption—they can trigger legal, regulatory, and reputational consequences that persist long after systems are restored.

Wipers and Destructive Payloads

Not all attackers are financially motivated. Nation-state actors and politically aligned groups have repeatedly deployed wiper malware designed to irreversibly destroy data or corrupt systems. Cisco Talos, for example, identified "PathWiper" in 2025 being used against a Ukrainian critical infrastructure organization, delivered through legitimate administrative tools to maximize reach and disruption.[28]

Unfortunately, nation-state actors now regularly engage in cyber-crime activity to generate cash and fund state-sponsored priorities, including nuclear weapons development.[29] This blurring of motives means that even small and mid-sized organizations are now potential targets of groups operating out of adversaries. For these actors, destructive attacks and financial extortion are two sides of the same coin—tools to generate revenue, exert pressure, or destabilize adversaries.

[25] Palo Alto Networks, Global Incident Response Report 2025
[26] CISA, #StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability
[27] Office of Information Security, HC3: Threat Profile
[28] Cisco Talos, Newly identified wiper malware "PathWiper" targets critical infrastructure in Ukraine
[29] CISA, Cybersecurity & Infrastructure Security Agency – Nation-State Threats

SOC Casebook

Custom Detection Rules Help Protect Connected Devices

During an authorized penetration test, a consultant downloaded a staged payload from a remote server onto a workstation that was USB-tethered to a medical infusion pump.

The action matched ingress tool transfer (T1105) and triggered a Comcast Business written EDR detection rule: an unknown binary hash coupled with an outbound HTTPS fetch from an uncategorized domain.

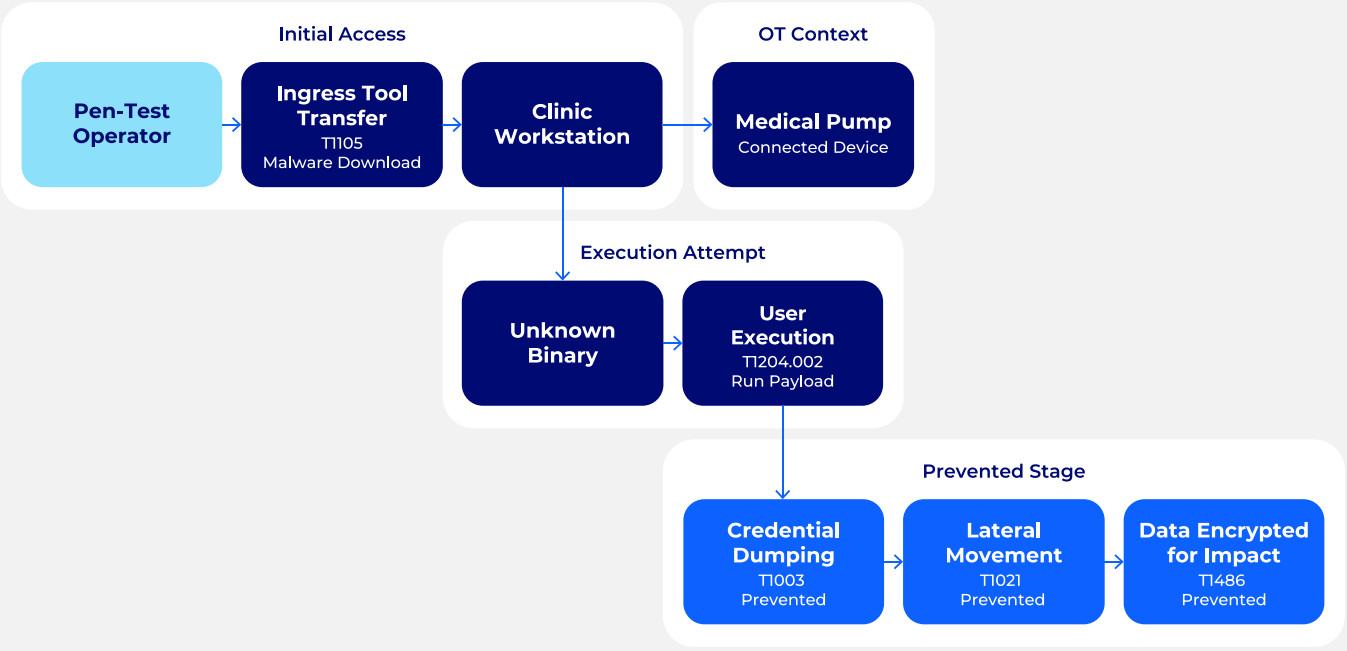
Seconds later the file attempted to execute (T1204.002), but before any post-exploitation steps could fire, Comcast Business MDR analysts quarantined the host and contacted the customer. Built-in EDR analytics and the customer's MDR platform recorded no alerts, underscoring the value of custom detections.

SOC Insights:

Custom rules close visibility gaps: Proprietary analytics surfaced a threat missed by default detection logic.

Early interruption stops the chain: Blocking execution at the download stage prevented credential theft, lateral spread, and encryption-for-impact.

Layered EDR + MDR shortens dwell time: Integrated monitoring reduced detection-to-response to minutes, a critical advantage against fast-acting malware.



DDoS: Escalating Scale and Sophistication

DDoS attacks have become a persistent threat to organizations of all sizes, and one that carries serious implications. A successful DDoS attack can result in business downtime that can lead to financial loss and reputational damage, especially if customer-facing services are taken offline.

Comcast Business detected 44,069 DDoS events last year, while research such as NETSCOUT's DDoS Threat Intelligence Reports from 2023 and 2024 show a 27.9% year-over-year uptick in detected DDoS attacks, pointing to a DDoS landscape growing in both size and complexity.[30]

According to our analysis, attackers now commonly leverage DNS amplification and reflection-based tactics, such as DNS NXDOMAIN ("water torture") attacks, to flood entire networks. We also saw a surge in "carpet bombing" DDoS, where attackers spread traffic across numerous IP addresses or subnets simultaneously to complicate mitigation. Such attacks can fly under the radar of defenses that focus on a single IP, overwhelming networks in aggregate. The net effect is a higher baseline of disruptive traffic that businesses must be prepared to absorb or deflect.

DDoS attack patterns have also shifted toward short, intense bursts used to probe defenses, identify vulnerabilities, or mask other cyber intrusions. In practice, a threat actor might unleash a 60-second blast of malicious traffic to degrade a victim's web servers, overwhelm a security appliance or just probe cybersecurity infrastructure. Geopolitical tensions further complicate the threat landscape, as politically motivated hacktivists like the pro-Russian group NoName057(16)[31] employ DDoS for disruption or propaganda, rather than monetary gain.

Much like we are seeing across other threat types, artificial intelligence is helping attackers augment DDoS attacks. According to NETSCOUT's 2024 DDoS report, AI is being used to bypass CAPTCHAs and enable more advanced capabilities like behavior mimicry and real-time attack adaptation. These developments make attacks more efficient and relentless while lowering the barrier to entry for attackers.

[30] 2023 NETSCOUT DDoS Threat Intelligence Report / NETSCOUT DDoS Threat Intelligence
[31] Netscout, The threat actor NoName057(16) has likely conducted over 1,500 DDoS attacks since March 2022

Recommendations for Strengthening Defense

The 2025 threat landscape is intensifying and evolving in complex ways. Adversaries are launching high-volume early-stage attacks, leveraging new tactics like residential proxy networks and AI-driven scams to conceal their activities, and continuing to exploit human weaknesses. This paints a challenging picture, but it also highlights where defenders should focus their efforts. To navigate these threats, consider a multi-layered, adaptive security strategy that includes SD-WAN, MDR/XDR, DDoS mitigation, and vulnerability management to help organizations address the following priorities.

Reinforce the Perimeter

Maintain strong preventive measures on the front lines. Application firewalls with unified threat management (UTM), strict identity and access controls, multi-factor authentication, and network segmentation can mitigate the risk to your attack surface. Many opportunistic attackers will move on to easier targets if they encounter well-fortified basic defenses.

Implement Robust Patch Management

Establish a routine for regularly updating and patching all software and systems, use automated vulnerability scanning tools to identify and prioritize the remediation of vulnerabilities, and develop and enforce policies so patches are applied promptly.

Deploy Advanced Detection and Response Technologies

Accept that some attacks will slip through. Invest in advanced detection and response capabilities to catch intruders quickly. This includes deploying AI-driven analytics and using EDR and extended detection and response (XDR) tools to spot subtle malicious behavior, as well as ensuring 24/7 monitoring via a security operations center (in-house or through a trusted MDR partner). The faster you can detect and contain an intrusion, the less damage it can do. Adopting a “when not if” mindset regarding intrusion means continuously hunting for signs of compromise and being ready to respond at a moment’s notice.

Empower People and Ease the Burnout

Security is ultimately a human endeavor. Organizations should invest in tools and services that amplify human analysts rather than overwhelm them with alerts that aren’t actionable. Automate routine tasks and enrich alerts with context so security analysts can make decisions faster. Consider managed services to extend your team’s capabilities (for example, an MDR partner to shoulder 24/7 monitoring and response). The goal is to reduce alert fatigue and staffing strain so your experts can focus on strategic initiatives without burning out.

Build a Cybersecurity Culture

Simultaneously, continue to educate and engage the general employee base, turning the weakest link into the first line of defense. A culture of security (where employees report suspicious emails and adhere to best practices) can thwart many attacker’s attempts at the initial access stage.

Rethink Risk Management

Adopt a modern risk calculus. Since not every threat can be eliminated, leadership must identify high-impact scenarios and consciously decide which risks to mitigate, transfer, or accept. Bolster this strategy by regularly practicing incident response and maintaining robust business continuity plans to ensure rapid recovery from an attack.

How Comcast Business Can Help

In the face of an ever-changing threat landscape, Comcast Business offers advanced cybersecurity and networking solutions, spanning secure SD-WAN, SASE, MDR and XDR, and DDoS Mitigation, to help reduce dwell time, and lower operational burden for security teams.

Our solutions include:

Secure SD-WAN with Advanced Security

Combines resilient software-defined networking with built-in Unified Threat Management (UTM) security controls, Next-Generation Firewall (NGFW), Intrusion Prevention System (IPS), URL filtering, and Data Loss Prevention (DLP), providing consistent policy enforcement and secure connectivity for users on-site or in the cloud. This helps ensure that your distributed locations and remote workforce can achieve optimized performance and enterprise-grade security at the network edge.

Secure Access Service Edge (SASE)

A unified, cloud-delivered framework that integrates networking and UTM security. Comcast Business's SASE offering brings together SD-WAN connectivity with advanced security functions—SWG, DNS security, Cloud Access Security Broker (CASB), Zero Trust Network Access (ZTNA), and DLP—under one centrally managed service. The result is adaptive security against user-dependent risk for threats like phishing, drive-by compromise, and shadow IT.

Unified Threat Management (UTM)

An all-in-one security platform that consolidates essential features—next-generation firewall, intrusion prevention, antivirus/anti-malware, web filtering, and more—into a single, centrally managed solution. UTM simplifies security management and provides comprehensive visibility across your network, helping to block commodity exploits and attacks before they reach your users or critical systems.

Managed Detection and Response (MDR)

24/7 threat monitoring and active cyber defense managed by our team of experts. MDR combines advanced threat detection technology with SOC-led human threat hunters who investigate and triage incidents in real time. Automated response contains or disrupts threats before a major security incident occurs. This service helps businesses quickly identify hard-to-detect threats, contain incidents, and reduce dwell time.

Vulnerability Scanning and Management

Proactive assessment services to identify, prioritize, and remediate security weaknesses in your IT environment. Regular automated scanning and expert analysis help you close gaps (such as unpatched software, misconfigurations, or exposed ports) before attackers can exploit them. Ongoing vulnerability management ensures your organization's "attack surface" stays as small and well-fortified as possible.

DDoS Mitigation Services

Network-based defenses against Distributed Denial of Service attacks. Comcast Business provides DDoS monitoring and mitigation that can identify unusual traffic spikes in real time and filter out malicious traffic bursts. These services help keep your websites, applications, and internet-facing services available even when under heavy attack, minimizing disruption and downtime.

Managed Endpoint Detection & Response (EDR)

Advanced endpoint security for computers that connect to your network, coupled with 24/7 threat identification and response by the Comcast Business SOC. Our managed EDR solution continuously monitors laptops, servers, and other endpoints for suspicious behavior, using machine learning to detect malware, ransomware, and other threats that evade traditional antivirus. When a threat is detected, the SOC's analysts can validate the alerts and, if EDR is combined with MDR, trigger automated containment actions to prevent the threat from spreading—helping prevent a single compromised device from turning into a widespread incident.

DNS Security

Offering network security for small businesses, SecurityEdge® is a cloud-based internet security solution that uses DNS filtering to help protect all connected devices on your network from malware, phishing scams, ransomware, and botnet attacks from bad domains. This easy-to-install cloud-based solution offers customizable web filtering with threat intelligence updated every 5 minutes.

Learn more about how Comcast Business can help protect your business today.

Learn more

COMCAST BUSINESS