PROFILES IN *Confidence*

RICK ORLOFF

CISO

Everpure

Headquarters: Santa Clara, CA

Employees: 6,000+

Annual Revenue: $4 Billion

Rick Orloff leads security at Everpure, formerly Pure Storage, shaped by years of experience navigating evolving threats and business challenges. His perspective reflects a broader shift in cybersecurity leadership, one that moves beyond prevention and more toward resilience and enabling the business to move faster without necessarily increasing risk.

At Everpure, Rick focuses on building a strong security program, grounded in fundamentals and complimented with leading edge capabilities.

RESILIENCE IS KEY

For Rick, resilience is not a response to today's environment, it is the baseline requirement for operating in it. As geopolitical tensions and economic pressures continue to evolve, security programs must be built to withstand disruption, not just prevent it.

"Relying on resilience is not new," he says. Rather than treating each new threat as a separate problem to solve, Rick believes organizations need a durable foundation that can absorb change. A well-designed resilience strategy allows teams to adapt as new risks emerge, without needing to rebuild their approach each time the landscape shifts.

"If you do not have a resilience program already, you are doing something wrong," he explains.

This shift reflects a broader evolution in security leadership. The goal is no longer just to defend against specific threats, but to ensure the organization can continue to operate and recover quickly, regardless of what those threats or global changes may be.

FROM PREVENTION TO CONTAINMENT AND RECOVERY

Rick also highlights a fundamental shift in how CISOs think about security. "Threat actors are probably going to get in at some point," he says.

As a result, the focus has moved away from trying to build impenetrable defenses and has moved toward controlling impact. Rick explains that leaders are now asking different questions. How do we minimize exposure? How do we reduce blast radius? How do we recover quickly? Can we operate while experiencing technical interruptions?

This evolution reflects a more realistic view of the threat landscape. Security is no longer defined by keeping attackers out, but by how well an organization can respond when something goes wrong.

STRUCTURING AI WITH CLEAR GUARDRAILS

As AI adoption accelerates, Rick approaches it with a structured framework designed to balance enablement with control. "I structure AI as a swim lane," he explains.

On one side are governance and risk controls, including policies, identity management, and oversight. On the other are technical controls that define how AI systems interact with data and environments along with the ability to identify deviations.

Rick says that identity is one of the key principles. Each AI system must operate with its own unique identity and clearly defined permissions based on the Principle of Least Privilege. This prevents overexposure and limits the potential impact of misuse or compromise.

Equally important is controlling access to data. AI systems should only be able to interact with the specific data sets required for their function, with monitoring in place to detect any deviation. "If it goes anywhere else, I get an alert," Rick

explains.

This combination of governance and technical enforcement creates a model that allows organizations to adopt AI confidently while maintaining control.

ENABLING THE BUSINESS WITH AI

Rick is clear that the role of security is not to block innovation, but to support it. “From the executive level, it is more about how we can enable AI,” he says.

Business leaders expect security to manage risk, but they also expect security to help accelerate adoption of new technologies. That requires a structured process for evaluating and approving tools without introducing unnecessary friction.

At Everpure, that process is grounded in clarity. If a tool does not meet core requirements including identity management or data protection, it is not approved. If it does, it can be enabled quickly and safely. This approach positions security as a partner rather than a barrier.

AI AS A FORCE MULTIPLIER FOR TEAMS

Rick also sees AI as an opportunity to elevate how security teams operate.

“If AI is replacing my folks, I have them doing the wrong job,” he says.

Rather than eliminating roles, AI allows teams to shift focus. Routine tasks and lower severity issues can be automated, freeing experienced professionals to focus on more complex and critical work.

“If I can have AI handle my lower severity stuff, I can have my top talent focus on critical things,” he explains.

This shift is not about reducing headcount. It is about increasing impact and ensuring that teams are working on the problems that matter most.

A NEW SECURITY DOMAIN EMERGING

Looking ahead, Rick expects AI to fundamentally reshape the structure of cybersecurity itself. “I think there is going to be a whole new specialist area, a whole new security domain purely on technical AI security controls,” he says.

As AI systems become more autonomous and capable, they will require new skill sets and specialized controls.

Rick comments that this evolution mirrors previous shifts in the industry, such as the rise of cloud security, but with greater speed and broader impact.

ADAPTING TO CONTINUOUS CHANGE

Rick has seen this pattern before. New technologies emerge, are initially resisted, and eventually become foundational.

“Back in the day, I was one of those guys that said I am not putting my company data in someone else’s cloud,” he recalls.

Today, cloud is standard. He expects AI to follow a similar trajectory, but at an exponential pace eclipsing Moore’s law.

His focus is on building a program that can evolve alongside that change. One that combines resilience, structured governance, and strong fundamentals, while enabling the business to take advantage of what comes next.