A GOVERNMENT TECHNOLOGY Q&A

government technology

Strengthening security and improving responsiveness with limited resources

State and local governments are once again finding their resources strained as they deal with a COVID-19-related spike in citizen demand for services. At the same time, they must deal with new cybersecurity threats as remote work multiplies network connections.

These problems don't have easy solutions. But in this *Government Technology* Q&A, Jared Pane, principal solution architect at Elastic, discusses simple ways agencies can improve the citizen experience and make their online work environment safer without busting the budget.

Jared Pane, Principal Solution Architect, Elastic

Q: Staffers working from home are struggling to handle a record number of claims and questions. How can today's technology help them deliver these resources faster?

Pane: By leveraging the power of search, agency employees can find the information they need much faster. They can also make it easier for citizens to answer questions on their own, conserving staff resources.

When agencies connect a unified search experience to their internal content, a search engine does the work of combing through disparate data sources quickly to deliver relevant results. With unified workplace search, it doesn't matter whether content is in a document folder, an internal shared drive, or a cloud-based app – the search engine finds it. Managers can set access parameters to ensure only qualified people see sensitive information.

Agencies can also add a search bar to the front end of their websites for citizens. The engine uses metadata to deliver appropriate results, so someone who wants to renew their vehicle registration isn't directed to information about obtaining a driver's license.

Creating a search bar from scratch is notoriously difficult and expensive, but Elastic's ready-made search products are quick to install. Built-in analytics show what people are searching for and the quality of the results, so agencies can tweak the system to make improvements.

Q: State and local agencies are likely to experience financial difficulties for some time, making technology modernization difficult. Is there anything they can do to improve the performance of existing networks and apps?

Pane: Gaining better visibility into app and system performance helps a lot. When administrators are trying to address an issue, they typically hold meetings with various IT teams and it can be difficult to track down the source of a problem.

When finances are tight, open source technology represents an opportunity for agencies to build and deploy unified solutions quickly, without upfront costs and contractual entanglements.

With Elastic's free and open, unified solutions, agencies can see logging, metrics, application performance, and uptime across the entire network infrastructure, all from one place. This reduces problem resolution time from hours to minutes, giving staff more time to concentrate on higher-level tasks.

Q: Hackers are taking advantage of remote workers – cyberattacks have surged 400 percent during the COVID-19 pandemic.[1] What can agencies do to help security teams respond better to threats?

Pane: For effective cybersecurity, agencies need a 360-degree view of what's happening on the network. That means security teams need to consider all of the data in their systems. Some providers charge by volume, forcing agencies to pick and choose what data to put in. But if you can't put all your data in, how do you know if you have a breach?

It's important to find a provider that offers a standard fee, allowing agencies to scale. Once all data is in a security system, machine learning, dashboards, and alerting can be applied to spot anomalies and respond in real time.

Q: How can governments protect the growing number of device endpoints from phishing attempts and other attacks?

Pane: Employees working from home should start by using a VPN with two-factor authentication. But a VPN is still a network connection. All it takes is one person to open a bad link or attachment and you've got a virus or malware in your system.

Endpoints are most likely the first point of attack on an agency. To stop attacks, you need to have an endpoint monitoring system on every device. With endpoint monitoring and detection, a bad file may be downloaded, but it will be prevented from detonating. IT can easily locate, quarantine, and analyze it in a secure, isolated environment and then make system changes to ensure it doesn't get in again.

Contact sled@elastic.co for more information.

1. https://www.msspalert.com/cybersecurity-news/fbi-covid-19-cyberattacks-spike-400-in-pandemic/

© 2020 e.Republic. All rights reserved.

elastic

Search. Observe. Protect.