US Cybersecurity - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2026 - 2031)

Market Report | 2026-02-09 | 120 pages | Mordor Intelligence

AVAILABLE LICENSES:

- Single User License $4750.00
- Team License (1-7 Users) $5250.00
- Site License $6500.00
- Corporate License $8750.00

Report description:

US Cybersecurity Market Analysis

The US cybersecurity market is expected to grow from USD 92.73 billion in 2025 to USD 99.79 billion in 2026 and is forecast to reach USD 144.07 billion by 2031 at 7.62% CAGR over 2026-2031. This expansion is fueled by federal zero-trust mandates, a sharp increase in ransomware attacks on critical infrastructure, and accelerated cloud migration that now places 94% of organizations in multi-cloud settings . On-premise architectures still hold the largest deployment footprint because defense, financial services, and healthcare operators retain legacy systems that must remain behind local controls; however, cloud-delivered security is advancing at a 15% CAGR as enterprises seek scalable protection and real-time threat intelligence. Venture capital continues to stimulate innovation, with USD 11.6 billion invested in US cyber start-ups during 2024, much of it channeled into AI-driven threat-detection platforms that reduce analyst workload. Mandatory SEC breach-disclosure rules, rising cyber-insurance premiums, and a persistent talent shortage collectively reinforce long-term demand, positioning the US cybersecurity market as a strategic priority for both public and private sectors.

US Cybersecurity Market Trends and Insights

Federal Zero-Trust Mandates Accelerating Security Modernization Across Agencies

Executive Order 14028 obliges every civilian agency to adopt zero-trust architecture, triggering multi-year modernization projects that ripple through state and local governments. The Department of Homeland Security recently awarded USD 17 million to ASRC

Federal for USCIS integration services, and the Treasury's new USD 20 billion PROTECTS vehicle underscores federal buying power. Twenty-three states have published their zero-trust roadmaps, with California allocating USD 50 million for identity-centric controls across all agencies by 2026. Contractors must follow suit, extending zero-trust requirements deep into defense and financial services supply chains. The cascade effect positions the US cybersecurity market as the primary beneficiary of sustained public-sector spending.

Surge in Ransomware Attacks Targeting Mid-Market Healthcare and Education Institutions

Change Healthcare's February 2024 breach halted prescription processing for 67,000 pharmacies and cost UnitedHealth Group USD 2.3 billion in remediation. Ascension Health faced a similar disruption three months later when a ransomware attack paralyzed electronic health-record systems across 140 hospitals. The Department of Health and Human Services confirmed that 100 million patient records were exposed last year, fueling federal pressure on hospitals to modernize defenses. Educational institutions are equally vulnerable; the FBI attributes multiple campus closures to ransomware that erased student-services databases. These events amplify spending urgency, pushing healthcare security outlays to an expected 14.6% CAGR, well above the overall US cybersecurity market trajectory.

Fragmented State-Level Privacy Regulations Creating Compliance Complexity for Vendors

CCPA in California, CDPA in Virginia, and CTDPA in Connecticut impose divergent breach-notification and consumer-rights requirements that force vendors to maintain state-specific compliance frameworks. The SEC's amended Regulation S-P now obliges financial institutions to notify individuals within 30 days of a data compromise, overlapping with stricter state deadlines. Mid-market security providers report average annual compliance costs of USD 2.3 million, eroding margins, and deterring market entry. Fragmentation slows product rollouts and complicates go-to-market planning, shaving an estimated 1.2 percentage points from the US cybersecurity market CAGR.

Other drivers and restraints analyzed in the detailed report include:

Adoption of 5G and Edge Computing Expanding the Threat Surface for Critical InfrastructureRapid Migration to SaaS and Multi-Cloud Driving Demand for Cloud-Native Security PlatformsAcute Talent Shortage Elevating Labour Costs and Project Timelines

For complete list of drivers and restraints, kindly check the Table Of Contents.

Segment Analysis

Solutions remain the primary revenue driver, holding 67.30% of the US cybersecurity market share in 2025, while managed services are forecast to grow at a 15.1% CAGR through 2031. Identity and access management adoption surged after federal zero-trust directives, and application security spending expanded alongside containerized development pipelines. Network security appliances face displacement from software-defined alternatives, whereas endpoint protection evolves toward XDR suites that ingest telemetry from laptops, servers and mobile devices. Cloud-security subcategories-particularly cloud-native application protection platforms (CNAPP)-post the fastest acceleration, reflecting multi-cloud complexity that legacy tools cannot address. Professional services hold a resilient niche in compliance audits and incident response, though the labor shortage constrains capacity and pushes billable rates higher.

Managed services growth stems from acute talent constraints and regulatory pressures that force even resource-rich enterprises to seek external expertise. MSSPs increasingly deliver security-operations-centre (SOC) functions via subscription, lowering entry thresholds for mid-market businesses. The offering mix is also shaped by tool-sprawl fatigue: 90% of large organizations run

overlapping vulnerability scanners that they now seek to consolidate into integrated platforms. Vendors respond by embedding AI analytics and orchestration features, reinforcing solution stickiness and expanding average revenue per customer. Consequently, solutions retain scale, while services inject higher growth velocity into the overall US cybersecurity market.

On-premises setups accounted for 57.20% of revenue in 2025, largely because defence, financial-services and healthcare sectors must preserve data sovereignty and legacy integrations. Federal agencies continue to maintain classified networks behind air-gapped environments, although analytics layers increasingly migrate to commercial clouds. Financial institutions such as JPMorgan Chase invest in hybrid architecture that combines on-premises key-management with cloud-native detection, ensuring regulatory compliance without sacrificing agility.

Cloud-delivered security solutions expanded at a 14.4% CAGR, buoyed by reduced capital spending, elastic scaling and the speed of software-as-a-service rollouts. Organizations deploying SECaaS report implementation cycles 40% shorter than appliance-based alternatives, accelerating time to risk reduction. Providers integrate threat-intelligence feeds and behavioral analytics, delivering a continuously updated control plane that adapts to evolving attacker techniques. The growth differential widens the revenue gap over time, causing the on-premises slice of the US cybersecurity market to contract in relative terms, even as absolute spending remains stable in compliance-heavy industries.

The US Cybersecurity Market Report Segments the Industry Into Offering (Solutions, Services), by Deployment Mode (Cloud, and On-Premise), by Organization Size (SMEs, and Large Enterprises), by End User (BFSI, Healthcare, and More). The Market Forecasts are Provided in Terms of Value (USD).

List of Companies Covered in this Report:

Cisco Systems, Inc. Palo Alto Networks, Inc. Microsoft Corporation (Security BU) Fortinet, Inc. IBM Corporation CrowdStrike Holdings, Inc. Check Point Software Technologies Ltd. Zscaler, Inc. Okta, Inc. Trend Micro Incorporated Splunk Inc. Proofpoint, Inc. Cloudflare, Inc. Mandiant (A Google Cloud Company) Rapid7, Inc. SentinelOne, Inc. Sophos Ltd. Darktrace plc Akamai Technologies, Inc. Netskope, Inc. Arctic Wolf Networks, Inc.

Additional Benefits:

The market estimate (ME) sheet in Excel format
3 months of analyst support

Table of Contents:

US Cybersecurity - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2026 - 2031)

Market Report | 2026-02-09 | 120 pages | Mordor Intelligence

To place an Order with Scotts International:

- - Print this form
- - Complete the relevant blank fields and sign
- - Send as a scanned email to support@scotts-international.com

ORDER FORM:

Select license	License	Price
	Single User License	$4750.00
	Team License (1-7 Users)	$5250.00
	Site License	$6500.00
	Corporate License	$8750.00
	VAT	
	Total	

*Please circle the relevant license option. For any questions please contact support@scotts-international.com or 0048 603 394 346.

** VAT will be added at 23% for Polish based companies, individuals and EU based companies who are unable to provide a valid EU Vat Numbers.

Email*		Phone*	
First Name*		Last Name*	
Job title*			
Company Name*		EU Vat / Tax ID / NIP number*	
Address*		City*	
Zip Code*		Country*	
		Date	2026-02-26
		Signature