CYERA | EBOOK

Beyond DLP: Embracing the New Necessities of Data Security

Cyera's Yotam Segev on Need for DSPM and Enhanced Data Protection in Age of Gen AI

Yotam Segev

Segev has more than 15 years of experience in the software industry. He previously served as the head of the cyber department for Israeli Military Intelligence, Unit 8200, where he co-founded and ran the unit's cloud security division. Segev assumed that role after completing the Israeli Defense Forces' Talpiot program, where he served as cyber team lead. He is a frequent speaker at industry conferences and events and a recognized thought leader in the technology, data security and cybersecurity fields.

Data loss prevention tools have served their purpose over the years but because of their inflexibility and pushback from users, they never really caught on. It's time to adopt the more dynamic approach offered by data security posture management, said **Yotam Segev**, co-founder and CEO at Cyera.

Digital environments have become increasingly complex as employees use external AI engines and large language models to analyze data, which is creating a "very stressful situation" for security teams. Organizations should embrace the proactive capabilities of DSPM before it's too late, Segev said.

"At the heart of that is the ability to differentiate between the data that matters and the data that clutters. We're absolutely fine with 98% of our data going outside to these LLMs. But there are specific data types, documents and information that we don't want to make it there, and we have to be able to find it to stop it from going there," he said.

In this video interview with Information Security Media Group, Segev discussed:

- The need for organizations to adapt to the changing digital landscape to secure their sensitive data;
- The integral role of DSPM in modernizing data security frameworks;
- How Cyera customers are using DSPM to gain unprecedented visibility over data.

> “The new approaches are allowing people to achieve data security goals and objectives and to protect data better and do it in a way that doesn’t get in the way of the business, doesn’t interrupt the business workflows and doesn’t create friction.”

New Approaches to Data Security

TOM FIELD: Too often, we give data security short shrift. We don’t talk about it nearly enough. What was the past focus on data security, and where do you believe we’ve fallen short?

YOTAM SEGEV: In the past, a lot of the data security efforts went toward data loss prevention. DLP is a way to try to catch the data at the last minute as it’s leaving the environment. That approach created a lot of friction with the business and a lot of anxiety for CISOs. Many people tried to implement these technologies and did not get the results they wanted, were not able to maintain it over time and found that it created more problems for them than value. That sometimes left a sour taste in people’s mouths with regard to data security.

The new approaches – DSPM or data security posture management, first and foremost – are allowing people to achieve data security goals and objectives and to protect data better and do it in a way that doesn’t get in the way of the business, doesn’t interrupt the business workflows and doesn’t create friction.

Data Security Is the New Necessity

FIELD: You have referred to data security as the new necessity. Why is that true now?

SEGEV: “Why now” is first and foremost generative AI. We always knew we have a problem. We always knew the problem is not solved. But with gen AI hitting the enterprise, this problem is getting more severe each day. Organizations that won’t step up and put the right programs in place today will find themselves in a very sticky situation faster than we all imagined.

Keeping Certain Data Out of LLMs

FIELD: Talk about the impact of the emergence of gen AI. We hear about organizations that don’t have proper governance and people that might be using private data on their public LLMs.

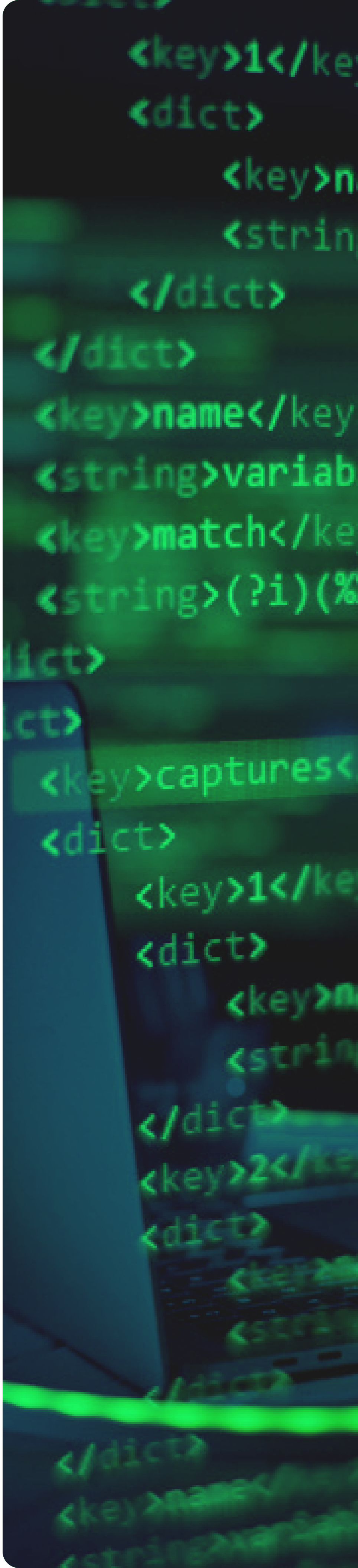
SEGEV: It starts simply with the classic problem of DLP – what data lives on our organization into where. But in this new reality, where every employee in the enterprise can very easily accelerate the workflows and get amazing returns by using public web-hosted LLMs, these LLMs are not necessarily the place we want our proprietary data to live. It's becoming a very stressful situation. At the heart of that is the ability to differentiate between the data that matters and the data that clutters. We're absolutely fine with 98% of our data going outside to these LLMs. But there are specific data types, documents and information that we don't want to make it there, and we have to be able to find it to stop it from going there.

Providing Visibility and an Asset Inventory

FIELD: How is Cyera tackling data security to help customers know what to secure and how to secure it?

SEGEV: First and foremost for us is visibility. We need the ability to connect to all of the enterprise ecosystems – be that SaaS, IaaS, PaaS, on-premises and, in the future, endpoint network email as well – and be able to use machine learning and AI to understand what data lives there and give the central teams in the enterprise – the security teams and compliance teams – visibility and an asset inventory around data. What data do we have, and where does that data live?

Because so many systems are so different from each other, it can be difficult to get a simple answer to that question. What does Office 365 have to do with an SRE bucket in an MS SQL database in Azure with a Snowflake data lake? All of these systems are so different, and the security teams can't handle that complexity. They're looking for a way to simplify and get a concise answer to that question, and that's the first step of every security program we've ever undertaken. What do we need to protect? What's the inventory? What's the asset inventory that we're looking to secure here?



> “We are no longer going out to do security for security’s sake. We can improve our security but at the same time get amazing benefits in cost savings by identifying all the junk we have lying around this extensible garage we live in in the cloud and cleaning that up and recouping the costs.”

Data Security as a Business Enabler

FIELD: Resources can be tough to come by these days. What are your recommendations to security and technology leaders about how they can build their business case around data security and get the board’s attention?

SEGEV: These days it’s easier than it ever was before. Many boards understand that data is the new lifeblood of the organization, and if we’re to maintain a competitive advantage, we have to be able to protect our proprietary data that makes our business unique, makes our company unique and allows us to service our customers better than anyone else. And that data comes in very different shapes and forms for different verticals and businesses. I haven’t met a company that doesn’t have some types of data they really want to keep to themselves and be the only ones leveraging. That is a pretty clear understanding at all levels of the stack today. More than that, when CISOs pursue these objectives and projects, they have a valuable position to provide to each of their peers.

We are no longer going out to do security for security’s sake. We can improve our security but at the same time get amazing benefits in cost savings by identifying all the junk we have lying around this extensible garage we live in in the cloud and cleaning that up and recouping the costs. We get amazing value by being able to accelerate data cataloging initiatives and help to develop and take to market data products – whether it’s propriety in-house gen AI products or the classic solutions that we’ve been working on for years – and be able to assist the enterprise by putting in a foundational layer that will be crucial for everything that is happening in the next 10 and 20 years of data the organization is generating.

How is that data being generated? Where does it live? How much of it do we have? What’s unique, and what’s not? By answering those questions, CISOs can become a true business enabler and provide value to the entire enterprise.

Results for Customers

FIELD: What results are Cyera’s customers seeing? Are they starting to clean up their virtual garages?

SEGEV: They are. We have customers that are very focused on the cloud savings, cost savings and use cases as a main driver to allow them to justify the project. They're seeing incredible returns that more than pay for the project itself and allow them to improve their security while also becoming more efficient. We have many customers that are seeing this tool, this product, this platform, open up interaction within the enterprise in a different way.

Here's an example: When I asked CISOs in the past, "How do you inventory data?" they told me, "We survey application owners. We go one by one through the tens, sometimes hundreds, of application owners and we ask them what data they are collecting in their application and how they are keeping that data secure." The reality is that oftentimes the application owners don't know. We are seeing other customers informing the application owners, enriching them with more insight and understanding of what their business is doing, than they have had before. And that's being highly valued by the business.

Questions to Ask

FIELD: What questions should security and technology leaders watching this interview be asking within their own organizations about how they're securing data?

SEGEV: The first question is: "What are the crown jewels? Oftentimes we thought about that as a separate question from the technical discovery classification, but the reality is that today, data moves and changes so fast that you can detach these two aspects in order to have a clear take on what the crown jewels that put the company at risk are. You have to be doing automated data discovery and classification. Otherwise, you might be missing out on a lot of things that your organization is collecting that you don't even know about. The first reaction we're getting from our customers, even at the POC stage, is that they are finding out about data that they never imagined the organization is collecting.

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 36 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® · CU INFO SECURITY® Just for Credit Unions · GOV INFO SECURITY® · HEALTHCARE INFO SECURITY®

infoRisk® TODAY · CAREERS INFO SECURITY® · Data Breach® Prevention. Response. Notification. TODAY · CyberEd.io

CIO.inc · DeviceSecurity.io · PaymentSecurity.io · FraudToday.io

CYBER THEORY · CyberEdBoard · Xtra mile LIFECYCLE MARKETING · GREYHEAD

iSMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io