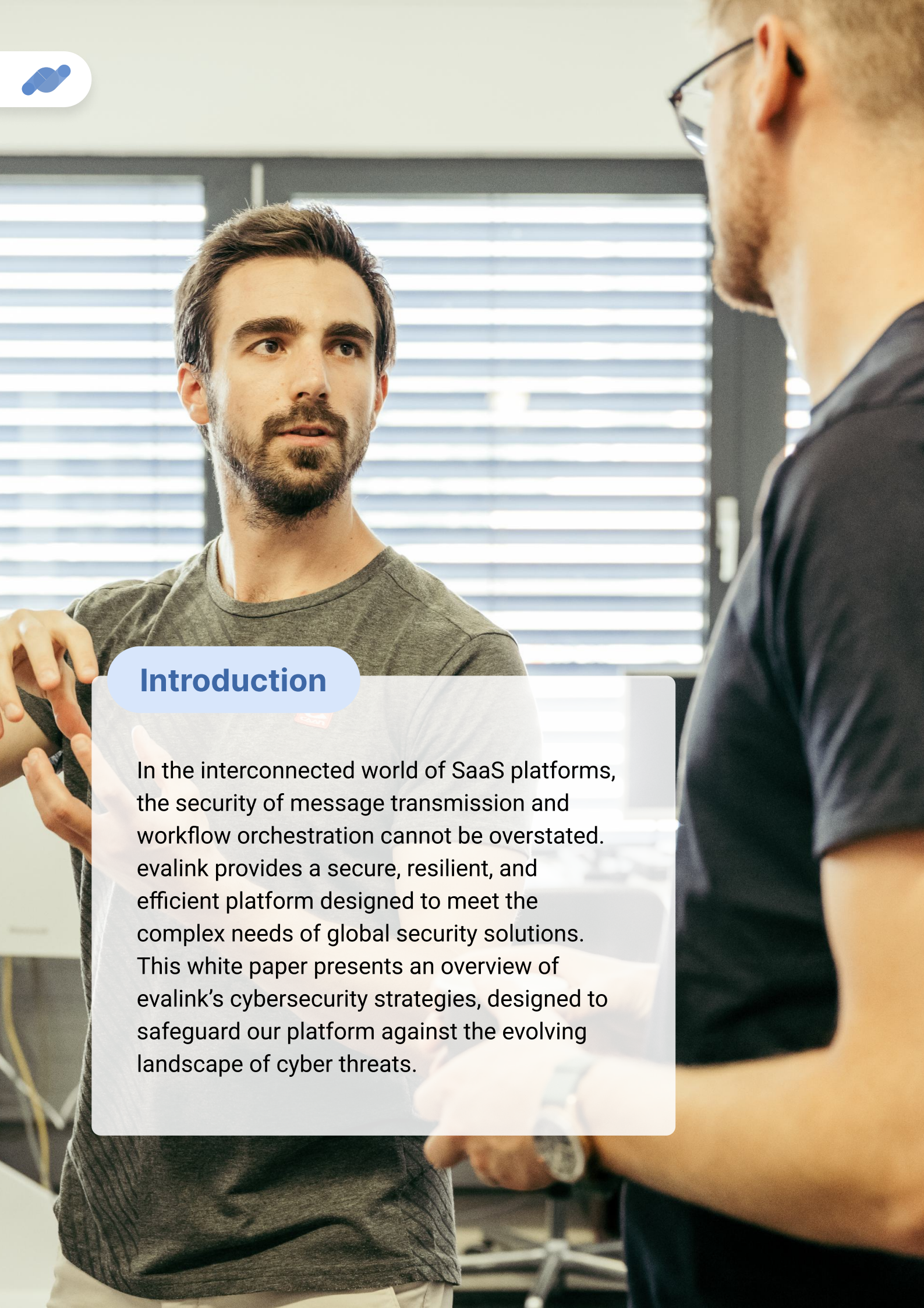
evalink | Whitepaper

Ensuring cybersecurity excellence in evalink

Executive summary

evalink operates at the forefront of secure message transmission and responder workflow orchestration, offering integrated security solutions on a global scale. In an era where cybersecurity threats are increasingly sophisticated and pervasive, evalink prioritizes robust cybersecurity measures to protect its platform and its users. This white paper outlines our comprehensive cybersecurity framework, from our security-by-design principles and stringent testing protocols to our adherence to international standards and continuous monitoring and improvement practices.



Introduction

In the interconnected world of SaaS platforms, the security of message transmission and workflow orchestration cannot be overstated. evalink provides a secure, resilient, and efficient platform designed to meet the complex needs of global security solutions. This white paper presents an overview of evalink's cybersecurity strategies, designed to safeguard our platform against the evolving landscape of cyber threats.

Zero Trust Architecture

Adhering to a zero-trust architecture, we require stringent authentication and authorization for all service interactions, underscoring our commitment to a security-first approach in every aspect of our platform's operation.

Security by Design

At evalink, our architecture is built on the foundational principles of least privilege and shared nothing. Each microservice within our platform is meticulously designed to require authentication via our central Identity and Access Management (IAM) system, ensuring services are authorized to perform only designated actions. This approach minimizes potential attack vectors and reinforces our commitment to security at every layer of our platform.

Testing and Development Security

Our deployment process incorporates rigorous security and resilience testing, employing both automated tools and manual expertise to scrutinize our services in environments that mimic real-world conditions. This ensures that our platform not only meets but exceeds the industry standards for security and performance.

Cloud Infrastructure and Resilience

evalink's infrastructure leverages a dual-region setup across multiple availability zones, ensuring unparalleled service continuity and resilience. Utilizing AWS Global Accelerator, we enhance our platform's latency, availability, and resistance to DDoS attacks, underpinned by the protection of AWS Shield.

Secure Network Infrastructure and Access

At the heart of evalink's cybersecurity strategy is a network infrastructure, which upholds the highest standards of security and accessibility. All internet-facing services are accessible solely through load balancers residing within secured perimeter zones, commonly referred to as Demilitarized Zones (DMZs). Our internet-facing services are shielded by comprehensive AWS-powered protections, including firewalls and Web Application Firewalls (WAF).

Identity and Access Management

Central to evalink's security framework is our advanced identity and access management (IAM) system, powered by Auth0. Auth0 is a leading provider in IAM solutions, offering a robust and flexible platform that ensures secure and seamless authentication and authorization processes across our services.

Data Encryption

We enforce strict encryption protocols for all data in transit and at rest. By implementing TLS/SSL for data in transit and utilizing AWS's encryption services for data at rest, alongside the advanced AES-256 encryption standard, we ensure the integrity and confidentiality of our data.

Continuous Monitoring and Response

Our security operations team monitors our systems around the clock, employing advanced anomaly detection and leveraging AWS GuardDuty and Security Hub for comprehensive oversight of potential threats. This proactive stance allows us to mitigate risks before they impact our service.

Penetration Tests

We ensure the security of our software and Services by conducting penetration tests by renowned security external companies. These tests are an essential part of our security strategy, allowing us to identify vulnerabilities and rectify them before they can be exploited. By engaging with external experts, we benefit from an unbiased perspective, ensuring that our security measures are both robust and up to date.

Regular Threat Modelling and OWASP Assessments

Regular threat modelling and OWASP assessments are conducted by our cybersecurity teams to continuously evaluate and improve the security posture of our platform. These practices help in identifying potential vulnerabilities and ensuring that our defenses are aligned with the latest security standards and best practices. Through thorough and consistent assessments, we maintain a proactive stance against cybersecurity threats, safeguarding our infrastructure and protecting our clients' data.

Audit and Compliance

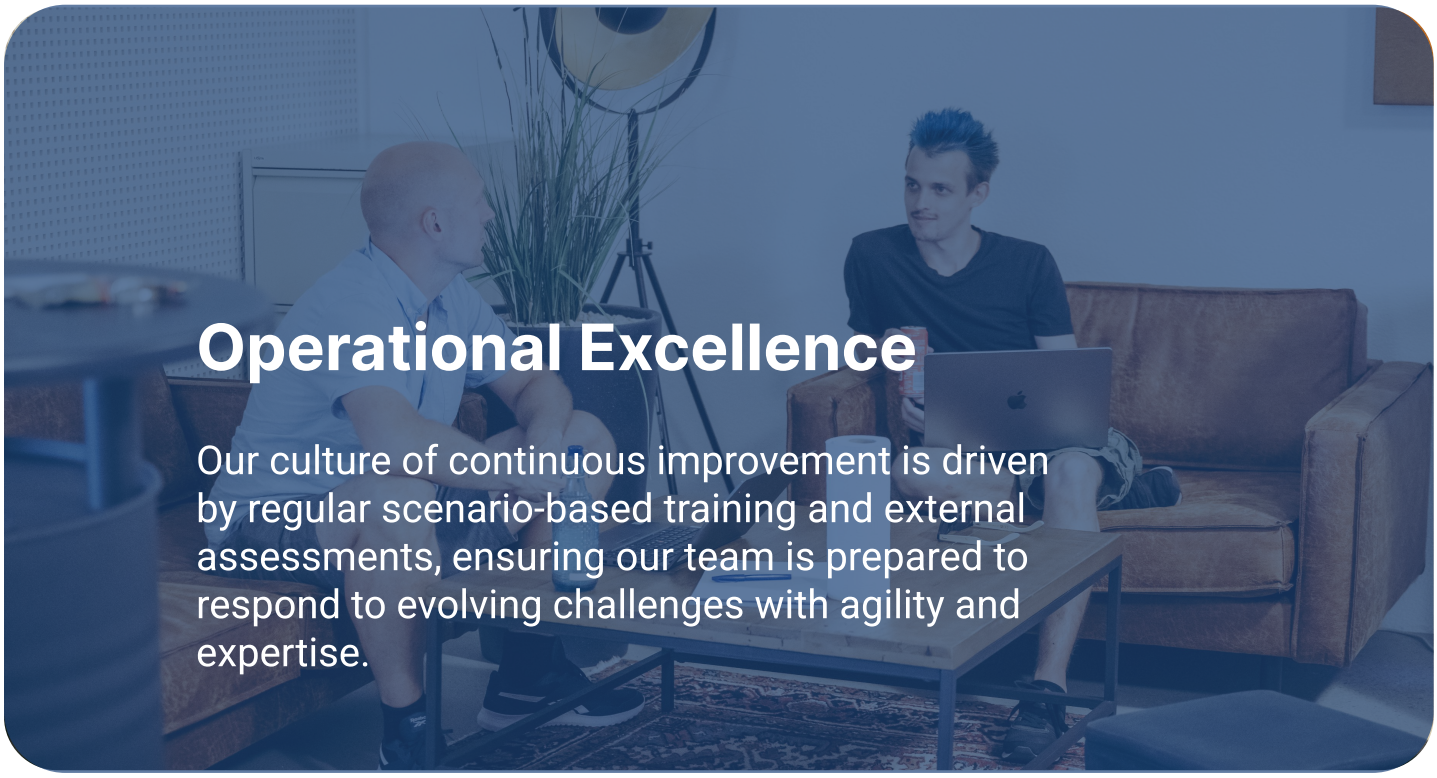
Our commitment to security is validated by regular penetration testing conducted by external experts, affirming the resilience of our software and services. Furthermore, our practices are certified against ISO 9001 and ISO 27001 standards, and we continuously refine our architecture through the AWS Well-Architected Review.

Human Factor and Employee Security

Recognizing the critical role of human factors in cybersecurity, we implement stringent security clearance protocols for all prospective employees, complemented by extensive, role-specific training. This ensures our team is not only highly skilled but also deeply versed in the principles of information security.

Malicious Content

We employ robust measures to scan all uploaded files for viruses and malicious code, ensuring insecure content is promptly identified and blocked.



Operational Excellence

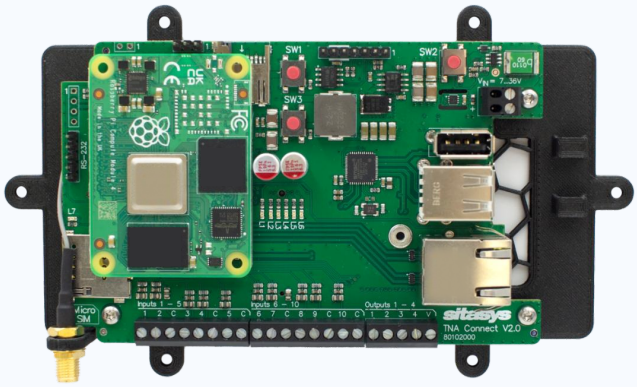
Our culture of continuous improvement is driven by regular scenario-based training and external assessments, ensuring our team is prepared to respond to evolving challenges with agility and expertise.

evalink transmitter (TNA) Hardening

The security of our TNA transmitters, including the TNA 4i and TNA Connect, is of paramount importance to us. To enhance their security, we utilize Buildroot for the immutable firmware of these devices. Buildroot facilitates the creation of highly tailored builds by allowing us to include only the necessary packages and components. This approach significantly minimizes the attack surface by reducing the number of potential vulnerabilities present in the system.

One of the key advantages of using Buildroot is that it builds the system from source, granting us complete control over the versions of packages used. This control is critical for security, as it enables us to apply patches and respond to vulnerabilities swiftly. Our ability to quickly integrate security patches as soon as they are available ensures that our TNAs are protected against known vulnerabilities at all times.

Moreover, the firewall on our TNAs is configured to enhance security further. It does not allow incoming traffic and is configured not to respond to ICMP messages, which makes it more challenging for network scanners to detect our devices.



evalink TNA Connect

evalink

CONCLUSION

At evalink, cybersecurity is not just a policy; it's a core aspect of our culture and operations.

Our ongoing commitment to safeguarding our platform is evidenced by our rigorous security measures, continuous improvement practices, and compliance with international standards. As we move forward, evalink remains dedicated to enhancing our cybersecurity framework, ensuring we remain at the cutting edge of secure SaaS solutions.

Contact us for more information: evalink.io/contact