TAG Security Annual 2023

SPECIAL REPRINT EDITION

EXPLORING ADVANCED LINUX SECURITY AND MULTI-CLOUD BENCHMARKING SOLUTIONS

AN INTERVIEW WITH AUSTIN GADIENT
CTO & CO-FOUNDER, VALI CYBER

WHAT SHOULD A BOARD UNDERSTAND ABOUT AI

CYBERSECURITY IN THE SPACE DOMAIN: SAFEGUARDING OUR FUTURE

TAG DISTINGUISHED VENDOR

valicyber

The need to reduce cyber risk has never been greater, and Vali Cyber has demonstrated excellence in this regard. The TAG analysts have selected Vali Cyber, Inc. as a 2024 Distinguished Vendor, and such an award is based on merit. Enterprise teams using Vali Cyber's platform will experience world-class risk reduction—and nothing is more important in enterprise security today.

The Editors,
TAG Security Annual
www.tag-cyber.com

EXPLORING ADVANCED LINUX SECURITY AND MULTI-CLOUD BENCHMARKING SOLUTIONS
An interview with Austin Gadient
CTO & Co-founder, Vali Cyber
3

WHAT SHOULD A BOARD UNDERSTAND ABOUT AI
Dr. Edward Amoroso
7

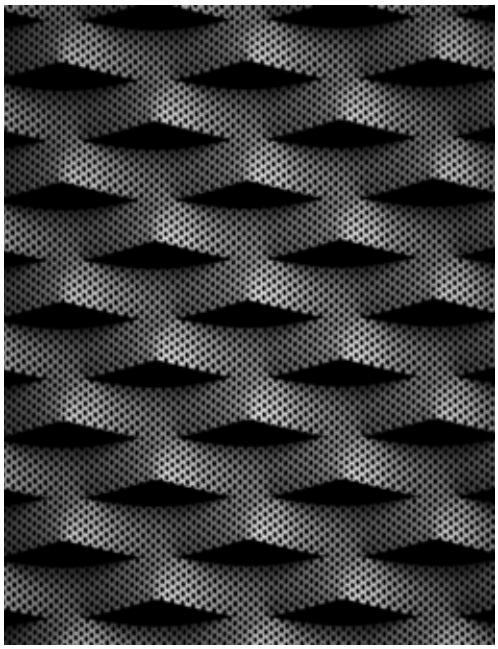
CYBERSECURITY IN THE SPACE DOMAIN: SAFEGUARDING OUR FUTURE
Davind Neuman
12

REPRINTED FROM THE TAG SECURITY ANNUAL

AN INTERVIEW WITH AUSTIN GADIENT
CTO & CO-FOUNDER, VALI CYBER

EXPLORING ADVANCED LINUX SECURITY AND MULTI-CLOUD BENCHMARKING SOLUTIONS

We recently interviewed Austin Gadient, Vali Cyber's CTO and Co-founder, to discuss how their ZeroLock™ platform secures Linux environments and detects malicious activities. We cover its unique features like behavioral analysis, lockdown rules, seamless integration, and GDPR and CCPA compliance efforts. Read on for insights into Vali Cyber's innovative solutions and commitment to enhancing cybersecurity and compliance.



TAG: How does Vali Cyber's ZeroLock™ platform secure Linux environments and detect/stop malicious activity?

VALI CYBER: The ZeroLock platform employs advanced techniques to ensure the security of Linux environments and effectively detects and halts various forms of malicious activity, such as ransomware, cryptojacking, attacks by malicious actors with stolen credentials, and exploits targeting known vulnerabilities.

ZeroLock utilizes behavioral analysis to identify suspicious activities and anomalies within Linux environments. Its agent autonomously monitors processes, system calls, network traffic, and file access patterns to detect malicious. It responds in real time, stopping the attack and restoring any affected system files.

Additionally, ZeroLock enhances Linux security with "lockdown rules," fine-grained controls for files, processes, and network access. These rules minimize the attack surface, harden Linux endpoints, and enable MFA for SSH, even in disconnected settings, establishing a zero-trust environment.

In the unfortunate event of an attack, ZeroLock provides file rollback, swiftly restoring all lost files and ensuring minimal downtime for critical systems. This can happen automatically or at a push of a button, and all without having to store our client's data.

Lastly, it's not just about what we can do but how we can do it. We focus on operationalization by ensuring ease of deployment and management, all while running on extremely low overhead and only 50MB of memory.

TAG: In the security space, the term "single pane of glass" is prevalent. Overburdened Cybersecurity teams want to simplify and streamline. What do you think about that approach?

VALI CYBER: I empathize with the perspective. However, there are greater risks in deploying a weaker solution on Linux systems. With the continued push to the cloud, we're seeing increased attacks on Linux. To protect its most critical data, a company must consider a best-of-breed approach combining the best solutions for each OS used—which is why integrations are so important.

Through its API, ZeroLock offers seamless integration with third-party systems, allowing easy connectivity with Security Information and Event Management (SIEM) systems, Security Orchestration, Automation, and Response (SOAR) platforms, data lakes, data warehouses, and centralized threat-hunting platforms. In fact, we're proud to announce a recent integration project with SwimLane. To see that in action, see our free webinar..

ZeroLock enhances Linux security with "lockdown rules," fine-grained controls for files, processes, and network access.

TAG: How portable is ZeroLock? What architectural frameworks are best suited?

VALI CYBER: Running on Linux distributions with kernel 3.5 or higher, ZeroLock is versatile and integrates seamlessly with various architectures, including public, private, and hybrid clouds, dedicated servers, virtual machines, containerized workloads like Kubernetes, and air-gapped environments. Its lightweight nature ensures easy deployment across diverse platforms, offering robust security regardless of the underlying system.

Managing ZeroLock is a streamlined process. Notably, the ZeroLock Agent requires no reboot for installation or updates, and a single instance can effortlessly scale to accommodate over 20,000 agents on a modestly sized server, as verified on an AWS t2-xlarge instance.

TAG: In the context of GDPR and CCPA, how does Vali Cyber ensure compliance while safeguarding sensitive data?

VALI CYBER: We strongly emphasize data privacy and regulatory compliance, specifically aligning with the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). Vali Cyber enforces rigorous access controls and user permissions through its ZeroLock™ platform, ensuring that only authorized personnel can access sensitive data. Role-based access control (RBAC) mechanisms enable organizations to customize access based on job roles and responsibilities. Plus, multi-factor authentication provides an extra layer of user verification.

Secondly, the ZeroLock Management Console platform incorporates comprehensive audit trail capabilities, meticulously logging all sensitive data access activities and processing. This transparency empowers organizations to demonstrate compliance by providing a clear audit trail of data handling. Vali Cyber collaborates with organizations to establish and implement data retention policies that adhere to regulatory requirements. Organizations can manage their data according to GDPR and CCPA guidelines by automatically deleting or archiving data per predefined rules.

Lastly, the ZeroLock Management Console is deployed on customer infrastructure within the specified geographic region to address data residency requirements. This strategic approach ensures compliance with the relevant data residency regulations, offering organizations additional assurance.

TAG: Are there any other features you'd like to highlight?

VALI CYBER: Sure. I'll focus on two. The first is that the ZeroLock Management Console provides multi-factor authentication and integration with centralized single-sign-on (SSO) authentication solutions. ZeroLock also uniquely enforces multi-factor authentication (MFA) over SSH as an additional layer of security to ensure secure access to Linux systems protected by ZeroLock.

Why is this important? 50% of all attacks on Linux use compromised credentials. Multiple authentication factors reduce unauthorized access risk and strengthen overall security, allowing administrators to define and enforce specific authentication policies. MFA capabilities are available both for SaaS and customer infrastructure deployments.

The second feature is extremely low overhead. Everyone strategizes about lowering cloud costs, but they should consider the unrecognized cloud cost of their security products. We developed ZeroLock with low overhead in mind, then built SecurityPerf, an open-source benchmarking tool to help us accurately measure overhead.

In our testing, ZeroLock runs at <5% overhead. What's shocking is hearing from security teams that their solutions can have overheads exceeding 50%, which essentially means every cloud server purchased only delivers half its potential productivity—significantly affecting the company's efficiency and bottom line.