HFS

HOT VENDORS

HFS OneEcosystem™ Hot Vendor: Eclypses

Author:

Joel Martin, Executive Research Leader

Hot Vendor Program Lead:

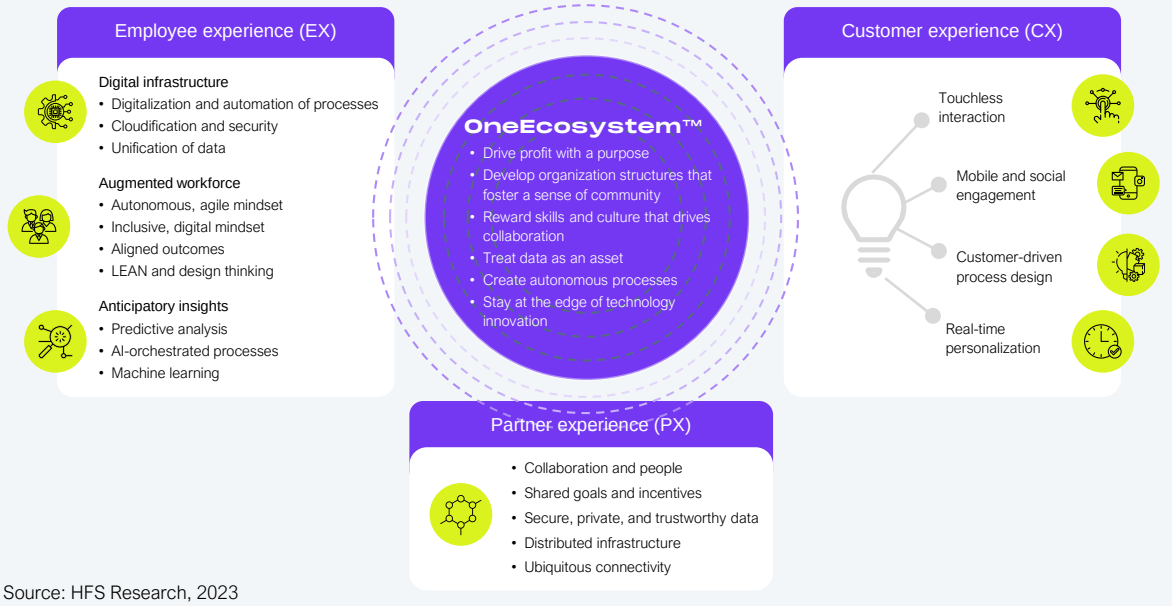
David Cushman, Executive Research Leader, Hot Vendors Editor-in-Chief

Excerpt for Eclypses

Executive summary

HFS Hot Vendors are an exclusive group of emerging players, each with a differentiated value proposition for the HFS OneOffice™ or HFS OneEcosystem™. We selected this Hot Vendor for its alignment with the HFS OneEcosystem in Exhibit 1.

Exhibit 1: The HFS OneEcosystem adds partner experience to employee and customer experience



Source: HFS Research, 2023

HFS analysts regularly speak with numerous exciting start-ups and emerging players. We designate a select few as HFS Hot Vendors based on their offerings' distinctiveness, ecosystem robustness, client impact, financial position, and, in this case, impact in our OneEcosystem framework. HFS Hot Vendors may not have the scale and size required to feature them in our Horizons reports, but they have the vision and strategy to impact and disrupt the market.

In the rapidly changing space of digital operations, enterprises realize they cannot be everything to everyone. Enterprises consuming third-party services, service providers, and technology providers need a smart ecosystem to succeed and survive in the future. HFS Hot Vendors are service and technology providers hand-picked by our analysts to help you flesh out your smart ecosystem with offerings that solve today's complex business problems and exploit market opportunities.

HFS Hot Vendors display truly differentiated offerings and out-of-the-box thinking that can be inspiring and useful. This report profiles one HFS Hot Vendor selected through our rigorous five-step assessment. The HFS Hot Vendor designation remains in place for one calendar year.

Every Hot Vendor joining our program remains listed on our exclusive and searchable database.

Eclypses: A revolution in cryptographic solutions for safeguarding data and information in transit, on–premises, or in the cloud

Eclypses is an emerging cybersecurity solution provider focused on delivering a cloud-native cybersecurity solution built on its Eclypses Cryptographic Library (ECL) called MicroToken Exchange . MTE™ is a patented technology for automatically obscuring data payloads at the application level. Rather than complex, multi-tier combinations of security hardware, software, and certifications, their solution is based on a container model that makes it easy for a company to “drop and forget” its capabilities into any application communicated with endpoints, user devices, or system-to-system back-office applications. Its MTE technology converts a data payload into a random string of values. These values replace any form of structured or unstructured data and are not decipherable if intercepted or accessed by an unauthorized agent. MTE provides innovative security against man-in-the-middle cyberattacks with minimal effort needed to deploy, manage, or support.

A renaissance in security and cryptography is needed to protect data and trust

Today’s firms must prioritize securing data from hackers and other bad actors who constantly seek to infiltrate and compromise data on systems, intellectual property, customer information, and financial records. Having data exposed or allowing a malicious party to access systems or data harms a firm's brand, trust, and financials. However, the complexity of today’s systems, applications, and architectures has created a large attack surface that most firms struggle to manage.

Security applications are a mix of policy, software application-based patch management, and cryptography solutions, including SSL/TLS certificates, encryption algorithms (AES, DES, RSA, etc.), SIEM, endpoint solutions, and more. Firms continue to increase their attack vectors to manage data security by maintaining fluency and currency of up-to-date policy, patches, and cryptographic solutions. This complexity is costly regarding the technology, support, and resources needed to maintain compliance and a state of readiness.

As we see daily, a growing, sophisticated network of private and state-backed hackers continues to overcome these solutions and gain access to crucial data that can negatively impact a target company, its customers, and its employees. As technology continues to evolve, the workforce and customer dynamics become more diverse, and the need for globally integrated supply chains requires dependencies on a wide variety of partnerships. The result is a growing acceptance that companies face accepting a certain level of loss.

This complacency cannot be tolerated . Eclypses offers firms a revolutionary security solution for securing data in transit between IoT, mobile, API (application programming interfaces), or cloud data repositories or applications. Its solution isn’t based on adding layers to the existing security fabric. Instead, it focuses on protecting data in a zero-trust, zero-touch, and automated manner.

Eclypses solutions render data unintelligible to any user or system other than its targeted, verified, and validated endpoints

Eclypses solutions are unlike many security solutions already deployed by enterprises. While traditional security solutions are based on technology teams or IT services partners bolting on protection at later stages (such as TLS or SSL), Eclypses encrypts data directly at the application layer. This approach provides the highest level of security as it ensures each data packet is encrypted before it can be intercepted or compromised.

The Eclypses solution consists of its patented and FIPs 140-3 Level 1 validated Eclypses Cryptographic Library (ECL), MicroToken Exchange (MTE), Managed Key Encryption (MKE), and Secure Data Replacement (SDR) solutions. Eclypses designs, manages, and maintains these solutions, which are then made available via cloud-native deployment models that can be integrated via microservices into nearly any application or data architecture.

Eclypses focuses on simplicity, resiliency, and low latency

Rather than investing in building a new public key infrastructure (PKIs), Hash algorithms, or hardware security module that would require additional training, resources, and support costs, Eclypses has developed its solutions to be native to cloud and data transmission. Focusing on data has prioritized what is most valuable for a company to protect. Eclypses created a new technology for data in transmission to achieve this and ensure it was easy to adopt.

Eclypses MTE is a security solution built for cloud-native applications (web, mobile, and API), Internet of Things (IoT) deployment, and enterprise applications. MTE secures data at the application level by:

- Focusing on the data, not changing or modifying the user experience or how people work, transact, and collaborate as part of normal workflows;
- Encrypting autonomously at the data layer, removing weak points at the user, operating system, or communications layers; and
- Rendering data obsolete until validated through its patented cryptographic solution at each endpoint, preventing a man-in-the-middle attack of injecting, intercepting, relaying, or decrypting data.

Eclypses MTE protects against man-in-the-middle attacks, including payload injection, replay and delay, data inspection, spoofing and eavesdropping, and operating system attacks, including heightened privilege and memory reading.

To enable customers to deploy MTE quickly, Eclypses provides support and toolkits for multiple language interfaces, including Java, C#, Swift, JavaScript/WASM, Python, C++, C, Objective C, and Go, software development kits (SDKs), and uses a container-based solution via AWS Marketplace.

Eclypses focused on the application and data layer to reduce complexity

As companies continue to evolve their infrastructure to move computing, data management, network management, and applications to public and hybrid cloud architectures, they have increased the attack surface for bad actors. As a result, multiple vendors, systems, applications, data repositories, endpoints, identity and access management tools, and policies must be kept current. To do so currently requires a firm's technology teams to invest significantly in people, testing, implementation, and compliance reporting, such as SOC-2.

HFS views securing each part of the application, operating system, network, and data fabric creates significant technology and process debt, leaving too many possible vulnerabilities to data leakage, malicious hacking, cybercrime, phishing, and ransomware. Further, the data must be protected as companies adopt microservices, containers, and web APIs to exchange information across systems, endpoints, and users.

While data protection has typically been achieved with Hash functions to map data of arbitrary size to fixed-size values to hide its payload, the rise in computing power, exposed security keys, and leaked credentials has reduced this standard's effectiveness. While new Hash functionality is being created, its complexity creates latency and reduces computing efficiencies valued in many industries.

The Eclypses solution can be integrated on top of existing security solutions or natively within applications. For complex IT shops with a committed security policy and investments, implementing MTE can support data integrity and protection across global offices, legacy systems, or remote endpoint devices. Small and medium-sized enterprises lacking the budget or resources may find MTE a solution that absolves them of the high cost of protecting their data while remaining compliant with industry or partner policies and requirements.

Growing partnerships with companies such as AWS enable Eclypses to streamline and strengthen data protection for enterprises

Its breakthrough came in 2023 when MTE was accepted into the AWS Marketplace. Through AWS, it can now reach millions of global customers seeking to protect their web and mobile application data, user/system credentials, and critical business and customer data.

Clients using AWS can access the Eclypses MTE Relay as a container application and deploy with minimal client-side code, no server-side code, and without adding headcount or new security certifications. For more complex applications, it offers MTE API relay, a server-to-server solution for encrypting back-office and automated system-to-system data transmission. The Eclypses Cryptographic Library powers both solutions and can support current computing. They have also been tested to comply with emerging quantum computing cryptography standards.

Additionally, as firms will continue to require their partners and customers to meet increasingly rigorous data security and privacy requirements to remain compliant with policies, Eclypses must develop its go-to-market channels beyond its strength with Amazon's AWS and the AWS Marketplace. While AWS's buy-in to this solution will make Eclypses MTE solutions available to millions of potential customers via its AWS Marketplace, it will need to replicate this with Google's Cloud and Microsoft's Azure markets.

To further accelerate growth, Eclypses should seek out partnerships with integration, software engineering, and managed services firms, which can make its solutions a steady-state deliverable across their clients. Beyond Azure and AWS, HFS believes the firm must continue to develop partners in the managed services space and create a licensing model that encourages the ease of deployment at scale.

In addition to working with AWS, Eclypses is targeting relationships with other ISV partners in the cloud and cybersecurity industries.

Customer impact and adoption is creating a new mindset toward how we protect our most important asset, our data

HFS spoke to Eclypses customers, who praised the firm's solution as critical to their ability to bring solutions to market. Doris Schwartz, CEO and founder of WILLPORTtrust, a financial services application with backing from investment and banking firms, cited MTE as "not just an improvement over traditional methods but a transformative leap forward."

For firms dealing with financial and customer information, the Eclypses solution has been certified to meet the criteria of FIPS 140-3. This certification complies with regulatory requirements and industry standards, reducing the risk of non-compliance penalties while enhancing a firm's data and application security capabilities.

The business results shared with HFS by Eclypses customers include:

1. A reduced attack surface: By encrypting data at the application layer, the attack surface is reduced, making it harder for attackers to exploit vulnerabilities.
2. Cost savings: By preventing data breaches and reducing the need for incident response and remediation, Eclypses helps save on potential costs associated with security incidents, bespoke security software and hardware costs, and specialized talent to build, manage, and maintain systems.
3. Improved operational efficiency: With MTE in place, the client can focus on its core business activities without the constant concern of potential data breaches, improving overall operational efficiency.
4. Ensure market credibility: One client cited enhancing its market credibility as a reason for leveraging Eclypses' MTE, which attracts potential clients who prioritize data security.
5. Creating competitive advantage: Eclypses offers state-of-the-art data security and allows us to position our business as a leader in security consciousness and innovation.

Client improvement recommendations for Eclypses include providing more detailed and accessible tutorials, guides, and documentation to help users maximize the software's benefits.

HFS' take

We chose Eclypses as an HFS OneEcosystem™ Hot Tech because it brings a revolutionary new way for encryption that can be applied effectively and robustly without complex licensing, resourcing, or integration efforts by its clients. Eclypses is unique in the market because it designed its MTE solution for how companies operate now, in a dynamic, cloud-native operating mode, by addressing how to make security robust and resilient without encumbering systems or processes with complex overhead or taxing compute power.

With application, infrastructure, and data technologies all evolving, it is essential that security does as well. Eclypses delivers an innovative and unique approach to data security without the implementation burden of complex, heritage crypto solutions. The ability for companies of all sizes to adopt MTE and other Eclypses solutions makes it easier for larger organizations to improve their security policies while ensuring their suppliers have access to tools to remain compliant and preferred.

As the industry prepares for potential compromise scenarios from post-quantum crypto exploits, increasing data security from Eclypses is a future-proofing option to enhance and embed a pervasive data security model across the business.

After multiple demos and customer and partner validation, HFS believes Eclypses has a game-changing solution for the cybersecurity and cryptography marketplace. While it lacks the brand awareness of Palo Alto Networks, Cisco, OKTA, CrowdStrike, and others, it offers an innovative solution that can effectively be deployed across a large segment of a company's application and data landscape.

Vendor fact sheet

- **Founded**: 2017
- **Headquarters**: Boston, USA
- **Key executives**: David Gomes (CEO), Larry Murray (CRO),Jeff Dance (CIO), Tim Reynolds (CDO), Dan Lemoine (Senior Director of Operations), Taylor Brooks (AWS Cloud Alliance Director)
- **Number of employees**: <50
- **Funding source**: Private high-net-worth individual investors, amount not disclosed.
- **Number of clients**: Approximately 50
- **Key clients**: WILLPORTtrust, Voatz, Archethought, WholesalePayroll, global social platform provider, large banking and financial services firm
- **Domain**: Security Software, Cybersecurity, Cloud-Native Applications
- **Solutions portfolio**: Eclypses Cryptographic Library (ECL), MicroToken Exchange (MTE), Managed Key Encryption (MKE), Secure Data Replacement (SDR), Eclypses MTE Relay Server, Eclypses API Relay
- **Industry Application**: Available across all industries

The HFS Hot Vendor report team

Author

Joel Martin
Executive Research Leader

Joel leads HFS's global software services practice. In his role, he looks at emerging trends, cost metrics, and technologies that can impact an organization's application, software development, and security strategies. Joel has worked for global software, semiconductor, and advisory firms. He regularly advises business and technology teams on the need for a 'future of software' business strategy to rethink their approach to legacy, SaaS, and cloud technologies.

Hot Vendor Program Lead

David Cushman
Hot Vendors Editor-in-Chief
Executive Research Leader

David is an executive research leader for HFS and is editor-in-chief of the HFS Hot Vendors program. He also leads our OneOffice™ Emerging Technology Practice, is our strategic lead on generative AI, Web3, and metaverse, and covers automation and employee experience. He is a published author (*The 10 Principles of Open Business*, Palgrave Macmillan), a former Tier 1 consulting director, and a digital strategy and innovation expert with leadership experience in start-up, scale-up, and enterprise digital transformation.

HFS

About HFS

- **INNOVATIVE**
- **INTREPID**
- **BOLD**

HFS is a leading global research and analysis firm trusted at the highest levels of executive leadership. Our mission is to help our clients—major enterprises, tech firms, and service providers—tackle challenges, make bold moves, and bring big ideas to life by arming them with accurate, visionary, and thought-provoking insight into issues that impact their business.

Our analysts and strategists have deep, real-world experience in the subjects they cover. They're respected for their independent, no-nonsense perspectives based on thorough research, demand-side data, and personal engagements with industry leaders.

We have one goal above all others: to propel you to success.

www.hfsresearch.com

hfsresearch

www.horsesforsources.com