Security Pros Share the Secret to Data Resilience

Here's a stat that might drop your jaw: About 90% of the world's data was generated in the last two years.

"I think a lot of us are trying to figure out how to become better swimmers because we're all drowning in data," said Bill Oyler, Practice Director, Professional Services, Data Center at Presidio.

The good news? Organizations are finally starting to figure out how to take advantage of this rising tsunami of unstructured and structured data without exposing themselves even more to cyber threats. But, there's a learning curve.

In our recent Tech Talk, "Proactive Data Defense: Combating Cyberthreats in a Rapidly Evolving Landscape," Oyler and Talbert Houle, Principal Security Consultant at Presidio, chatted with Jason Walker, Director of Technical Strategy, Cyber Resiliency at Pure Storage, about how enterprises can take advantage of their increasing amount of data while keeping it secure.

The AI Data Challenge

Hype or not, AI data is changing the way companies manage their infrastructures, forcing them to adopt ever more flexible solutions to future-proof their data storage.

"I think what's really exciting is that AI is about 75% less expensive on premises versus in the public cloud, so we're kind of starting to see a re-emergence of on-premises solutions," Oyler said. About 80% of the world's most critical data now lives on premises, he added, and having access to that critical data is key to enabling all this new AI technology.

As we all know by now: "Garbage in, garbage out; gold in, gold out." Your data analysis is only ever as good as the data that feeds it.

"If I'm a bad guy or even if I'm just an unknowing participant of someone who's adding information that an AI system's going to consume, I need to make sure that data is good," Houle said.

Bad information can create AI data-related scenarios that genuinely impact an organization's ability to use its data productively and proactively. That said,

measures like the new EU AI Act are providing companies with a framework to gauge their AI data security preparedness.

Still, all companies are going to have to face the issue of scale.

Living in the World of 300-terabyte Flash Modules

All-flash arrays are rapidly becoming the future of AI data storage for their speed, efficiency, and simplicity. But with 300-terabyte flash modules now on the radar, quick, efficient, and sustainable scalability has become paramount for any organization working in the shadow of the data tsunami.

“It’s interesting because we’re running into all these weird bottlenecks that we never had before, like a PCI bus,” Oyler said. “We’ve been talking about switches in the 800 gigabits per second range, which is unfathomable.”

Cost comes into play here, too, because if you’re putting all this data into the cloud, your cloud storage costs are going to skyrocket, but data storage in the age of AI doesn’t have to be expensive.

Pure Storage, for example, offers all-flash, capacity-optimized storage systems that are far more economical than disk-based storage with a competitive acquisition cost at under $0.20 per GB, including three years of service. This not only saves money but rack space and energy—a key advantage for ESG initiatives.

Privacy, Visibility, and Defense in Depth

But anywhere you have lots of data, you also have lots of risk. A recent survey found that 86% of IT leaders place the reduction of their organization’s risk profile as their top priority.

How are enterprises keeping up with the changing data landscape? Improving data privacy has become probably the biggest flashpoint, with things like GDPR, California’s CCPA, and the EU’s DORA cropping up.

“These privacy laws are starting to become even more strict, so it’s extremely important to have good controls to know where is that data, how is that data being used, and do I have a way to be able to prove that if the customer or a person wants to know where all this information is, I can show it and I know that I can prove that it’s been deleted from all these locations,” Houle said. “These capabilities are extremely hard to get and most organizations don’t have them.”

Things like NIST CSF 2.0 and the federal government’s zero trust maturity model

are helping organizations measure where they're at for data protection, but usually, it's just a matter of when, not if.

"Zero-day attacks, they're almost impossible to stop, so really it gets down to the point of once you become breached, can you actually detect and can you prevent further spread," Houle said.

And that's why getting back to the "fundamentals" is so important, Houle stated. These fundamentals include having good data visibility and good layered defense in depth to address the inevitability of data breaches.

Segmenting the Growing Attack Surface

"The more data, the more points of inference that an individual can get access to, and the larger the attack surface becomes," Houle said.

Endpoints, servers, IoT devices—they've all become newly accessible entrance points to cybercriminals, making organizations more vulnerable than ever to attacks. "Basically with all this new flexibility that we're getting comes all this new responsibility that we now have as engineers," Oyler said.

How to protect your data? "MFA is of course extremely important," said Houle, "as is awareness, and also logging, which is critical to both detection and response." And there's also segmentation—meaning, installing critical data storage systems in secure places with strict access controls.

Good and consistent disaster recovery doesn't hurt either, Houle added, and that's where the idea of tiers comes into play.

The New Resilience Imperative: Tiered Storage Architectures

A tiered data storage architecture assumes at least one system is going to be compromised and builds in layers of safety to protect the other parts of that system, or other systems, from also getting compromised.

"Multiple tiers of protection is really the key," Oyler said. "And we're talking about at least three tiers of protection." These tiers can be things like snapshots, replication, and immutability.

But achieving a true tiered data storage system and becoming cyber resilient doesn't just happen by snapping your fingers.

Watch the entire tech talk to learn about creating a data protection plan that prevents disruption from things like unplanned outages.