

OXEN NETWORKED

FEBRUARY 2026
VOLUME 4 • ISSUE 3



Hot Topics in
Cybersecurity

INSIDE CONTENTS

- 3** SECURITY IN A MULTI-CLOUD ENVIRONMENT
- 4** THE CASE FOR EMAIL SECURITY
- 6** 2026 CYBERSECURITY REPORT
- 7** OXEN HONORED AT MSP TITANS OF THE INDUSTRY AWARDS





WESTERN IOWA - Harlan
Corporate Headquarters

CENTRAL IOWA - Ames

EASTERN NEBRASKA - Omaha

CENTRAL KANSAS - Wichita

SOUTHWEST MISSOURI - Joplin

Contact OXEN at hello@oxen.tech
Northern Region - Cori McKissick
cmckissick@oxen.tech
Southern Region - Kelle White
kwhite@oxen.tech

OXEN NETWORKED is a publication of OXEN Technology. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form, electronic, photocopying, recording, mechanical, or otherwise without the prior written permission of OXEN Technology. All rights are reserved.

EDITORIAL AND

CIRCULATION CONTACT:

Kelle White, VP of Sales & Marketing
316.500.2362, kwhite@oxen.tech

TRADEMARKS:

All brand names and product names used in this publication are trade names, service marks, trademarks, or registered trademarks of their respective owners.

ADDITIONAL ISSUES:

Extra issues are available to business customers on a limited basis while supplies last. Contact Kelle White at 316.500.2362.

POSTMASTER SEND CHANGES TO:

Kelle White, VP of Sales & Marketing
OXEN Technology
Wichita, KS 67209
kwhite@oxen.tech

Copyright © 2026 by OXEN Technology
and Cornerstone Publishing Group, Inc.



PRINTED ON RECYCLED PAPER

OXEN NETWORKED

Resolve to invest more in cybersecurity in 2026. The threat landscape is evolving quickly, and you'll need a new level of readiness in the new year. This February issue of OXEN NETWORKED provides guidance on how to move forward.

On page 3, we focus on **Security in a Multi-Cloud Environment**, with insights provided by Andrew Hartwig, Security Engineer. This article looks at both the flexibility advantages of a multi-cloud setup as well as its security challenges and how to address them.

We present **The Case for Email Security** on pages 4 and 5. Email remains the #1 attack vector for cybercriminals, and today's threats are more advanced, more targeted, and more costly than ever. You'll want to make sure your email security program is up to the task, and OXEN Technology is here to help.

Ryan Pieken, Sr. Consultant - CIO/CISO Services, shares his **2026 Cybersecurity Report** on pages 6 and 7. You'll find an overview of the mounting challenges ahead, along with strategic recommendations for cybersecurity steps you can take now.

OXEN Technology wants your organization to be successful in 2026 and for cybercriminals to fail in their attempts to disrupt your progress. When you take advantage of our resources and expertise, your defenses get stronger. Please contact us to discuss the details.



Sincerely,

Kelle White

Kelle White

Vice President, Sales
OXEN Technology



SECURITY IN A MULTI-CLOUD ENVIRONMENT

By Andrew Hartwig, Security Engineer



The appeal of multi-cloud lies in its flexibility – the ability to leverage the strengths of different cloud providers, avoid vendor lock-in, and optimize costs. However, this approach also introduces a new layer of complexity.

CHALLENGES AND STRATEGIES

One of the biggest challenges in multi-cloud security is the inconsistency of security controls. Each cloud provider (such as AWS, Azure, and Google Cloud) offers its own set of tools, configurations, and terminology. This makes it difficult to enforce uniform security policies across environments. Without a centralized framework, organizations risk gaps in coverage and increased threat exposure.

Identity and access management (IAM) is another area that becomes more complex in a multi-cloud setup. Managing user permissions across multiple platforms can lead to misconfigurations, over-privileged accounts, and potential security breaches. Implementing federated identity solutions like Entra ID, Duo, or Okta can help streamline access control and enforce least privilege principles across clouds.

Compliance and governance also add complexity. Cloud providers may store data in different geographic regions, which can complicate adherence to regulations like GDPR, HIPAA, or CCPA. Automating compliance checks using tools like AWS Config, Azure Policy, and Google Cloud Platform's Security Command Center can help ensure that policies are consistently enforced, and audits are easier to manage.

Data protection is paramount in any cloud environment, and in a multi-cloud setup, it's essential to maintain consistent encryption standards. Encrypting data both at rest and in transit, using customer-managed keys (CMKs), and rotating keys regularly are best practices that should be applied universally.

TOP SSO PROVIDERS FOR MULTI-CLOUD ENVIRONMENTS

Entra ID is tightly integrated with Microsoft 365 and Azure services. It supports hybrid environments, conditional access policies, and seamless integration with both on-premises Active Directory and Windows Hello. Entra ID is especially well-suited for enterprises already invested in the Microsoft ecosystem.

Duo, part of Cisco, provides a cloud-hosted SSO solution that supports both SAML 2.0 and OpenID Connect (OIDC) protocols. Duo adds phishing-resistant MFA, device trust checks, and adaptive access policies to cloud and on-premises applications. It integrates smoothly with existing identity providers like Active Directory, Google Workspace, and Okta, making it a flexible choice for organizations prioritizing security and ease of deployment. Duo's SSO also supports passwordless authentication and is a strong fit for regulated industries like health care, finance, and education.

Okta is a cloud-native identity platform known for its extensive integration network, supporting over 7,000 applications. It offers adaptive multi-factor authentication (MFA), passwordless options, and granular access policies based on user behavior, device health, and location. Okta's Universal Directory and lifecycle management features make it ideal for organizations seeking flexibility and scalability.



THE CASE FOR EMAIL SECURITY

Why protecting your inbox protects your entire business

By Kelle White - VP Sales

Cybersecurity attacks aren't usually loud or dramatic. In fact, most breaches start quietly with a single compromised email account. Email remains the #1 attack vector for cybercriminals, and today's threats are more advanced, more targeted, and more costly than ever.

That's why organizations can no longer rely on spam filters and hope for the best. True protection requires comprehensive email security, backed by multi-factor authentication and strong identity protection. You need to build all three into your cybersecurity strategy.

EMAIL IS THE NEW FRONT DOOR, AND ATTACKERS KNOW IT

More than 90% of successful cyberattacks begin with email. Criminals exploit inboxes because:

- Users trust email as a communication channel.
- Email systems touch nearly every part of the business.
- One compromised inbox often leads to full network compromise.
- Email is an easy gateway for social engineering.

Attacks today include:

- Business Email Compromise (BEC)
- Vendor impersonation

- Zero-day malware
- Ransomware delivered through attachments or links

MULTI-FACTOR AUTHENTICATION (MFA)

MFA is your first line of defense against account takeover. Why? MFA ensures that even if a criminal steals a password, they still can't get into the account. A second verification step creates a barrier that prevents unauthorized access.

Why MFA matters:

- Passwords are stolen or cracked daily.
- Phishing emails often aim specifically to steal credentials.
- Attackers reuse passwords across platforms.
- Stolen identities lead to long-term compromise.

By using MFA, your organization will reduce account takeover risk.

IDENTITY PROTECTION

Identity protection secures the person behind the password.

It includes:

- Identity Threat Detection & Response (ITDR)
- Monitoring user behavior for suspicious activity
- Impossible travel logins
- Unfamiliar devices
- Privilege escalation attempts
- Lateral movement indicators

Credential Protection:

- Ensuring credentials aren't leaked on the dark web
- Preventing reuse across systems
- Eliminating weak or shared passwords

In addition, role-based access controls give users only the access they truly need, and conditional access policies block risky logins or require extra verification when necessary.

WHAT A MODERN EMAIL SECURITY STRATEGY SHOULD INCLUDE

A true email security stack should address the full attack chain:

- Advanced Threat Protection
- Malware and ransomware scanning
- Impersonation and BEC detection
- Outbound email protection

- Data Loss Prevention (DLP)
- Robust MFA on all accounts
- Identity threat monitoring

Here's the bottom line: Email is the weapon, identity is the target, and MFA is the shield. If any one of these is weak, the whole system becomes vulnerable.

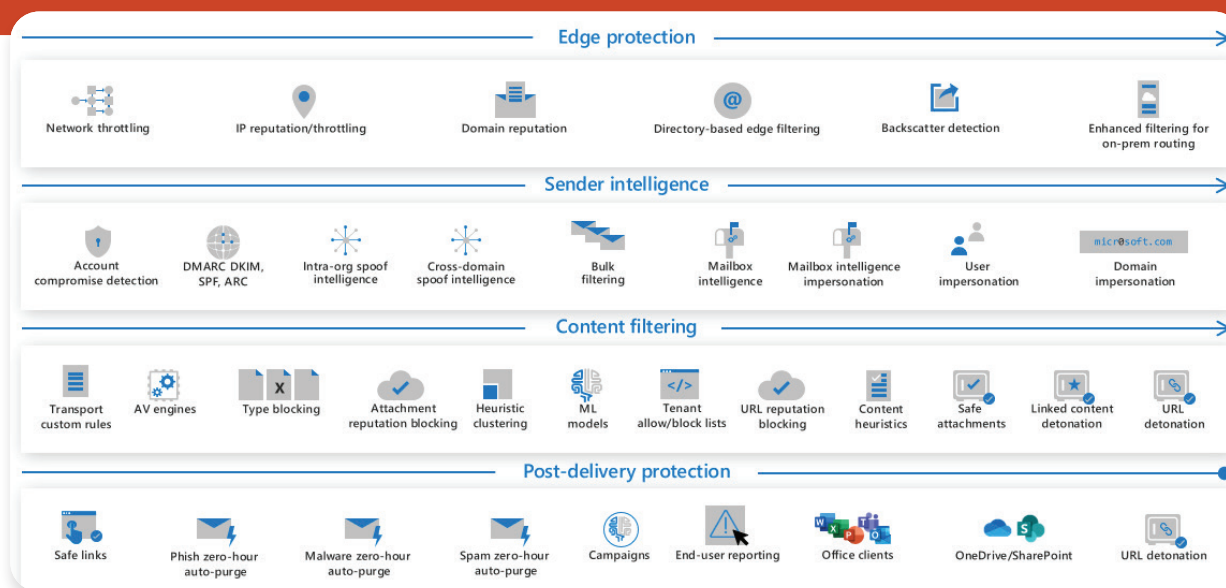
HOW OXEN TECHNOLOGY HELPS PROTECT YOU

We combine all three pillars into a layered security framework:

- Business Protection Security Stack
- Advanced Email Security Filtering
- EDR + 24/7 SOC Monitoring
- Identity Management + Conditional Access
- Dark Web Monitoring
- Security Awareness Training
- MFA Everywhere

Ready to strengthen your organization's security? OXEN Technology can assess your environment and build the right mix of email security, identity protection, and MFA. Your inbox shouldn't be your biggest vulnerability. Let's make it your strongest line of defense.

EMAIL SECURITY: PHASE 4 FILTERING



2026 CYBERSECURITY OUTLOOK

Strategic insights for organizational leaders



By Ryan Pieken
Sr. Consultant - CIO/CISO Services

Cyber threats are increasingly sophisticated and potentially destructive. Make sure your organization is well prepared to address the challenges in the coming year.

EXECUTIVE SUMMARY

As we approach 2026, the cybersecurity landscape is evolving at an unprecedented pace. Organizations operating in sectors such as banking and critical infrastructure face mounting challenges as the sophistication and frequency of cyber threats accelerate. Regulatory pressures continue to grow, demanding robust compliance and proactive risk management. This report provides an authoritative overview of key trends, practical frameworks, and strategic solutions – particularly focusing on the CIS framework and Microsoft cloud security tools – to empower organizational leaders in building resilient, compliant operations.

EVOLVING THREAT LANDSCAPE

Cyber threats are becoming more targeted and disruptive, with ransomware, supply chain attacks, and advanced persistent threats (APTs) topping the list of concerns for organizations. Sector-specific risks are especially acute for banking, where attacks targeting financial data and payment systems can have systemic consequences, and for critical infrastructure, where operational disruption can impact public safety and national security. Attackers are leveraging AI-driven techniques, exploiting cloud misconfigurations, and seeking out vulnerabilities in remote work environments.

CYBERSECURITY COMPLIANCE

Regulatory environments are tightening, driven by the need to protect sensitive data and maintain operational

continuity. In banking, compliance with frameworks such as FFIEC, GLBA, and PCI DSS is mandatory, requiring continuous monitoring, data encryption, and incident response capabilities. Critical infrastructure sectors must adhere to requirements outlined by NERC CIP, NIST, and other national standards, focusing on asset protection, threat detection, and resilience planning. Failure to comply not only risks penalties but also exposes organizations to reputational and operational harm.

THE CIS FRAMEWORK: BUILDING ROBUST SECURITY

The CIS Controls framework remains a practical guide for organizations seeking to strengthen their security posture. By prioritizing fundamental controls – including inventory management, vulnerability assessment, secure configuration, and access control – leaders can systematically address common attack vectors. Implementing CIS controls provides a defensible baseline for compliance, risk management, and continuous improvement. Practical steps for adoption include:

- Assessing current security maturity against CIS benchmarks
- Aligning control implementation with regulatory requirements
- Automating monitoring and reporting processes
- Establishing governance for ongoing review and adaptation

MICROSOFT CLOUD SECURITY SOLUTIONS

Microsoft offers a comprehensive suite of cloud security tools designed to address modern threats and compliance requirements. Key solutions include:

- **Microsoft Defender for Cloud:** Threat protection and security posture management across cloud workloads
- **Azure Sentinel:** Cloud-native SIEM for intelligent threat detection and incident response
- **Azure Active Directory:** Identity and access management with multi-factor authentication and conditional access
- **Microsoft Purview:** Data governance and compliance, supporting regulatory mandates in banking and critical infrastructure
- **Microsoft Intune:** Mobile device management and endpoint security for remote workforces

These solutions map directly to CIS controls and regulatory requirements, enabling organizations to automate compliance, detect threats early, and respond effectively.

STRATEGIC RECOMMENDATIONS

- Integrate CIS Controls into your security strategy for a scalable, compliance-ready foundation.
- Leverage Microsoft cloud security tools to automate detection, response, and reporting.
- Conduct regular risk assessments and pen tests focusing on sector-specific threats and regulatory changes.
- Invest in continuous training and awareness programs for all staff.
- Establish strong governance and incident response plans, tested through realistic exercises.
- Engage with OXEN trusted advisors to stay ahead of emerging threats and compliance developments.

THE PATH FORWARD

Cloud security and compliance are the twin pillars of effective cybersecurity in 2026. By embracing proven frameworks like CIS, implementing advanced cloud security solutions from Microsoft, and maintaining a vigilant approach to sector-specific risks, organizational leaders can position their organizations for sustainable success. The journey requires strategic investment, ongoing education, and a commitment to continuous improvement – but the rewards are measured in operational continuity, regulatory confidence, and stakeholder trust.

OXEN Technology is here to lead your organization forward on the cybersecurity journey. Please contact us at hello@oxen.tech or 888.296.3619, option 3.



OXEN HONORED AT MSP TITANS OF THE INDUSTRY AWARDS

OXEN Technology was honored at the prestigious MSP Titans of the Industry Awards, held on December 10, 2025, in Beverly Hills, California. Amidst a gathering of the nation's top technology leaders, OXEN Technology stood out as a finalist in the highly competitive Best MSSP (Managed Security Service Provider) category.

The MSP Titans of the Industry Awards, presented by MSP Success, are widely considered the ultimate recognition for Managed Service Providers. These awards are strictly merit-based and honor companies that demonstrate exceptional innovation, service excellence, and business growth.

Being named a finalist is a significant achievement. OXEN Technology was selected from hundreds of submissions nationwide, placing us in an elite group of "Titans" who are setting the standard for cybersecurity and IT management.

President Heather Lantz, representing OXEN's Operational Excellence team, attended the event to accept the recognition on behalf of our company.

"It is an honor to be a finalist and a part of such an elite group of other MSSPs," Lantz said. "This recognition validates our team's relentless dedication to keeping our clients secure. In the Best MSSP category, judges looked specifically for providers who go above and beyond to protect businesses from evolving cyber threats – a core mission at OXEN Technology."

STRONG AS AN OX



Strong on experience. Strong on knowledge. Strong on skills. If you want strong IT services, put our team to work for you. **To schedule a free consultation, visit www.oxen.tech/contact or call 888.296.3619.**

