Central Funding for Cybersecurity Tools to Ensure Holistic Visibility and Response

Initiated: 2022
Completed: 2024

Contact: James Weaver
North Carolina State Chief Information Officer
Secretary, N.C. Department of Information Technology
919-809-3845
james.weaver@nc.gov

NCDIT | NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Executive Summary

Recognizing the importance of protecting the state's government IT systems, data and assets from cyberthreats, the N.C. Department of Information Technology has prioritized central funding for a number of tools to ensure holistic cybersecurity visibility and response across North Carolina.

NCDIT's Enterprise Security and Risk Management Office (ESRMO) takes a whole-of-state approach to cybersecurity management, partnering with federal, state and local entities to gain and share insights that help inform cybersecurity policy and strategy statewide. Ensuring that entities have the technology they need to identify and respond to threats is critical to the success of this approach. Commonality in tools also allows the state to operate as a centralized security operations center, helping speed up response and giving an improved picture of the state's overall cybersecurity landscape.

Central funding for enterprise security at a whole state level started with the implementation of Tanium as a unified endpoint management and response tool that spanned across state agencies. This project began in 2018, and many of the department's optimized agencies adopted the tool as early as 2019. From 2022 to 2024, NCDIT successfully deployed the client to additional agencies including the state departments of Agriculture, Environmental Quality, Health and Human Services and Public Safety.

Expanding this effort, NCDIT secured funding in North Carolina's state budget for fiscal year 2024 to centrally fund Cloudflare, a web application firewall that provides edge protection for web applications and services, and CrowdStrike, which provides next generation endpoint protection for all executive branch agencies, for two years. NCDIT's goal is to secure recurring funding for these important tools to ensure key security capabilities are readily available at no cost to these agencies, eliminating a deterrent to implementation.

Providing enterprise security at a statewide level also allows NCDIT to obtain bulk discount rates and pass those savings on to other state and local entities that may not otherwise be able to afford the service. In many cases, the targets of cyberattacks are smaller entities that may not have the personnel, funding or resources to adequately prepare for and defend against cyberthreats, and their vulnerabilities can threaten the security of the entire state.

Idea

Web application firewall (WAF) protection plays a critical role in protecting state assets exposed to the wider public internet. It is a highly recommended component of any public-facing web application because it restricts public inbound traffic's would-be attack vectors on infrastructure to specified IP address ranges.

The service provides a scalable and easily implemented set of core protections from common attacks, including SQL injection, cross-site scripting and distributed denial-of-service. These core protections are managed and routinely updated at the enterprise level to enable additional protections from the latest exploits.

The WAF service is implemented on most web applications using a Domain Name System (DNS) proxy through Cloudflare. Changes made to the DNS when implementing Cloudflare can prevent the need to expose an individual load balancer or server Intrusion Protection System to the wider internet. Implementation of WAF includes the introduction of powerful real-time traffic monitoring tools to identify traffic that may be getting blocked, the type of traffic it is and where it originated. In addition, the visibility into traffic and potential campaigns targeting state infrastructure provides critical intelligence on who is targeting the public-facing infrastructure and what methods are being attempted.

CrowdStrike serves as an ideal complement to Cloudflare's edge protection by providing a cloud-native approach to enable customers to detect, prevent and respond to cyber threats effectively. It provides real-time visibility across all the state's endpoint devices and identifies abnormal activity so it can be addressed.

CrowdStrike has redefined security with its advanced cloud-native platform. The tool provides a lightweight, unified agent on endpoints for comprehensive protection. The cloud-native platform leverages real-time indicators of attack, threat intelligence and enriched telemetry from across the industry. The platform provides protection across endpoints (laptops, servers and workstations), cloud workloads and identity platforms. The CrowdStrike platform was an innovator within the industry and launched the next-gen security platform initiative, moving beyond previously detected threats based solely on indicators of compromise and developing detection capabilities leveraging heuristic behavioral based analysis and response. These features have enabled the ESRMO's ability to provide unmatched value to covered entities.

Both Cloudflare and CrowdStrike offer a multi-tenancy model that allows NCDIT to serve as the "parent" instance and various agencies across the state to serve as "child" instances. By providing these tools centrally, NCDIT's ESRMO can constantly monitor and assess alerts and events and then triage them and respond as needed. At the same time, each individual agency receives the same level of administrative control and security access, and their teams can directly observe and analyze the data as well.

This model enables statewide oversight and visibility that can be utilized for deeper intelligence and investigation of alerts and activity across the wide state landscape. NCDIT is able to provide agencies the direct ability to monitor and respond to security threats efficiently and quickly while maintaining broader visibility of trends and behavior that can help guide better statewide strategy to secure platforms and services.

Implementation

NCDIT has seen tremendous success in its implementation of Cloudflare and CrowdStrike.

There are currently 95 state agency root domains being protected within Cloudflare with over 400 DNS records held under those root domains across 20 agency accounts. Application developers and owners are provided training, resources and support from NCDIT. This ensures that applications can be added to the platform and managed by the teams working within the applications.

For CrowdStrike, NCDIT deployed more than 60,000 clients across the state over the past two years, including nearly 37,000 in just a few days. This deployment vastly improves the security

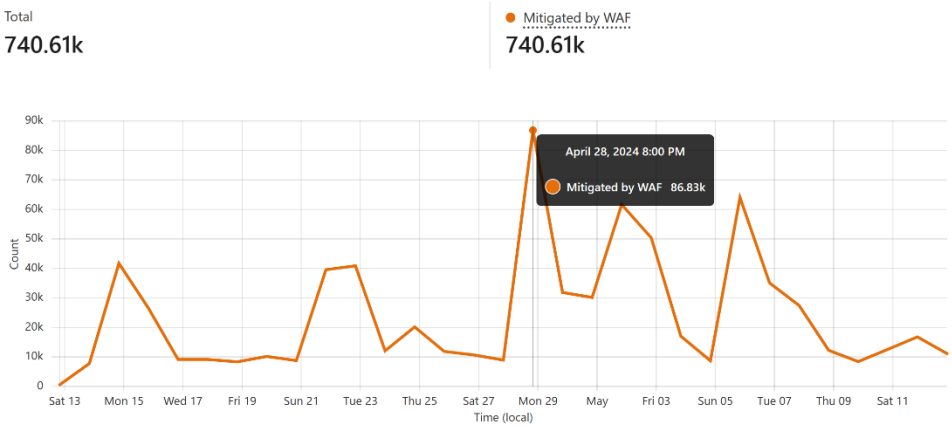
posture across the executive branch agencies and allows NCDIT's ESRMO to have global insight into rising cybersecurity threats that may be targeting various state agencies.

The rapid adoption of Cloudflare and CrowdStrike, in addition to the support of the federated tenancy model, allows individual agencies as well as the ESRMO to quickly identify threats to the state from endpoint devices, cloud workloads and public-facing web pages.

Impact

The implementation of both Cloudflare and CrowdStrike at agencies across North Carolina has played a significant role in helping the state prevent cyberattacks.

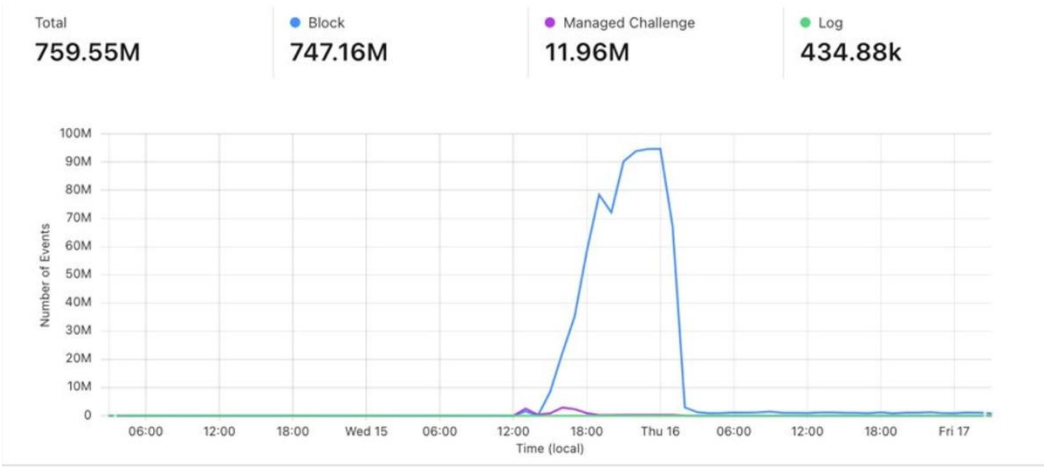
Among its benefits, Cloudflare provides increased security by blocking malicious traffic, improved performance by reserving compute cycles and memory for legitimate traffic, and simplified management through a dashboard that logs application traffic in real time.



Last 30 days of blocks from DHHS account

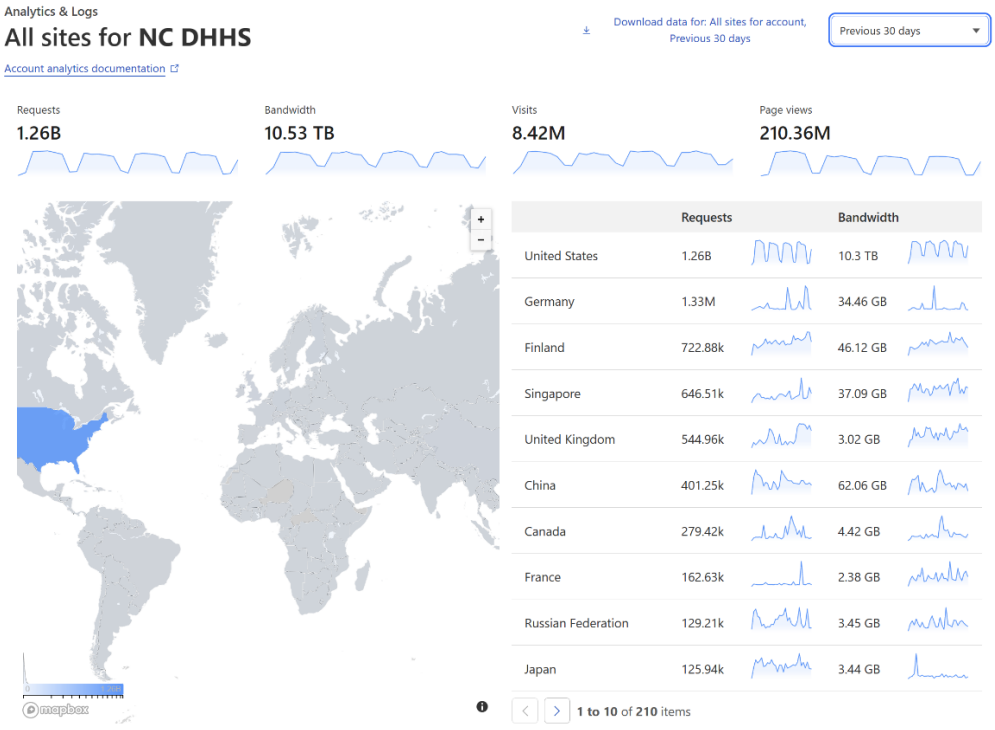
In the last 30 days alone, Cloudflare has blocked 1.1 million instances of malicious http/s traffic across 20 state agencies. For instance, at the N.C. Department of Health and Human Services, the Cloudflare WAF rules and toolset have blocked over 800,000 instances of malicious traffic or potential threat attempts, representing just a small sample from a single state agency.

Cloudflare's WAF service had a tremendous impact on a state entity that fell under a distributed denial-of-service (DDoS) attack in November 2023. The attack was successful and brought down the entire domain and application set. Although this entity was not a state agency, NCDIT was brought in to leverage the existing tool and assist with remediating the outage. Once the entity was onboarded to the Cloudflare WAF service, its site was returned to normal operation and began immediately blocking malicious traffic. At peak, around 1 billion malicious traffic blocks were logged in the entity's newly established Cloudflare account. The attacks and number of WAF blocks fell to zero immediately after deploying WAF on the applications.



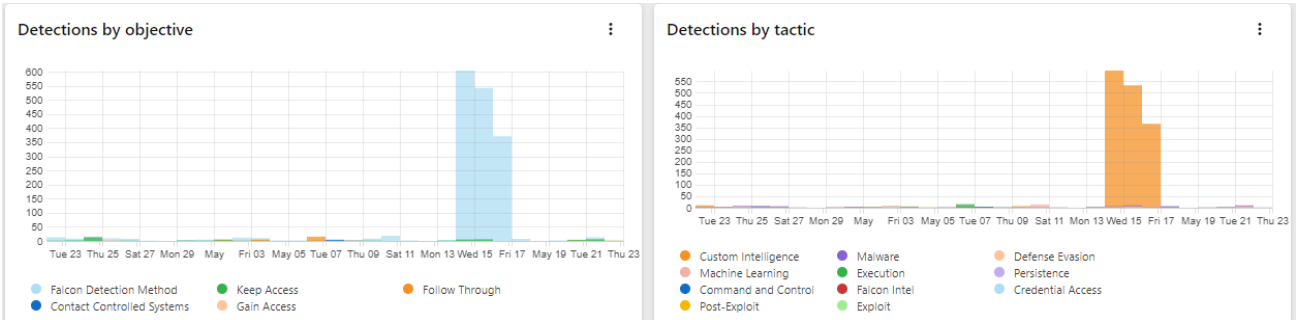
State Entity DDoS attack – November 2023

The robust security analytics tools and traffic logging on the Cloudflare dashboard grant application owners a fully customizable and live view of the traffic passing through the Cloudflare proxy. Developers and application owners have the ability to perform this granular level of traffic monitoring while also being able to deploy mitigation methods within the same dashboard.



CrowdStrike has been an essential part of the cybersecurity strategy in the enterprise environment. Through adoption of this platform as its primary Extended Detection and Response (XDR) solution, and its subsequent funding and roll out to state agencies, along with some county and local entities, NCDIT has increased the security posture, reduced risk and generally contributed to the ability of each covered entity to serve North Carolina. This deployment provides NCDIT's ESRMO with visibility to the threat landscape and facilitates its ability to ""hunt for bad" across the environment. This means that when NCDIT receives valuable information from its partners, it can utilize the CrowdStrike ecosystem to search, identify, contain and remediate threats more quickly and effectively than otherwise possible.

In the past 30 days alone, CrowdStrike has allowed the ESRMO to identify hundreds of high and medium severity incidents out of nearly 7,000 detected security events. This resulted in over two dozen true positive events in categories such as command and control, execution and defense evasion, many of which were aided by machine learning and CrowdStrike intelligence.



The identification of these threats and their actions allow the team, in conjunction with the state's Joint Cybersecurity Task Force support when needed, to quickly contain these threats and prevent them from becoming serious incidents such as theft of data, system outages and ransomware.

These two tools have allowed the ESRMO to provide a no-direct-cost, best-in-class resources that have proven value in protecting state, county and local agencies through a centralized approach that reduces the overall cost for these solutions and facilitates the additional support needed to quickly and effectively address cybersecurity threats as they arise rather than having to wait for another agency to become a victim.

Next Steps

NCDIT's goal is to secure recurring funding for Cloudflare and CrowdStrike. With these tools now in place, the department will proceed to extend coverage to any impacted local government entity needing temporary coverage or assistance. The protection and security posture of North Carolina's public-facing web applications and services is an ever-changing blueprint, and expanding coverage is of paramount importance to securing the state's resources, data and infrastructure. As the state continues to navigate the evolving landscape of cybersecurity threats, it is imperative to collectively prioritize and implement robust measures to safeguard digital infrastructure.

In addition, the ESRMO and the Statewide IT Procurement Office, both part of NCDIT, have worked together to streamline the procurement process for cybersecurity solutions, which previously consisted of multiple contracts. These cybersecurity software, products and services have been consolidated into a single, comprehensive contract that will better serve the needs of state and local government agencies, public schools, community colleges and the member campuses of the University of North Carolina system. It is a mandatory Statewide Term Contract for the use of executive state agencies and may also be used as an optional Convenience Contract by non-state agencies as permitted by law.

The Statewide IT Procurement Office anticipates that the solicitation for the new Cybersecurity State Contract will be publicly posted for bid by the end of May. Bid awards for each cybersecurity category will be determined by the ESRMO.