Highlights

Software-Defined Flash Storage Architectures

Tuesday May 9 at 10:00 AM PST

G2M RESEARCH

Flash devices such as solid-state drives (SSDs) have increased in size to the point where an individual device can easily support multiple virtual machines.

The best way to take advantage of these capabilities is to utilize these latest SSDs as part of a software-defined storage architecture, where resources can be put together and taken apart as workloads demand.

Join our industry experts to explore best practices for SSD-based software defined architectures.

Tuesday, May 9 at 10am

Are You At #RSA2023?

The FBI Is…

Posted by Mike Heumann, April 24, 2023

RSA Conference is the world's leading cybersecurity conference. This is its 32nd year of bringing together the world's top cybersecurity, government and business leaders to learn, discuss emerging trends and formulate best strategies to help organizations and communities address current and future cyber threats. The FBI is the lead federal agency for investigating cyber attacks. They are participating in key informational sessions each day at #RSA2023. G2M is here as well, if you want to connect [mikeheumann.g2m@gmail.com]

The FBI works with our federal counterparts, foreign partners, and the private sector to defend networks, attribute malicious activity, sanction bad behavior, and take the fight to our adversaries overseas. The FBI fosters this team approach through unique hubs where government, industry, and academia form long-term trusted relationships to combine efforts against cyber threats. Within government, that hub is the National Cyber Investigative Joint Task Force (NCIJTF). The FBI leads this task force of more than 30 co-located agencies from the Intelligence Community and law enforcement. The FBI has specially trained cyber squads in 56 field offices. The rapid-response Cyber Action Team can deploy across the country within hours to respond to major incidents. The Internet Crime Complaint Center (IC3) collects reports of Internet crime from the public. Using these complaints, the IC3's Recovery Asset Team has assisted in freezing hundreds of thousands of dollars for victims of cyber crime. CyWatch is the FBI's 24/7 operations center and watch floor, providing around-the-clock support to track incidents and communicate with field offices across the country.

The Cyber Division priorities in rank order are:
(a) cyber intrusions;
(b) child sexual exploitation;
(c) intellectual property rights; and
(d) internet fraud.

One of the most notable examples of their recent success is disrupting Sodinokibi/REvil ransomware, which cyber actors used to compromise global meat processing company JBS and software company Kaseya in 2021. RSA provides a unique opportunity to gain insight into all the major players in the cybersecurity space, including many who act in partnership with the FBI.

#RSA2023 panel discussions featuring FBI Cyber:
Monday, April 24 - 9:40-10:30am- Hardening Your AI/ML Systems: The Next Frontier of Cybersecurity
Bryan Vorndran, FBI (moderator); Neil Serebryany; CalypsoAI; Christina Liaghati, MITRE; Bob Lawton, ODNI

Tuesday, April 25 - 1:15-2:05pm- It's Not All Fun And Games: Cyber Threats to Professional Sports
Joseph Szczerba, FBI (moderator); Steve Grossman, NBA; Tomás Maldonado, NFL; Dave Munroe, NHL

Tuesday, April 25 - 2:25-3:15pm- Stronger Together: US-Ukrainian Cyber Partnership
Bryan Vorndran, FBI (moderator); Laura Galante, ODNI; Alex Kobzanets, FBI; Illia Vitiuk, Security Service of Ukraine

Wed, April 26 - 9:30-10:30am- The National Cyber Strategy as a Roadmap for a Secure Cyber Future
Melinda Rogers, DOJ (moderator); Bryan Vorndran, FBI; Liesyl Franz, DOS CDP; Eric Goldstein, CISA; Robert Knake, ONCD

Thursday, April 27 - 8:30-9:20am- From Public-Private Partnerships to Operational Collaboration
Morgan Adamski, DOD (moderator); Cynthia Kaiser, FBI; Todd Conklin, USDT; Kyle Pfeiffer, DOE; Clayton Romans, CISA JCDC; Michael Toecker, DOE CESER

The Majority of Resale Core Routers Contain Confidential Information

Posted by Karen Heumann, April 24, 2023
ESET researchers found that, more often than not, core routers are not wiped clean before they are decommissioned and offered for resale. The findings were, frankly, astounding – 56.25% contained trivially accessible and sensitive corporate information and included the following:

22% contained customer data
33% exposed data allowing third-party connections to the network
44% had credentials for connecting to other networks as a trusted party

89% itemized connection details for specific applications
89% contained router-to-router authentication keys
100% contained one or more of IPsec or VPN credentials, or hashed root passwords
100% had sufficient data to reliably identify the former owner/operator

In addition, ESET researchers also found it very difficult to contact the corporations to provide them with these sensitive findings. In fact, at the time of publication of this ESET research, they were unable to reach three of the impacted companies.

Table 3. Overview of the companies identified from the nine easily accessed router configurations in this study[2]

Vertical	Reach	Employees	Revenue (US$, M)
Light manufacturing/supplier	Products/subassemblies integrated in larger companies' products	5–50	5–25
Legal	Nationwide (US) law firm	50–100	5–25
Creative	Services multiple tier one, household brand companies	100–500	25–100
Data center	Direct data services, as well as managed MSP services for region	100–500	25–100
MSP	Manages fintech companies	100–500	25–100
Open-source software	Has over 100 million users, worldwide	100–500	500–1,000
Events	Operates trade shows and equipment rentals	1,000–5,000	25–100
Multinational technology company	Global data company	10,000+	1,000+
Telecoms	This was CPE (Customer Premises Equipment) for a transportation company	10,000+	1,000+

ESET Specialized Security Researcher Cameron Camp and Chief Security Evangelist Tony Anscombe presented these findings at RSA in their presentation "We (Could Have) Cracked Open the Network for Under $100".

Anscombe also presented a Birds of a Feather session, "Is Legislation and Regulation a Friend or Foe of Cyber Defenders?" which examined the many cybersecurity regulations being proposed or levied, including the US Securities and Exchange Commission (SEC), Federal Deposit Insurance Corporation (FDIC), Executive Order on the Nation's Cybersecurity, and proposals by governments around the globe, and whether recent legislation and regulation is assisting or hampering cybersecurity teams.

Featuring RSA Innovation Finalists & Winner… HiddenLayer

Posted by Mike Heumann, April 24, 2023

This year's 10 finalists for the RSA Conference 2023 Innovation Sandbox competition: AnChain.AI; Astrix Security; Dazz; Endor Labs; HiddenLayer; Pangea; Relyance AI; SafeBase; Valence Security; and Zama. And, the winner is… HiddenLayer!

HiddenLayer helps enterprises safeguard the machine learning models behind their most important products with a comprehensive security platform. HiddenLayer offers turnkey AI/ML security that does not add unnecessary complexity to models and does not require access to raw data and algorithms. Founded in March of 2022 by experienced security and ML professionals, HiddenLayer is based in Austin, Texas, and is backed by cybersecurity investment specialist firm Ten Eleven Ventures.

The HiddenLayer ML Model Scanner delivers:

- Malware Analysis: Scans ML models for embedded malicious code that could serve as an infection vector and launchpad for malware.
- Vulnerability Assessment: Scans for known CVEs and zero-day vulnerabilities targeting ML models.
- Model Integrity: Analysis of ML model's layers, components, and tensors to detect tampering or corruption.
- Comprehensive Detection: Utilizes a combination of static detection, dynamic analysis, and machine learning techniques to identify malware, vulnerabilities, model integrity, and corruption issues.
- Catalog a Known-Good State: Baseline your ML models for identifying future tampering.

AnChain.AI (HQ in San Francisco) is an AI-powered cybersecurity company enhancing Web3 security, risk, and compliance strategies. AnChain.AI was founded in 2018 by cybersecurity and enterprise software veterans from FireEye and Mandiant and has 100+ customers from over 10+ countries in

these sectors: VASPs, financial institutions, and government, including the U.S. SEC (Securities and Exchange Commission). AI's AML engine screens over $1 billion in daily crypto transactions.

Astrix Security helps cloud-first companies defend against the clear and imminent threat of service supply chain attacks. By ensuring their core systems securely connect to third-party cloud services, they enable them to safely unleash the power of app-to-app integration and automation. Astrix instantly detects and mitigates integration threats with automated remediation workflows - all while continuously minimizing third-party exposure with zero-trust policies and automated enforcement guardrails.

Dazz delivers automated remediation for fast-moving security and development teams. Dazz plugs into the tools that find code flaws and infrastructure vulnerabilities, cut through the noise, prioritize the vulnerabilities that matter, and deliver a one-click fix to the code owner in a developer-friendly way. Dazz was founded in 2021 and is headquartered in Palo Alto, CA.

Endor Labs created the first open source dependency lifecycle management platform to help OSS consumers select, secure and maintain dependencies effectively. 80% of code in modern applications is code your developers didn't write, but "borrowed" from the internet. With over 3M Open Source Software (OSS) projects, 43M versions, and 3.1T downloads yearly, development teams can gain tremendous benefits from leveraging the OSS ecosystem, as long as organizations invest in the tooling to address the security, scalability and sustainability challenges that come with it. Endor Labs gives developers and security teams the context they need to prioritize open source risk.

Pangea is the first Security Platform as a Service (SPaaS) delivering comprehensive security functions which app developers can leverage with a simple call to Pangea's APIs. Like AWS for compute, storage, database, and many other microservices, Pangea provides out of the box microservices to embed security directly into Apps. Pangea was formed to unite security for developers, delivering a single location where API-first security services come together to make delivery of secure user experiences achievable and easy.

Believing that the global data protection and privacy environments have been far more complex than they should be, Relyance is reimagining what data protection means in a globalized, technology-driven world. Building the trust and governance infrastructure for the internet. Data protection and trust go beyond borders, beyond organizations, and beyond individual teams. Relyance is shifting the entire landscape of data protection technology through automation and machine learning.

The SafeBase Trust Center enables Security and Sales teams to proactively share and automate access to security, compliance, and privacy information. With SafeBase, organizations avoid redundant questionnaires, build customer trust, and close deals faster.

Valence Security offers collaborative remediation workflows that engage with business users to contextualize and reduce SaaS data sharing, supply chain, identity, and misconfiguration risks with scalable policy enforcement and automated workflows. With Valence, security teams can secure their critical SaaS applications like Microsoft 365, Google Workspace, Salesforce, and Slack and ensure continuous compliance with internal policies, industry standards and regulations, without impeding business productivity or the speed of SaaS adoption.

Zama develops open source cryptographic tools that make protecting privacy easy with homomorphic encryption regardless of where the application is running. Founded in 2019, Zama is a remote-friendly company with headquarters in the center of Paris.

G2M Research Multi-Vendor Webinar Series

Our webinar schedule is below. We are offering a Cybersecurity series and an Enterprise Storage & Technology multivendor series.

"The Need for Speed: NVMe™, NVMe-oF™, and Data Processing Accelerators" webinar featured Tony Afshary, Vice President, Products and Marketing at Pliops; Rob Davis, Vice President of Storage Technology at NVIDIA; and Peter Onufryk, Intel fellow for NVMexpress. Companies are focused on storage/networking/processing acceleration. Higher-level networking protocols and custom protocols for specific workloads require "offloads" to lower CPU utilization and increase application performance. Advanced storage capabilities such as those offered by NVMe and NVMe-oF can also tax CPUs, reducing cycles available for workloads. And then there is security, data resilience, and other very real needs that take CPU cycles away from workloads. This webinar explored where non-hyperscalers go to accelerate their workload in the same way hyperscalers do. The webinar video is available to view and a copy of the slidedeck is available here.

Interested in Sponsoring a webinar? Contact **G2M** for a prospectus. We can create custom webinar, custom webinar series, and add or modify topics to specifically appeal to your target audience. View our webinars and access slide deck presentations on our website.

Enterprise Storage & Technology

Software-Defined Flash Memory Architectures	May 9
Custom Webinar featuring Pliops, more info soon!	June
NVMe & NVMe-oF – Past, Present, & Future	July 11
GPUs, SSDs, & Shared Memory: Accelerating Computing?	August 22

Securing Data – How Storage & Cybersecurity Technologies Can Work Together	Sept 26
The Open Compute Platform (OCP) Movement – Providing Compute-At-Scale Value to On-Premises Deployments	October 24
Storage Architectures for HPC Clusters	November 21
2024 Trends – Cloud, On-Premises, & Hybrid Compute/Storage	December 12

Cybersecurity

The Increasing Complexity of Cybersecurity Regulatory & Compliance for the Financial Services Industry	May 25
xDR- The Promise versus the Reality	August 3
10 Features of an Effective Attack Surface Management Tool	September 7
How Secure is the Cloud for Your Workloads?	October 12
Do You Need a SIEM? Use Cases Where a SIEM Makes Sense.	November 9

Upcoming Conferences

April 24-27	RSA Conference, San Francisco
May 1-3	IAHSS AC&E, Nashville, TN
May 2-4	ACT Expo, Anaheim, CA
May 9-12	Black Hat Asia 2023, Singapore
May 15-17	Forth Roadmap Conference, Portland, OR
May 16-17	SIA GovSummit, Washington DC
May 17-18	Expo Summit Global, Santa Clara, CA
May 21-25	ISC, Frankfurt, Germany
May 22-25	Dell World, Las Vegas
May 22-25	Government Fleet Expo, Dallas, TX
June 2-6	School Transportation Network Expo East, Indianapolis, IN
June 4-8	Cisco Live, Las Vegas
June 5-7	Gartner Security & Risk Managemnt, National Harbor, MD
June 7-9	Synnex Red, White and You, Greenville, SC
June 11-14	36th Electric Vehicle Symposium & Expo, Sacramento, CA
June 11-16	2023 VLSI Symposium, Kyoto, Japan
June 14-16	Interop Tokyo, Chiba, Japan
June 20-22	HPE Discover, Las Vegas
June 20-22	Info Security Europe, London

July 14-19	School Transportation Network Expo, Reno, NV
August 5-10	Black Hat USA, Las Vegas
August 8-10	Flash Memory Summit, Santa Clara, CA
August 28-31	VMWare Explore, San Francisco, CA
August 30-Sept 1	Security Expo, Sydney, Australia
September 11-13	Gartner Security & Risk Management, London
September 11-13	Global Security Exchange, Dallas, TX
September 18-20	Crowdstrike fal.con, Las Vegas
September 18-21	SDC 2023, Fremont, CA
October 2-4	DattoCon, Miami, FL
October 3-4	CyberTech Europe, Rome
October 16-19	Gartner IT Symposium/Xpo, Orlando, FL
November 15-16	Microsoft Ignite, TBD
Nov 27- Dec 1	AWS re:Invent, Las Vegas