A HOLISTIC APPROACH TO CYBERSECURITY IN GOVERNMENT

INDUSTRY PERSPECTIVE

ThreatTrack®

EXECUTIVE SUMMARY

There are few issues more pressing in government today than cybersecurity. It's a national security matter that has gradually elevated from a back-office issue to one that the White House, Congress and governors across the U.S. now must plan for and address.

The stakes have become increasingly high as hackers routinely exploit known and unknown computer vulnerabilities and infiltrate government networks to steal sensitive data and cause harm. It only takes one click on a malicious email or file to unknowingly give hackers access to internal networks. That's why security experts divide organizations into two simple groups: those that have been compromised, and those that don't yet know they've been compromised.

With that in mind, what options do agencies have when it comes to detecting and defending against these attacks? How are today's security firms innovating to keep government networks safe? To learn more, GovLoop sat down with experts from ThreatTrack Security, a company with decades of cybersecurity experience, to answer these and other questions. In this report, you'll hear from ThreatTrack President **John Lyons**; **Jason Greenwood**, Senior Vice President of Marketing; and **Usman Choudhary**, Chief Product Officer.

After reading this report, you'll have a better understanding of:

- **The current cybersecurity landscape**
- **How agencies are tackling evolving cyberthreats and challenges**
- **ThreatTrack's layered approach to security that empowers security professionals**
- **Innovative capabilities ThreatTrack is developing to enhance government cybersecurity**

Let's begin with a brief overview of today's cyber landscape and how it has evolved over time.

UNDERSTANDING THE CYBER LANDSCAPE

Today's cyberthreat landscape is one security experts are familiar with, in terms of the types of attacks agencies face.

That's because attackers routinely use known vulnerabilities and exploits to breach sensitive networks, but they do so in subtle and clever ways.

"The malicious tactics themselves haven't changed all that much, whether it's a watering hole, or drive-by or phishing attack," said Jason Greenwood, Senior Vice President of Marketing at ThreatTrack.

The tools hackers now use, however, have become more sophisticated, and malware is changing from something static and reliant on brute force to something more dynamic and refined. For example, encryption technology allows attackers to encrypt parts of the malicious code so security tools cannot detect them as easily.

Polymorphic malware is also a growing problem, as attackers can now substantially change parts of the malicious code so it is more difficult to detect attacks through traditional analysis.

"Every one of those malicious codes is different, so you can't use signature-based detection in order to stop those attacks," Greenwood said.

Additionally, attackers are capitalizing on the wide use of email communication; spear phishing attacks are among the most prevalent tactics ThreatTrack has observed in the past 18 to 24 months. In spear phishing attacks, malware is disguised as a message from a trusted source, making it more difficult for recipients to realize the email is compromised. A significant change from previous spear phishing attacks, though, is that now the malicious code is much more likely to do extensive reconnaissance before exploiting the system.

In terms of Lockheed Martin's Cyber Kill Chain, a model that identifies what actions adversaries must complete to achieve their objectives, the focus for both attackers and security vendors is the delivery phase. For vendors, "this means concentrating on intercepting the threat prior to exploitation," Greenwood said. "But for malicious actors, it really means focusing on a reconnaissance phase, building highly targeted delivery systems that can exploit not only the main target of the attack but the target supply chain as well."

The defense industrial base is a prime example of this; attackers can target the ecosystem of organizations that work with the Department of Defense in order to gain a foothold inside government agencies.

Despite the consistency of attack types from the past to the present, the growing sophistication and focus on reconnaissance means there are several new challenges that agencies and security officers face.

TACKLING EVOLVING CYBERTHREATS & CHALLENGES

Cybersecurity isn't a new problem, and it's not getting easier; it's getting harder.

"The answer from the federal government is to try to create standards, so that all agencies will have to meet a common level of security and do this through compliance," said ThreatTrack President John Lyons. "But the problems you end up with are who decides what compliance should entail and how do you establish certification and policies around the type of tools that should be used. The other issue is once you've created these standards, who actually has the funding to buy the tools?"

Progress has been made on the funding issue, especially through the Continuous Diagnostics and Mitigation (CDM) program developed by the Department of Homeland Security and the General Services Administration. CDM provides agencies the opportunity to expand their continuous monitoring capabilities through more cost-effective access to security tools that they may not have been able to afford otherwise.

"The problem is that in an attempt to provide funding for universal federal compliance reporting, CDM greatly limited the types of solutions and vendors that were eligible in the program. This steered the federal market away from seeking solutions for their security problems and focused them on fitting their strategies around the only solutions for which funding was available," Lyons said.

In addition to limited consensus on which vendors should receive security certifications and what commitments should be expected from vendors, the growth of the Federal Risk and Authorization Management Program, or FedRAMP, a program to assess and authorize cloud-based offerings, has also created new challenges.

Traditionally, the federal government has used on-premise systems and developed security protocols with those types of systems in place. FedRAMP's growth, however, means a growth in cloud-based products, both on premise and off, which creates a new risk dynamic. Achieving the best possible results from security efforts will require a willingness to "go back and really look into what you should be monitoring, how you should be monitoring it and what the expectation is from the vendors that you'll allow to be certified," Lyons said.

The challenges associated with adapting to cloud-based services highlight the influence of the changing IT landscape. More and more agencies and organizations have hybrid environments, with a mix of on-premise and cloud-based services. Networks are changing, transcending from something in a building to something vast and mobile that involves contractors, remote employees and the cloud.

However, these challenge areas are where ThreatTrack excels.

A LAYERED APPROACH TO CYBERSECURITY

Agencies can't rely on reactive security defenses and techniques to keep pace with the frequency and sophistication of evolving cyberthreats.

They need security solutions that enable them to be nimble and adapt to their changing IT and business environments.

What agencies need is a layered security defense that ensures they're prepared to quickly detect and thwart malicious actors before they wreak havoc on government networks.

"The term layered security describes a defensive strategy featuring multiple defensive layers that are designed to slow down an attacker," according to SANS Institute, a nonprofit that specializes in cybersecurity training. "The military calls this deep defense or defense in depth."

This type of defense is not dependent on tools alone or solely human expertise, but rather a combination of tools and sound insight to ensure agencies are equipped to defend against a range of cyberthreats.

"The solutions we're building are very adaptive for this type of environment," Usman Choudhary, Chief Product Officer for ThreatTrack, said. "We account for the fact that you're going to be in this hybrid or mixed environment with cloud-based services and internal services, as well as a more amorphous notion of a network because the network is not only something that's in your building but it transcends your enterprise."

Agencies must also consider the explosion of devices connecting to their network — both government-issued and personal devices. That's why ThreatTrack's solutions provide complete coverage, including Web, email and bring-your-own-device (BYOD) environments, all the way to the endpoint. Its comprehensive suite accounts for all facets of agencies' hybrid environments.

"We're not only providing agencies with tools that are doing detection and prevention, but we're also creating and have solutions that are proactive in nature," Choudhary said. "Our solutions help agencies to simulate attacks and predict what type of risk they have before they're exploited."

The main priority for agencies is to clearly and quickly determine when an attack is taking place. But the issue they face is that many solutions stop at the detection phase. Instead, ThreatTrack examines the attack progression of what's taking place, so that agencies aren't blindsided if malicious activity isn't completely rooted out of the network and later resurfaces in another form.

"We show the attack progression in a way where it really reduces the time you otherwise would've spent chasing after false positives," Choudhary said.

If you consider the nature of most targeted attacks, they usually don't involve a bad actor sending a single piece of malware to an individual. In many cases, attackers mount broad spear phishing campaigns by sending seemingly legitimate emails to a host of people in an organization. The attackers cast a wide net, but they often use a specific type of malware that's trying to find the path of least

> ***THE TERM LAYERED SECURITY DESCRIBES A DEFENSIVE STRATEGY FEATURING MULTIPLE DEFENSIVE LAYERS THAT ARE DESIGNED TO SLOW DOWN AN ATTACKER."***
>
> - SANS INSTITUTE

resistance to penetrate the network. Or they may use various types of malware and direct that malicious code at a particular role within an organization, such as a system administrator or chief financial officer.

ThreatTrack aggregates data on these types of attacks as they're unfolding and shows the correlation between the current attack and previous attacks with similar characteristics.

"We give you that historical view, but in a real-time context," Choudhary said. "It's important to have that data at your fingertips because that is the critical time when you can stop the attack from spreading."

"We want to make sure that whoever's analyzing this doesn't miss the forest for the trees," Choudhary added. "A lot of other solutions focus too much on the trees, and we're trying to raise that bar to look at the forest – the holistic view of the environment."

ThreatTrack's deep knowledge in the cybersecurity space — particularly in responding to advanced persistent threats and malware — spans decades, and that knowledge is infused into the company's solutions. The benefit for agencies is they don't have to invest heavily in services to supplement those solutions. To help agencies see the big picture when it comes to network security, ThreatTrack solutions provide automated warnings of future events and immediate issues that should be addressed.

But timely and accurate information is only valuable when the people who need it the most can understand it and use it to make better decisions. ThreatTrack developed its solutions with two primary user groups in mind: security analysts and IT network staff. Data is tailored to fit the needs of these and other user groups or personas.

For example, ThreatTrack can provide security analysts with analytics, specifically insights showing them what happened leading up to a cyberattack and whether that type of attack has ever been used against the organization. The ability to view aggregated data in a format that's appropriate to an employee's role can save time that is vital to subverting an attack.

"We built a framework that services data about what else is happening on the host besides the malware attempting to attack or infiltrate that host, and the data is in business terms that you can understand," Choudhary said.

But ThreatTrack's efforts to empower and equip government security personnel don't stop there. The company's team of cyber experts are constantly innovating to provide greater insights and visibility to those charged with securing the network.

HOW THREATTRACK INNOVATES IN CYBERSPACE

One of the few constants in the world of cybersecurity is change.

Security tools and defenses must evolve as threats become more sophisticated and destructive in nature. If not, agencies will always be steps behind their adversaries. That's why innovation in the security space must be a priority for government and its ecosystem of partners.

For ThreatTrack, innovation has taken on many forms over the past two decades. Machine learning inside of the network is one example. Today, many online companies and service providers use machine learning to track user viewing and buying habits, and they use that data to make recommendations based on the user's preferences.

"We plan to take our machine learning algorithms that we have around malware and also use those for looking at behaviors inside your network," Choudhary said. "We want to quickly identify anomalous and suspicious activities and separate them from the false positives. So we're using these learning techniques that are dynamic and can learn from your environment."

Using machine learning, ThreatTrack can profile all the activity on the network and establish a baseline of typical user behavior. When there's a deviation from that behavior, organizations can use that information to learn about the network and attacks coming into their environment. If it turns out that anomalous activity isn't malicious but perhaps a system glitch, there's also a lot agencies can learn from that information.

"So it's not just about anomalies but also learning about your threshold of risk," Choudhary said. "Our goal is to have this whole process automated. That's what we've done with the first part of our solution, and we're continuing to go down that path."

For agencies to be effective, automation and visibility are key. Unfortunately, security professionals at major corporations and agencies alike don't always have the level of visibility required to make those determinations. From a security perspective, organizations have mainly focused on stopping the delivery of malicious payloads.

"They haven't focused on the fact that everyone gets infected, so after that happens, what's next?" Choudhary said.

Traditionally, security tools have failed to link that type of threat information and activity to the network activity inside an organization.

"That part has been missing, and that's where our solutions excel," Greenwood said. "They look at the behaviors that are happening from a network, user and endpoint perspective, to identify those potentially malicious activities that are going on inside an agency's network."

Plus, ThreatTrack's solutions are designed to work together and provide users with a holistic view of activity across their network. In the current marketplace, vendors typically develop a suite of solutions from new capabilities acquired through acquisitions and mergers. The challenge, however, is integrating those solutions.

"As an organization, we're taking a different approach than some of the other players in this space," Lyons said. "We provide a complete solution for agencies, but we're very focused on how we fit into their existing security infrastructure."

Cybersecurity is a team sport that requires coordination and innovation between government and industry, both now and for the foreseeable future. ThreatTrack's team of experts understands that collaboration is key and can help build a holistic approach to securing government agencies.

> “AS AN ORGANIZATION, WE’RE TAKING A **DIFFERENT APPROACH** THAN SOME OF THE OTHER PLAYERS IN THIS SPACE. WE PROVIDE A COMPLETE SOLUTION FOR AGENCIES, BUT WE’RE VERY FOCUSED ON HOW WE FIT INTO THEIR EXISTING SECURITY INFRASTRUCTURE.”
>
> - JOHN LYONS, THREATTRACK PRESIDENT

ABOUT THREATTRACK

ThreatTrack Security specializes in helping organizations identify and eliminate advanced threats, targeted attacks and other sophisticated malware that are designed to evade the traditional cyber defenses deployed by enterprises and government agencies worldwide

ABOUT GOVLOOP

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 250,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.

govloop

1152 15th Street NW, Suite 800 Washington, DC 20005
Phone: (202) 407-7421 | Fax: (202) 407-7501
www.govloop.com
@GovLoop