

CYBERARK®

THE IDENTITY SECURITY COMPANY®

2025 TECHNOLOGY INNOVATION LEADER

Enhancing Customer Impact Through Powerful Technology Integration

RECOGNIZED FOR BEST PRACTICES IN THE GLOBAL MACHINE IDENTITY SECURITY INDUSTRY

FROST & SULLIVAN

Best Practices Criteria for World-Class Performance

Frost & Sullivan applies a rigorous analytical process to evaluate multiple nominees for each Award category before determining the final Award recipient. The process involves a detailed evaluation of best practices criteria across two dimensions for each nominated company. CyberArk excels in many of the criteria in the machine identity management space.



Security, Reliability and Scalability in Digital Operations

Machine identity security is an essential cybersecurity practice, ensuring the integrity and security of machine identities, as well as the communication between them. In addition to the physical hardware devices such as computers, mobile devices, servers, or switches, 'machine' in this context also refers to workloads including containers, APIs, Virtual Machines (VMs), applications, services, scripts, or code. Similar to how human users are authenticated to secure networks using various methods, unique identities for machines enable integrity and secure communications through the use of cryptographic keys and digital certificates.

With increasing adoption of cloud services, Internet of Things (IoT) devices, and microservices architectures, the number of machine identities within organizations has skyrocketed in recent years, bringing complexity to the enterprise security landscape. In the case of modern, fast-growth, cloud-native and global organizations, the number of machine identities substantially outnumbers that of human identities. With distributed workforces accessing and interacting with cloud resources and applications across multiple devices and cloud environments, constant business-critical data flowing through connected devices, and increasing integration of DevOps practices and toolsets, effective management and security of machine identities is crucial for all organizations.

Lack of proper management of ever-increasing machine identities brings the risk of unauthorized access,

leading to potential data breaches, fraud and service disruptions, as well as vulnerability from persistent and emerging threats. Beyond the risks to an organization's security posture, without robust machine identity security, organizations typically experience financial risks with decreased employee productivity and business continuity, customer dissatisfaction, loss of investor confidence, and SLA breaches. Machine identity security also supports compliance with regulatory standards such as NIST, GDPR and PCI DSS guidelines, maintaining accountability and transparency in organizations' security practices.

The first step of the management process involves discovering and maintaining a record of the machine identities across the network and use cases – as well as regularly updating it – with only access to privileged, administrative users. The practice then involves regular issuance, renewal and revocation of cryptographic keys and digital certificates, based on the business criticality and the nature of the machine identity, as well as monitoring and reporting of all activity. Especially with projects or use cases with a limited time frame, and identities shared with third-party vendors, the ephemerality of machine identities is critical. Due to the volume and velocity of such operations, reliability and scalability in machine identity security can only be achieved through automation.

Consolidated Machine Identity Security Through Control Plane

CyberArk's acquisition of Venafi marked a significant move in the area of machine identity security. Venafi, a pioneer and the category creator in the machine identity management space, has long been a key player with a specific focus on securing machine identities for the Global 5000 companies and government bodies across North America, Europe, and Asia Pacific. Catering to organizations in all stages of their identity lifecycle journey, the company's offerings help customers solve machine identity management challenges ranging from legacy applications to fully cloud-native environments. By integrating Venafi technology, solutions, and expertise into its broader human and machine identity security portfolio, including secrets management, CyberArk has greatly expanded its capabilities to include a complete and end-to-end machine identity management security suite.

> *"Machine identity lifecycle management is delivered through the CyberArk Control Plane, which consolidates customers' cloud environments, on-prem datacenters, public CAs, PKI products, as well as vaults and DevOps tools, into one centralized platform. While existing Venafi customers typically have a large on-prem presence, CyberArk's SaaS product segments experience the highest growth."*
>
> ***- Özgün Pelit***
> ***Sr. Industry Analyst***

As part of the consolidated solution, machine identity lifecycle management is delivered through the CyberArk Control Plane, which brings together customers' cloud environments, on-prem datacenters, public CAs, PKI products, as well as vaults and DevOps tools, into one centralized platform. While historically Venafi customers typically had a large on-prem presence, the CyberArk's SaaS product segments experience the highest growth, with the vendor assisting organizations in their migration journeys.

CyberArk's machine identity security management strategy primarily centers around the software workload space, with lesser emphasis on machine identities for physical devices. In addition to machine identity discovery through the Control Plane provides an integrated experience across machine identities. This includes certificate lifecycle management (TLS Protect), PKI-as-a-Service (Zero Touch PKI), code

signing (CodeSign Protect), and SSH management (SSH Protect). In addition, Venafi provides the industry's first workload identity issuer (Firefly) with REST, GraphQL, and gRPC interfaces to issue SPIFFE and TLS certificates and JWTs, as well as cloud-native identity security (TLS Protect for Kubernetes).

An Innovation Ecosystem Driving Success

Building on Venafi's pioneering position in the market, CyberArk boasts an unparalleled ecosystem of 1000+ integrations, with a significant portion exclusively available to CyberArk customers. The vendor has the closest integrations in secrets management across industry leaders in addition to CyberArk's own secrets management. Part of CyberArk's innovation strategy is to build a partner ecosystem of developers, fueling collaboration. Leaders that are part of the CyberArk-Venafi ecosystem include AWS, F5, Red Hat, Citrix, IBM, BMC, Palo Alto Networks and Check Point.

> *"Venafi boasted 600+ customers worldwide, over 100% year-on-year growth for its SaaS segment, and a 98% customer retention rate. CyberArk demonstrates great success in rolling out new technologies and driving adoption across its customer base are expected to exponentially increase machine identity management success."*
>
> ***- Özgün Pelit***
> ***Sr. Industry Analyst***

Venafi introduced its first opensource polyglot software development kit – Vcert – in 2016, and in 2021 was one of the first providers to offer its customers post-quantum algorithms and hybrid certificates in partnership with ISARA and Crypto4A. Further innovations by the vendor in the machine identity management include donation of opensource cert-manager for Kubernetes certificate management to Cloud Native Computing Foundation (CNCF) with 1.5 million downloads per day. Venafi also sponsored over 50 start-ups and opensource developers with the Machine Identity Management Development Fund having invested up to $12.5 million.

Prior to the CyberArk acquisition, Venafi boasted 600+ customers worldwide, over 100% year-on-year growth for its SaaS segment, and a 98% customer retention rate. Closely integrating Venafi with its 9,000 existing customers and hundreds of channel partners worldwide, CyberArk's success in rolling out new technologies and driving adoption in machine identity management are expected to exponentially increase.

Conclusion

The exponential growth in machine identities and the increasing frequency of attackers exploiting machine identities presents a growing challenge for organizations. While increasing interdependencies in organizations' digital architectures mean increased productivity and growth, failure with regards to proper identity security management comes with a greater risk of business disruptions and security breaches.

As a pioneering player, CyberArk partners with organizations at every stage of their machine identity security lifecycle journey. Marking key milestones in the industry with its innovation strategy, the vendor prepares customers for the future with its focus on trends and wide partner ecosystem.

With its strong overall performance, CyberArk earns the 2025 Frost & Sullivan Global Technology Innovation Leadership Award in the machine identity security industry.

What You Need to Know about the Technology Innovation Leadership Recognition

Frost & Sullivan's Technology Innovation Leadership Award recognizes the company that has introduced the best underlying technology for achieving remarkable product and customer success while driving future business value.

Best Practices Award Analysis

For the Technology Innovation Leadership Award, Frost & Sullivan analysts independently evaluated the criteria listed below.

Technology Leverage

Commitment to Innovation: Continuous emerging technology adoption and creation enables new product development and enhances product performance

Commitment to Creativity: Company leverages technology advancements to push the limits of form and function in the pursuit of white space innovation

Stage Gate Efficiency: Technology adoption enhances the stage gate process for launching new products and solutions

Commercialization Success: Company displays a proven track record of taking new technologies to market with a high success rate

Application Diversity: Company develops and/or integrates technology that serves multiple applications and multiple environments

Business Impact

Financial Performance: Strong overall financial performance is achieved in terms of revenues, revenue growth, operating margin, and other key financial metrics

Customer Acquisition: Customer-facing processes support efficient and consistent new customer acquisition while enhancing customer retention

Operational Efficiency: Company staff performs assigned tasks productively, quickly, and to a high-quality standard

Growth Potential: Growth is fostered by a strong customer focus that strengthens the brand and reinforces customer loyalty

Human Capital: Commitment to quality and to customers characterize the company culture, which in turn enhances employee morale and retention

© Frost & Sullivan 2025

About Frost & Sullivan

Frost & Sullivan is the Growth Pipeline Company™. We power our clients to a future shaped by growth. Our Growth Pipeline as a Service™ provides the CEO and the CEO's growth team with a continuous and rigorous platform of growth opportunities, ensuring long-term success. To achieve positive outcomes, our team leverages over 60 years of experience, coaching organizations of all types and sizes across 6 continents with our proven best practices. To power your Growth Pipeline future, visit Frost & Sullivan at http://www.frost.com.

The Growth Pipeline Engine™

Frost & Sullivan's proprietary model to systematically create ongoing growth opportunities and strategies for our clients is fuelled by the Innovation Generator™.
Learn more.

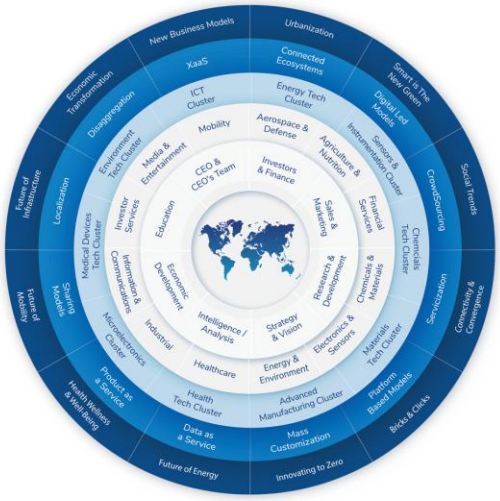


Key Impacts:

- **Growth Pipeline:** *Continuous Flow of Growth Opportunities*
- **Growth Strategies:** *Proven Best Practices*
- **Innovation Culture:** *Optimized Customer Experience*
- **ROI & Margin:** *Implementation Excellence*
- **Transformational Growth:** *Industry Leadership*

The Innovation Generator™

Our 6 analytical perspectives are crucial in capturing the broadest range of innovative growth opportunities, most of which occur at the points of these perspectives.



Analytical Perspectives:

- Mega Trend (MT)
- Business Model (BM)
- Technology (TE)
- Industries (IN)
- Customer (CU)
- Geographies (GE)