Take the Lead in Email Security with Cyberus Systems ZTSaaS

Cyberus Systems ZTSaaS: The Vanguard of Email Security in a Zero Trust World.

Email remains one of the most ubiquitous forms of communication in the business world, but it also represents one of the largest security vulnerabilities. **Cyberus Systems' Zero Trust Security as a Service (ZTSaaS)** addresses this vulnerability head-on, integrating a comprehensive suite of email security services that adhere to the Zero Trust model's strict 'never trust, always verify' principle.

The Criticality of Email Security

Email security is a cornerstone in the architecture of the Zero Trust model. Since email is a common vector for phishing, malware, and data breaches, implementing rigorous email security protocols is essential. In a Zero Trust framework, every email, regardless of origin, is treated as a potential threat and subjected to stringent security checks to protect your organization's sensitive data and systems.

As of April 2023, here are some key cybersecurity attack and breach statistics specifically related to Email Security:

1. **Phishing Attacks Prevalence**: Phishing attacks, often initiated via email, are among the most common cybersecurity threats. According to the 2021 Verizon Data Breach Investigations Report, phishing was involved in 36% of breaches.

2. **Spear Phishing and Targeted Attacks**: Spear phishing, where specific individuals or organizations are targeted, has become increasingly prevalent. The FBI's 2020 Internet Crime Report noted that business email compromise (BEC) schemes caused over $1.8 billion in losses.

3. **Malware Delivery**: A significant percentage of malware is delivered via email. Reports suggest that 1 in every 3,722 emails in 2021 contained malware.

4. **Ransomware via Email**: Email remains a common vector for ransomware attacks. Symantec's 2021 Internet Security Threat Report indicated that 65% of ransomware was installed via email phishing.

5. **Email Account Compromise**: Compromised email accounts are a frequent issue, often leading to further data breaches. Microsoft's Digital

Defense Report stated that credential phishing accounted for over 70% of email-based attacks they observed.

6. **Data Breaches Involving Email**: A significant number of reported data breaches involve unauthorized access to or disclosure of emails containing sensitive information.

7. **Cost of Email-based Attacks**: The average cost of email-related breaches remains high. According to IBM's Cost of a Data Breach Report 2021, the average total cost of a data breach was $4.24 million, with email breaches being a significant contributor.

8. **COVID-19-Themed Email Attacks**: The pandemic saw a rise in COVID-19-themed phishing emails, exploiting the crisis to trick individuals and organizations into revealing sensitive information.

9. **Impersonation and Social Engineering**: Email-based attacks increasingly involve impersonation and social engineering tactics. Fake emails from supposedly trusted sources remain a common method for deceiving recipients.

10. **Rise in Email Security Solutions**: In response to these threats, the adoption of advanced email security solutions, including those using AI and machine learning for detecting and responding to threats, has increased.

These statistics underscore the critical importance of robust email security measures, including employee education on recognizing phishing attempts, implementing advanced email filtering and monitoring solutions, and regularly updating security protocols.

Future Predictions and Projections

- **Enhanced Email Security Measures**: With the growing threat from email attacks, businesses are expected to invest more in advanced email security solutions, including AI and machine learning-based systems.

- **Increased Use of Multi-Factor Authentication (MFA)**: MFA is predicted to become a standard security measure for accessing email systems to prevent unauthorized access.

- **Greater Emphasis on User Training**: Organizations will likely increase their focus on training employees to recognize and respond to phishing and other malicious emails.

- **Development of Advanced Phishing Techniques**: Attackers are expected to use more sophisticated methods, including deepfakes and AI-generated content, to make phishing emails more convincing.

Cyberus Systems Impact on your Business's Security Posture.

Robust email security reinforces an organization's overall security posture by:

- Mitigating the risk of phishing and spear-phishing attacks that target employees.

- Preventing malware and ransomware from compromising systems through email.

- Ensuring confidential information remains secure through encryption.

- Complying with industry regulations by protecting personal and sensitive data transmitted via email.

Our solutions are tailored to align with the CISA Zero Trust Maturity model, providing protection

that meets traditional, advanced, and optimal security needs:

Traditional:

- **In & Outbound Email Spam Filtering:** Filters out known threats and unwanted messages, maintaining the integrity of your email communications.

- **Email Encryption:** Protects the confidentiality of your email communications, ensuring that sensitive information remains secure.

Advanced:

- **Phishing Simulation and Cyber Email Scams Protection:** Prepares your team to recognize and respond to sophisticated phishing and scam attempts.

- **White & Blacklist in Spam Filter:** Enhances productivity by allowing critical emails through while blocking harmful or irrelevant messages.

Optimal:

- **Spear Phishing Protection:** Utilizes advanced threat intelligence to protect against targeted attacks on your organization's key personnel.

- **Malicious URL Protection:** Prevents access to harmful websites through real-time scanning of URLs within emails.

Cyberus Systems ZTSaaS Edge Bolsters your Business Security Posture

With Cyberus Systems' ZTSaaS, your organization benefits from:

- **Regulatory and Standard Compliance:** Our email security solutions meet and exceed GDPR, HIPAA, PCI DSS, and other regulatory standards.

- **Layered Email Protection:** We provide a multi-faceted approach to email

security, from user training to advanced threat detection.

- **Technological Sophistication:** Our use of advanced threat intelligence and machine learning keeps you ahead of the latest email-based threats.

- **Proactive Threat Mitigation:** We employ predictive analytics and real-time monitoring to prevent threats before they impact your business.

Cybersecurity Statistics Highlighting the Need for Advanced Email Security

- **Phishing Prevalence:** Over 90% of cyber-attacks start with a phishing email, emphasizing the need for robust email security measures.

- **Effectiveness of User Training:** Organizations that conduct regular phishing training reduce susceptibility to phishing attacks by up to 40%.

- **Cost of Email Breaches:** Email compromises account for significant financial losses, escalating average costs into millions of dollars.

Step Up Your Email Security with Cyberus Systems

Don't let your email be the weak link in your security chain. Partner with Cyberus Systems for a comprehensive Zero Trust Security Assessment to identify gaps in your email security and discover how our ZTSaaS can fortify your digital communications against advanced threats.

Digitally Transform Your Business with Cyberus Systems ZTSaaS

Don't wait for a breach to reveal the weaknesses in your business security posture. Contact Cyberus Systems today to learn how our ZTSaaS can bolster your defenses with a zero-trust approach aligned with regulatory and industry standards.

Step into the Future of Cybersecurity with Cyberus Systems ZTSaaS

Embrace a Zero Trust security model that anticipates threats, adapts to new challenges, and acts to secure your endpoints. With Cyberus Systems, you're not just implementing a security solution; you're investing in a security partnership that prioritizes the protection of your most valuable assets.

Take the Next Step in Your Zero Trust Journey with Cyberus Systems' ZTSaaS

Are you ready to reinforce your organization's digital defense? It's time to act. Cyberus Systems invites you to elevate your cybersecurity posture with our state-of-the-art Zero Trust Security as a Service.

Step beyond the limitations of traditional defense in depth and safeguard your enterprise with our holistic, Zero Trust approach.

Embrace a future where every identity is meticulously validated, every access is scrutinized, and every user interaction is an opportunity to fortify your security.

Initiate Your Zero Trust Security Transformation

Unlock the full potential of cutting-edge identity protection. Begin your journey with a comprehensive Zero Trust Security Assessment from Cyberus Systems. Our expert team guides you through a detailed evaluation of your security measures, identifies potential vulnerabilities, and provides tailored recommendations to enhance your defenses.

Connect with Cyberus Systems Today! Start your Journey Toward ZTSaaS

Contact us to schedule your Zero Trust Security Assessment: https://cyberussystems/aspirin. Let us demonstrate how our ZTSaaS solutions can align with your unique needs, ensuring compliance with the most stringent regulatory and industry standards. Choose Cyberus Systems and commit to advanced, proactive security.

Your Next Steps:

1. *Please schedule a Consultation:* Reach out to our team and schedule a time to discuss your organization's security needs.

2. *Zero Trust Security Assessment:* Allow us to conduct a thorough assessment and tailor a strategy that fits your organization's profile.

3. *Customize Your ZTSaaS Plan:* Based on the assessment, we'll help you choose the mix of Traditional and Optimal services that align with your security maturity and business objectives.

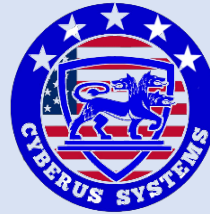4. *Implement and Thrive:* With our ongoing support, watch your

organization's security transform, building resilience against tomorrow's threats.

Your organization's security is paramount. Let Cyberus Systems be your ally in building a zero-trust environment.