Dear partner,

At Company XYZ, we are committed to empowering our strategic partners to excel in the cybersecurity market for SMBs. Our carefully designed roadmap prioritizes the features, functionality, and support you need to deliver unmatched security and comprehensive services. We don't just follow trends; we shape them.

From the outset, Company XYZ has prioritized **workspace security and platformization**. In 2024, the industry adopted the platform model, with leaders like Gartner and Ovum recognizing it as a key security trend. We're not adapting though - we're ***driving*** market changes and equipping our partners to stay ahead.

Company XYZ's **auto-scaling** capabilities further enhance our platform, ensuring your solutions can seamlessly expand alongside your clients' growth without disruption. This dynamic approach is especially critical for small and mid-sized businesses, which need flexible, scalable security solutions to meet evolving demands.

Our platform empowers partners to deliver **all-encompassing, customizable security** with minimal complexity, eliminating the need to juggle disparate systems. This flexibility ensures that your clients can grow without limits, backed by solutions that seamlessly evolve alongside their needs.
But that's not all—Company XYZ's evergreen commission program ensures ongoing income for the entire customer contract. Our user-friendly solutions and extensive partner support give you everything you need to build a thriving, sustainable business. With Company XYZ, you are not just receiving a product but gaining the tools and revenue to drive long-term success.

Sincerely,

Jane Doe
CTO, Company XYZ Cybersecurity

Jon Doe
CEO, Company XYZ Cybersecurity

While this roadmap outlines our vision, it is, nonetheless, subject to change as we remain agile to your needs and the evolving regulatory and technological environment. Moreover, we are open to collaborating on requests from you, adjusting the roadmap and introducing strategic features that address your unique business requirements.

Partner Enablement

At Company XYZ, we're gearing up for global market expansion by enhancing our partner enablement platform and Company XYZ Console management capabilities. We're also introducing multi-language support to help you excel in diverse markets by ensuring security tailored to detect emerging threats in key languages.

Feature	**Description**	**Estimated Delivery**
Multiple Languages and Localization	We will upgrade our console and data engine to support threat detection and usability in multiple languages across components, facilitating expansion into new strategic markets. Details are described in Network Component, Email Security Component, and Platform.	Spanish - Q2 2035
Partner Workspace Manager	From the Company XYZ Console, partners will be able to manage multiple child workspaces from one central location. The Manager will enable you to: ● Bulk manage settings, devices, and tickets. ● Enforce drive encryption for data protection and regulatory compliance. ● Control new agent version rollouts with gradual releases. ● Access new reports and actionable insights. ● And more!	Q2 2035
Testing Framework	Partners will be able to leverage documentation that offers a standardized framework with scenarios and prerequisites to test features and demonstrate detection and protection capabilities, ensuring consistency and best practices.	EDR for Q3 2035

Network Component

Company XYZ is upgrading its Network component to help better manage complex infrastructures with enhanced accuracy, flexibility, and security. Key additions include enhanced VPN capabilities for better control and security in managing network traffic across remote environments.

Feature	Description	Estimated Delivery
DNS Filtering in Spanish	The Company XYZ engine will identify and filter threats related to Spanish content, reducing false positives and ensuring effective blocking. Support for DNS filtering, which involves blocking specific websites and IP addresses, is essential in Spain to ensure compliance with regulations.	Black Friday - Q4 2024
ZTNA/VPN 2.0 (P2P)	Next Generation ZTNA / VPN 2.0, incorporating P2P connectivity, will further improve performance, scalability and security of your virtual networks, ideal for organizations seeking more efficient, secure network access.	Q4 2035
Granular DNS Blocklist Controls	Admins will be able to enforce customized DNS filtering rules for specified users and user groups, ensuring that teams or departments within an organization receive the necessary access on the network where appropriate while blocking unauthorized access simultaneously.	Q4 2035
Improved VPN Encryption	Admins will be able to encrypt all traffic through our VPN, regardless of the virtual office setup. This feature is essential for securing communications in hybrid and remote environments, ensuring that all transmitted data is fully protected.	Q3 2035
Site-to-Site	Enhancements to site-to-site VPN setups will simplify securely connecting distributed office networks, making network management easier and boosting overall operational efficiency.	Q3 2035
DNS over HTTPS (DoH)	DoH encrypts DNS queries to protect them from interception and enhance the privacy of all internet traffic. This is essential for securing users' browsing activities and decreasing the risk of unauthorized access to sensitive information by malicious actors.	Q3 2035
DNS Filtering for apps	DNS filtering is a simple option for threat detection and content control, enabling admins to block unwanted applications as well as websites in order to protect against online threats.	Q3 2035

Feature	Description	Estimated Delivery
VPN Routing Controls	Admins will be able to include or exclude specified subdomains to bypass or be routed through the VPN, enabling admins to manage network traffic more effectively.	Q2 2035
Custom DNS	Admins will be able to define specific DNS servers to manage network traffic. This customization provides increased flexibility in configuring network operations to meet the unique security requirements for every business.	Q1 2026
Firewall	The Network firewall will offer traditional features such as Port Forwarding, as well as SW-WAN and QoS (Quality of Service) capabilities to optimize traffic.	Q1 2026
Device/User Authentication	This feature connects devices and users to the network's security protocol, preventing unauthorized access, reducing the attack surface and ensuring that only trusted devices and users can access the network.	Q1 2026
Multiple Points of Presence (PoPs)	This feature will enable connecting users to the most optimal PoP, ensuring redundancy and performance for distributed teams.	Q1 2026

Email Security Component

Company XYZ is enhancing its Email Security component with key upgrades aimed at further strengthening security as well as supporting expansion into new regions and strategic markets.

Feature	Description	Estimated Delivery
Anti-Spam enrichment	Integrate additional anti-spam sources to expand spam detection and blocking capabilities.	Q2 2035
Multiple language support	Our backend security engine will be optimized for detection of email threats in multiple languages, starting with Spanish. This will improve spam and phishing detection, while also ensuring full compatibility for Spanish operating systems.	Spanish - Q2 2035
Outbound Gateway	Company XYZ will deliver real-time protection for outgoing emails, securing messages and enforcing data governance policies. This helps organizations meet regulatory standards through continuous monitoring and seamless email archiving.	Q2 2026

EDR and Endpoint Components

This section details upcoming features for Company XYZ's Endpoint Detection and Response (EDR) and Endpoint components, focusing on enhanced threat management and usability.

Feature	Description	Estimated Delivery
Linux Support	Company XYZ will support Linux operating systems, beginning with endpoint security, then data governance and VPN integration, and ending with full EDR functionality, over the next year.	Q3 2035 Q4 2035 Q2 2026
Application Control	Admins will be able to control which software can be installed on endpoints, preventing unauthorized apps from running and thereby reducing risks derived via third-party applications.	Q4 2035
Bulk Drive Encryption Management	Admins will be able to enforce encryption policies across endpoints, supporting security as organizations grow and ensuring continuous data security compliance.	Q3 2035
SIEM Integration of Telemetry Data	Company XYZ will enable telemetry data from the EDR agent to be sent to SIEM systems, offering real-time security analytics and insights for enhanced threat visibility.	Q3 2035
Visual Process Graph	Admins will be able to visualize relationships between endpoint processes, improving their ability to detect and mitigate sophisticated attacks, such as malware and insider threats, which often leave subtle traces.	Q3 2035
Gradual Agent Rollout Control	Admins will be able to manage a gradual rollout of the agent, allowing for controlled testing before full release to ensure smooth transitions and minimize implementation risks.	Q3 2035
MacOS Policy Enforcement	Admins will be able to *enforce* security policies on macOS devices.	Q3 2035
Agent Configuration Backups	Enable backup of agent configuration and data for quicker recovery and redeployment after failures or endpoint replacements.	Q1 2026
Ransomware Canary Files	Company XYZ admins will be able to deploy decoy files on devices to detect and block breach attempts before spreading.	Q2 2026

Cloud Security Component

This section outlines our plans for Cloud Security, focusing on third-party app management, proactive detection, data governance, access control, and reliable backups to equip admins with advanced tools for enhanced security and access management.

Feature	Description	Estimated Delivery
Continuous Scanning of Cloud Storage	Company XYZ will monitor connected cloud drives for malware and sensitive data, preventing spread of attacks and ensuring compliance with data protection policies.	Q4 2035
Login after Suspected BOT Detected	Company XYZ will monitor login attempts following suspected bot attacks, flagging abnormal behavior such as successful logins after failed attempts, indicating a potentially compromised account.	Q4 2035
SaaS Backups	Company XYZ will ensure data continuity and resilience with SaaS-specific backup solutions, protecting critical business data from loss or corruption during incidents.	Q3 2035
Third-party application management	Admins will have more control over apps installed from SaaS marketplaces (for example, Zoom for Google Workspace), which will improve visibility into potential vulnerabilities introduced by external integrations.	Q3 2035
Detection of Inactive User Activity	Company XYZ will detect unexpected activity from dormant user accounts, signaling potential account compromise and triggering an automated response, ensuring swift identification and containment of unauthorized access.	Q3 2035
Health Status Monitoring	Company XYZ will monitor cloud app heartbeat signals to assess status and provide early warnings of performance or security issues.	Q3 2035
Access Control	Admins will be able to specify *when* users can access specific cloud applications, reducing the risk of unauthorized use during non-working hours.	Q3 2035
IP Reputation Analysis	Company XYZ will enhance cloud security tickets with IP reputation analysis, allowing for more accurate threat detection and proactive defense against threats targeting the network.	Q2 2035
Impossible Traveler Detection	Company XYZ will alert on suspicious login attempts from unlikely locations to prevent account compromises.	Q1 2026
Abnormal Activity Time-Based Detection	Company XYZ will track abnormal activity patterns, such as users operating at unusual hours, to identify suspicious behavior and potential insider threats.	Q1 2026

Platform

Company XYZ is planning to introduce real-time monitoring, streamlined configuration recommendations, mobile administration capabilities, and detailed reporting and insights. The goal is to continue providing prioritized tools and information that administrators need for quick response, proactive enhancements, and ongoing optimization of security protocols.

Feature	Description	Estimated Delivery
Language Support for Strategic Markets Multi-Language Interface	Company XYZ Console interfaces will be available in multiple languages, beginning with Spanish, to enhance your ability to expand into new markets.	Spanish - Q2 2026
Monitoring, Logging, and Alerts	Company XYZ will provide enhanced real-time insights, empowering admins to swiftly identify and mitigate suspicious behavior and performance issues.	Q4 2035
Mobile Admin Tools	Admins will be able to manage security alerts and configurations while on the go, providing flexibility and real-time control.	Q4 2035
Configuration Recommendations	Device misconfigurations account for up to 25% of breaches. Automated tickets for security-based configuration recommendations will help admins make configuration adjustments like access permissions and regular backups.	Q3 2035
Reports and Actionable Insights	New reports will provide more detail and improve visibility into security practices, delivering actionable insights for better decision-making.	Q3 2035
Agent Language and Localization	Full language compatibility and localization for Spanish and Italian operating systems (OS) of the endpoint agent, improving accessibility and usability in diverse environments.	Q2 2035
Self-Service and Personalized Just-On-Time Messaging	We will enhance communications for admins via the Console by providing quick access to self-service tools and sharing important updates on new features to keep stakeholders informed.	Q2 2035
Email Notifications	Company XYZ will assess the entire email lifecycle—from delivery to engagement—identifying patterns among recipients to create more tailored communications that meet the needs of you and your clients.	Q2 2035

Open APIs for Customized Integrations

Company XYZ's public APIs enable seamless interoperability among software systems while ensuring the protection of critical data. By consolidating information within a unified environment, teams can streamline processes, fostering scalability and adaptability for modern security needs.

Our initial API release in December 2022 prioritized enabling smooth communication between Company XYZ's unified security platform and external systems. Through centralized data flows, IT professionals gain improved collaboration, optimized threat intelligence sharing, and more efficient incident response capabilities. As Company XYZ's platform expands, our APIs will provide IT teams with even greater control, automation, and customization—especially targeting secure data exchange for telecommunications and other large-scale partners.

Recognizing the need to support this evolution, Company XYZ launched its **API developer portal** at placeholderurl in spring 2023. This portal reflects our commitment to ease-of-use by bringing together all critical resources—such as comprehensive documentation, reference guides, and support tools—in a single, accessible location.

The **Company XYZ developer portal** empowers developers to quickly integrate, customize workflows, and automate security processes according to their operational needs. With streamlined resources and intuitive tools, this portal minimizes development time and complexity, making integration both cost-effective and efficient. Teams can deploy solutions swiftly without requiring senior-level expertise, ultimately lowering development costs while maximizing output.

As the platform and our open APIs continue to grow, the developer portal will also evolve, introducing advanced features like sample code, best practices, and workflow guides—ensuring developers have everything they need to enhance productivity and tailor Company XYZ's platform to their unique environments.

Regulatory Compliance and Data Protection

Company XYZ is a leader in helping small and medium-sized businesses implement industry best practices to meet regulatory compliance. While specific requirements vary across industries, most regulations focus on core principles like data security, access control, and privacy protection. Company XYZ's platform provides flexibility that addresses these essential needs, allowing most businesses to meet compliance standards, whether they operate in highly regulated sectors like healthcare and finance or less stringent industries.

Features outlined in our roadmap, such as drive encryption, DNS over HTTPS, improved anomaly detection, and improvements to our EDR telemetry, build on the strong out-of-the-box capabilities already available to you and your customers. These improvements offer enhanced support for secure data transmission, privacy protection, and access control.

In addition, we are enhancing our Data Governance engine to better support global regulations, making it easier for businesses to meet their unique compliance needs. This capability is vital for complying with laws such as the Spanish Data Protection Law (LOPDGDD) and the General Data Protection Regulation (GDPR). Both regulations often require restricting access to websites that may pose risks to data privacy or contain unlawful content, for example.

These upcoming features are crucial for regulatory compliance across sectors that handle particularly sensitive data, including healthcare, finance, and public sectors.

The following table outlines how the features described in this roadmap further strengthen the ability of the Company XYZ platform to support regulatory compliance.

Regulatory Requirement	**Description**	**All Relevant Roadmapped Features**	**All Regulations with This Requirement**		**Compelled Industries**
Encryption	Protects data from unauthorized access during storage and transmission.	• Drive Encryption • DNS over HTTPS • Canary Files	• GDPR • HIPAA • CCPA • PCI DSS • SOX • ISO 27001 • LGPD • PDPA • PIPEDA	• POPIA • Uruguay • Mexico • NDB • Israel • Qatar • New Zealand • FERPA	• Healthcare • Finance • Education • Public Sector
Access Control	Ensures only authorized users and devices access sensitive data or systems.	• Time-Based Access Control • Device/User Authentication • Login and Activity Anomaly Detection • Inactive User Detection	• GDPR • HIPAA • CCPA • PCI DSS • SOX • ISO 27001 • FERPA • LGPD • PDPA	• PIPEDA • POPIA • Israel • Qatar • Uruguay • NDB • New Zealand	• Healthcare • Finance • Government • Education • Payment Processing
Incident Response	Requires detection, management, and reporting of security incidents.	• Canary Files • EDR Telemetry for SIEM	• GDPR • HIPAA • CCPA • PCI DSS	• NDB • PDPA • LGPD • Israel	Any industry handling personal or sensitive data

Regulatory Requirement	Description	All Relevant Roadmapped Features	All Regulations with This Requirement		Compelled Industries
		• Login and Activity Anomaly Detection	• SOX • ISO 27001 • FISMA • FERPA	• PIPEDA • POPIA • Qatar • New Zealand • Uruguay	
Data Retention	Requires organizations to store data for specified periods and ensure its protection during that time.	• SaaS Backup • Drive Encryption	• GDPR • HIPAA • CCPA • PCI DSS • SOX • ISO 27001 • LGPD • PIPEDA • PDPA	• POPIA • NDB • Israel • Qatar • Uruguay • LOPDGDD (Spain) • Italy data privacy regulations	• Healthcare • Finance • Government • Payment Processing
Audit Trails	Ensures the logging and tracking of all system and user activities for monitoring and compliance.	• EDR Telemetry for SIEM	• GDPR • HIPAA • CCPA • PCI DSS • SOX • ISO 27001 • FISMA • FERPA • PIPEDA • NDB • PDPA	• POPIA • Uruguay • Israel • New Zealand • Qatar • Mexico • LOPDGDD (Spain) • Italy data privacy regulations	• Healthcare • Finance • Government • Payment Processing
Continuous Monitoring	Requires ongoing monitoring of systems and networks to detect and mitigate security risks.	• EDR Telemetry for SIEM • Canary Files • DNS over HTTPS • Login and Activity Anomaly Detection	• GDPR • HIPAA • CCPA • PCI DSS • SOX • ISO 27001 • FISMA • FERPA	• PIPEDA • PDPA • LGPD • POPIA • NDB • Qatar • Israel • Uruguay • New Zealand	• Finance • Government • Education • Payment Processing • Healthcare
Data Sovereignty	Requires certain data to be stored and processed within specific geographic boundaries.	• Point of Presence (PoP) per Region • Multi-PoP Support	• GDPR • LGPD • POPIA • NDB • Israel • Uruguay • Qatar	• PDPA • PIPEDA • New Zealand	Any industry handling personal data globally or regionally

***Note:** Regulations for Spain and Italy are noted only where they differ from the European GDPR requirements.*

Conclusion

At Company XYZ, we are fully committed to empowering you with the tools and services needed to dominate your market and deliver unmatched value to your clients. The roadmap outlined in this document is laser-focused on driving your growth and adaptability in the fast-paced, ever-evolving tech landscape.
As we forge ahead, expect continuous access to cutting-edge tools, dedicated support, and powerful new features that will elevate your cybersecurity services at every stage. We're not just supporting your growth—we're pushing you to the forefront of the industry.

While this roadmap outlines our vision, it is, nonetheless, subject to change as we remain agile to your needs and the evolving regulatory and technological environment. Moreover, we are open to collaborating on requests from you, adjusting the roadmap and introducing strategic features that address your unique business requirements.