CYBER DEFENSE MAGAZINE

eMAGAZINE

OCTOBER 2023

In This Edition

Cybersecurity Is Changing: Is the Experience Positive or Negative?

Navigating The Cybersecurity Horizon: Insights and Takeaways from Blackhat2023

Understanding The Impact of The SEC's Cybersecurity Disclosure Regulations

...and much more...

MORE INSIDE!

Securing The Virtual Runway to The Cloud

By Jason Mafera, Field CTO, North America, IGEL

The 'endpoint' has transformed from traditional desktop hardware to any number of devices, digital workspaces, and locations, offering new opportunities for cybercriminals who often seem one step ahead of data protection and defense technologies. Cybercriminals are finding the increase in workloads moving to the cloud a rich source of exploitation. This is complicated by the distributed nature of today's workloads and combinations of delivery technologies. Some workloads have moved to the cloud, some are still on premises, and all are available for access from anywhere on any device. The Thales 2023 Data Threat Report notes that respondents identify SaaS apps, cloud-based storage and cloud-hosted apps as key targets. It is a major concern as more companies are now storing sensitive data in the cloud. Thales reports 75% of respondents say almost half of their cloud data is classified sensitive.

While malware, ransomware and phishing continue to be primary threats, confidence in how to fight these threats has shifted, Thales reports. Endpoint security is now considered the number one control for effectiveness in protecting sensitive data, followed by IAM (Identity and Access Management) and network security.

The endpoint and IAM are key to addressing security concerns in light of the continuing hybrid environment: hybrid workers and hybrid cloud usage. More surfaces to attack and a diversity of devices, locations, and level of security awareness on the part of remote workers all add up to more risk of a data breach, reputational damage to the organization and costly downtime.

Data Security Begins with a more Secure Operating system on the Endpoint

Protecting this mixed universe of devices, remote work, and hybrid cloud deployments starts at the interface between the user and the access device, specifically the endpoint. Enterprises are finding that purpose built, security focused Linux based operating systems to be the endpoint OS of choice. It's designed with a lightweight, small modular footprint, is read only, and contains no persistent user profile. Its firmware files can be encrypted and partitioned to ensure the OS cannot be tampered with or modified by malicious applications or extensions. This is accomplished via a full chain of trust from the hardware to OS, all the way to the application layer, making it tamper-proof and inaccessible by ransomware. It also allows for unmounted encrypted backup partitions that aid in rapid recovery in the event of an unauthorized change to the OS.

Since the OS operates independently of applications or services, it further reduces the attack surface by delivering only what is required for the usage model and removing anything unnecessary. A secure Linux OS supports local applications, hybrid cloud environments and virtualization platforms, including AVD, AWS, Citrix, VMware, and cloud workspaces as well as SaaS and DaaS services. It also offers IT efficiency by enabling over-the-air updates and patching, saving valuable IT staff time, and ensuring patches are deployed consistently across the enterprise. In this model, if a device has internet access, it is part of the enterprise and fully managed and controlled.

A secure Linux-based edge OS provides flexibility and security attributes that are driving global growth from an estimated $6.27 billion in 2022 to $22.15 billion by 2029, a CAGR of 19.8%, according to Fortune Business Insights.

Mitigating Risk and Disruption via Cloud Workloads

Minimizing attack surfaces, in addition to a secure Linux OS, requires moving applications and data off endpoint devices and storing them in the cloud. Every data file does not need to reside in the cloud, but any sensitive data related to critical business operations, and to employees being as productive as possible, should live in the cloud.

Should an attack occur, employees will be able to continue work by accessing their files from the cloud, further ensuring business continuity.

Access Controls Essential to Threat Defense

Gartner describes IAM as "a security and business discipline that includes multiple technologies and business processes to help the right people or machines to access the right assets at the right time for the right reasons, while keeping unauthorized access and fraud at bay." That means it's critical to have processes in place to manage your users' identities, strongly authenticate those users for access, and enforce the principle of least privilege to resources across the delivery landscape. Using a secure Linux OS, separating critical data and applications from a device, and storing sensitive data in the cloud are essential to threat defense. Centralization provides better access to threat defense and response tools and allows for protection at scale. In concert, enterprises need to execute IAM access controls that provide real-time monitoring and anomaly detection to prevent unauthorized users gaining control over data or applications.

At the endpoint, the gating factor for secure access is validating the user identity. Regardless of device or location an employee must be able to easily and securely obtain the applications they need.. Their access depends on their roles and responsibilities and must be updated should they change roles or leave the company. In this hybrid model, it is also critical to implement modern multi-factor authentication (MFA) and single sign-on technology integrations that enhance security, mitigate the majority of phishing attacks, and enable ease of use for the end user while enhancing the overall security posture.

Reducing Risk is a One-on-One Mandate

From the endpoint perspective, a secure OS, moving applications to the cloud, and stringent access controls combined with adaptive MFA are the strongest defense against ransomware and malware. Even with all of the proper controls in place, people remain the weakest link against the best cybersecurity structure. Thales respondents still cite the #1 root cause of a cloud data breach as human error.

Workforce training and security awareness programs are critical to reducing human error. The Center for Internet Security's critical security controls include one on security awareness and skills training. "It is easier for an attacker to entice a user to click a link or open an email attachment to install malware in order to get into an enterprise, than to find a network exploit to do it directly," CIS says. Beyond phishing, enterprises need to train employees in password hygiene, remove the use of passwords where possible, and reiterate the risks of sharing sensitive data outside the network, with those who do not have privileged access.

More Security Work Ahead

Enterprises are making strides in security practices like removing passwords, enforcing MFA, and implementing full stack IAM solutions but the work is not over as cybercriminals in 2023 are becoming more active and successfully conducting attacks. They include LockBit, AlphaVM (BlackCat), and Black Basta, according to a Black Kite Ransomware Threat Report.

The report notes “common ransomware indicators among victims included poor email configuration, recent credential leaks, public remote access ports, out-of-date systems, and IP addresses with botnet activity.”

Despite this resurgence, only 49% of respondents from the Thales report have a formal ransomware response.

As cybercriminals create new methods of attack like file-less malware and encryption-less ransomware, enterprises need to reassess their security posture-beginning at the endpoint – and ensure that a best-defense, secure OS, separating data from devices and storing it in the cloud, and stringent access controls are in place. And the remaining 51% who do not have a ransomware response plan need to be thinking how to execute recovery when attacks occur, which has become especially challenging with today’s hybrid & distributed workforce.

About the Author

Jason Mafera is Field CTO, North America for IGEL. He comes to IGEL with more than 20 years of experience in the delivery of cybersecurity-focused enterprise and SaaS solution offerings and has worked for a broad range of companies from start-ups and pre-IPO organizations to public and privately backed firms. Prior to joining IGEL in October 2022, Mafera served as Head of Product and then Vice President of Sales Engineering and Customer Success for Tausight, an early-stage startup and provider of healthcare software focused on delivering real-time intelligence for securing and reducing compromise of electronic Personal Health Information (ePHI) at the edge. Before that, he held a succession of leadership roles with digital identity provider Imprivata. Mafera spent 12 years at Imprivata, first defining and driving to market the OneSign Authentication Management and VDA solutions, then leading the Office of the CTO. Early on in his career, he was systems engineer and later product manager at RSA, The Security Division of EMC.

Jason can be reached online at LinkedIn and at our company website www.igel.com