SECURING DIGITAL INFRASTRUCTURE

A GOVERNMENT TECHNOLOGY Q&A

What is XDR? And How Can It Help Keep Governments Secure?

Extended detection and response — or XDR — is an emerging endpoint-management technology that's becoming increasingly important in governments' efforts to safeguard their digital assets. In this Q&A, Jason White, a federal solutions architect with Trellix, a leading XDR platform, provides a concise overview of the value of endpoint management and the growing importance of XDR for state and local government organizations.

Q / What are the biggest challenges in endpoint management for government agencies today?

With hybrid work environments becoming standard, agency leaders struggle to assess the true security of the devices accessing their networks. Part of this is because device posture is constantly evolving as users interact with internet applications that could bring new threats into the network environment. Before agencies authenticate and validate a device, they must make sure it's in a condition suitable to connect to agency resources.

Q / How does XDR help agencies cope with endpoint security challenges?

There's a big push right now for endpoint detection response (EDR) capabilities across federal, state and local government agencies. The EDR market has taken off because it can surface threats that perhaps weren't detected by scanning files or scripts in an endpoint. Moreover, EDR can pull together multiple behaviors to get a better understanding of not just a specific threat, but how that threat targets a set of systems.

The evolution of that is extended detection response (XDR), where we pull telemetry data from a Zero-Trust architecture from networks, endpoints, clouds and the web into a single platform that can surface advanced attacks against devices and other endpoints. Ultimately, XDR helps us continuously decide the proper level of authentication and validation for each particular device.

Q / Zero-Trust security is a complex approach that requires continuous validation of every device, application and user in a network. One critical component of Zero-Trust adoption is a maturity model. Why is this important now?

The U.S. government requires federal agencies to move to a Zero-Trust architecture by 2024. They're also providing a tremendous amount of Zero-Trust resources, many of which have value outside of the federal government.

As part of this effort, the Cybersecurity and Infrastructure Security Agency (CISA) recently released a Zero-Trust maturity model[1] that allows organizations to understand the beginning and intermediate steps, and then, ultimately, what a mature Zero-Trust model looks like. Technology is really only going to be part of the challenge here.

Q / How will governments have to invest in technology in the evolution toward XDR?

There's no easy answer. Organizations will have to put together a lot of moving parts that might be in silos or segmented for security. It has to start with the investment they are willing to make internally to change their operating procedures and then assessing the tools they already have.

Q / What do agencies often overlook when managing endpoints in this evolving landscape?

In a dynamically shifting threat landscape, they need the ability to provide context to threat intelligence, which allows them to be predictive and proactive on defending their devices.

A critical step sometimes gets lost when people say, "Oh, I've got EDR; I've got machine learning." Yes, but are your making that intelligence actionable? The more agencies can make threat intelligence actionable, the better they'll be able to stay ahead of the emerging threat landscape.

[1] https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf