Securing Your People, Applications & Infrastructure in the Cloud

Why Modern Businesses Must Adopt Zero Trust Security for the Cloud Era

Protecting Remote Employees, SaaS Applications, Cloud Infrastructure, and Business Data

Against Today's Most Advanced Cyber Threats

Tom Ruffolo

President/CISA at eSecurity Solutions

@2024 eSecurity Solutions. All Rights Reserved.

EXECUTIVE SUMMARY

Securing Your People, Applications & Infrastructure in the Cloud

Cloud adoption and remote work have fundamentally changed cybersecurity. With most business data, applications, and workloads now residing in the cloud, attackers increasingly target identities, cloud apps, and remote users rather than traditional corporate networks. SMBs are especially vulnerable due to limited resources and reliance on cloud services.

Key Security Challenges

Organizations face three primary areas of risk:

- **Remote Workers** – Phishing, credential theft, insecure home networks, and unauthorized data access.
- **Cloud Infrastructure** – Misconfigurations, compromised accounts, ransomware, and unmonitored cloud assets.
- **Cloud Applications & Data** – SaaS breaches, OAuth token theft, shadow IT, and excessive user privileges.

The leading causes of cloud breaches are compromised identities, phishing attacks, access control, and misconfiguration.

Why Traditional Security Falls Short

Legacy VPNs provide secure connectivity but often grant broad network access once a user is authenticated. This approach creates significant risk if credentials are stolen or a device is compromised.

- Today's cloud-first environment requires security that controls:
- Who can access company resources
- What resources they can access
- How data can be used and shared
- Continuous verification of users and devices

Recommended Security Strategy

Modern organizations should adopt a Zero Trust architecture supported by Secure Access Service Edge (SASE) technologies:

- Multi-Factor Authentication (MFA)
- Zero Trust Network Access (ZTNA)
- Cloud Access Security Broker (CASB)
- Secure Web Gateway (SWG)
- Firewall-as-a-Service (FWaaS)
- Endpoint Detection & Response (EDR)
- Managed Detection & Response (MDR)
- Cloud Security Posture Management (CSPM)

Conclusion

Effective cloud security is no longer about protecting a network perimeter. It is about protecting identities, applications, data, cloud workloads, and remote users wherever they operate. Organizations that implement Zero Trust and SASE-based security gain stronger protection against modern threats while improving visibility, compliance, and business resilience.

@2024 eSecurity Solutions. All Rights Reserved.

Table of Contents

Introduction to SASE **4**

The Three Security Pillars in Cloud Security & SASE 4

Overall Cloud Security Statistics 5

SMB Cloud Specific Statistics 5

Cloud Security Pillar #1: Remote Worker Security **6**

Remote Worker Cybersecurity Statistics 6

Top Cyber Threats to the Remote Workforce 7

Security Risks for Remote Workers 7

Recent Attack Methods Targeting Remote Workers 8

Necessary Security Solutions for Companies with Remote Workers 10

SASE security versus VPNs for Remote Worker Security 11

How eSecurity Solutions Can Help Secure Remote Workers 12

Cloud Security Pillar #2: Security for Public & Private Cloud Workloads **13**

Cloud Infrastructure Cybersecurity Statistics 13

Security Risks for Public & Private Cloud Workload 14

Security Threats for Private & Public Cloud Workload 14

The Growing Risk to Public and Private Cloud Workloads 14

Public and Private Cloud Attacks 15

Cloud Infrastructure Breach Causes, Risks and Vulnerabilities 16

Necessary Security Solutions for Public & Private Cloud Infrastructure 17

How eSecurity Solutions Can Help Secure Cloud Infrastructure 17

Cloud Security Pillar #3: Security for Cloud Applications & Data **18**

Cloud Application Security Statistics 18

Security Risks for Public & Private Cloud Workload 19

Why SMBs Are Increasingly Vulnerable to Cloud-Based Threats 19

Major Threats to Insecure Cloud Applications & Data 20

Recent Actual Cloud Application Attack Exploits 21

How eSecurity Solutions Can Help Secure Cloud Applications & Data 21

Necessary Security Solutions for Your Cloud Applications 22

@2024 eSecurity Solutions. All Rights Reserved.

eSecurity Solutions
Expert Security•Trusted Advice

Securing Your People, Applications & Infrastructure in the Cloud

Why Modern Businesses Must Adopt Zero Trust Security for the Cloud Era

Protecting Remote Employees, SaaS Apps, Cloud Infrastructure, and Cloud Data

The world has changed and it is time for all businesses to change their security to add protection for their remote cloud-based assets. This needs to include protection from and for remote employees, from cloud applications and data as well as cloud infrastructures stored in public and private clouds. In addition to key identity and network security this will need to include zero trust security using Secure Access Service Edge (SASE).

The Three Security Pillars in Cloud Security & SASE

Cloud security requires more than protecting a corporate network. As organizations adopt remote work, cloud applications, and public and private cloud platforms, security must focus on three critical and interconnected pillars:

Remote Workers

Protecting employees, devices, and access to corporate resources

Public/Private Cloud

Protecting cloud workloads, systems, and networks from unauthorized access

Cloud Applications

Protecting applications and sensitive data from theft, misuse, and exposure

Because these pillars are interconnected, organizations must adopt a unified Zero Trust security strategy that continuously verifies users, devices, applications, and workloads.

@2024 eSecurity Solutions. All Rights Reserved.

Overall Cloud Security Statistics

As cloud usage expands, organizations face increasing security challenges. The following statistics highlight the scale of cloud usage, the most common security risks, and the growing investment organizations are making to protect their cloud infrastructure, applications, and data.

Cloud Adoption
98%
of organizations worldwide now utilize cloud services

Remote Work Risk
61%
of reported data breaches are caused by remote workforces

Breach Exposure
82%
of all breaches involve public, private, or multi-cloud data

SaaS Challenges
75%
of organizations experienced a SaaS related incident

83%
of companies reported cloud security as a primary concern

80%
of organizations experienced a cloud-related security breach in the past year

51%
of companies plan to increase their cloud security investments this year

$1 Million
average cost savings for companies using zero trust

Compromised Identities
70%
of cloud breaches originate from compromised identities

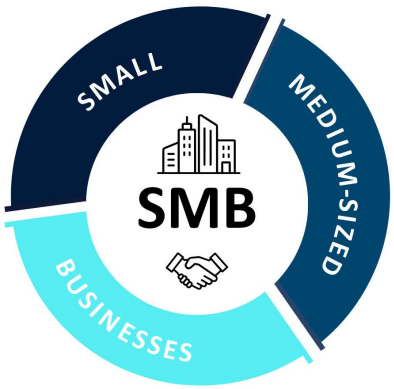
The Human Factor
73%
of organizations are affected by phishing attacks

Misconfiguration
23%
of all cloud security incidents are due to configuration error

Unmonitored Assets
32%
of cloud infrastructure sits idle and untracked

SMB Cloud Specific Statistics

Small businesses are not immune from the need for cloud security. Here are some facts that highlight the risks.



Targeted Rates
4x more
likely targeted for cloud attacks

Ransomware
82%
of ransomware attacks < 1,000 employee companies

Social Engineering
350% more
likely targeted in social engineering attacks

51%
of SMBs have no cybersecurity measures

20%
of SMBs have implemented MFA

47%
of SMBs have no privileged access control

@2024 eSecurity Solutions. All Rights Reserved.

Remote Worker Attacks & Vulnerabilities

Cloud Security Pillar #1

Remote workers add additional security risks that put your data and systems at risk. Yes, protecting the employees' remote environments is one goal, but the primary goal that companies must focus on is how to control access and usage of your data from remote workers. Where will that data end up if you don't?

Remote Worker Cybersecurity Statistics

Remote work offers flexibility and productivity benefits, but it also expands an organization's cyber risk. The following statistics highlight the increased security challenges associated with remote and hybrid work environments.

Mixing Home + Work Accounts

50%

of remote employees mix work and personal accounts increasing risk

Breach Likelihood

3x more

Remote workers are 3x more likely to accidentally expose corporate data

Insecure Home Infrastructure

50%

of IoT devices in home networks contain critical vulnerabilities

61%

of companies reported their remote workforce caused a data breach

58% ⬆

Increase in insider threats since widespread remote work adoption

Human error remains the leading cause of cloud security incidents, making remote work security a critical priority for every organization. As employees access company data across multiple devices, applications, and networks, even simple mistakes can create significant security risks.

@2024 eSecurity Solutions. All Rights Reserved.

Top Cyber Threats to the Remote Workforce

Remote employees are a common target for cybercriminals because they often work outside the protection of the traditional office environment. By exploiting human behavior through phishing, impersonation, and credential theft, attackers can often gain access to sensitive systems without needing to bypass advanced security controls. These are the most common security risks organizations face when supporting remote and hybrid work environments.

AI-Powered Impersonation

In 2025, 41% of SMB victims identified generative AI as the root cause of attacks. Cybercriminals use AI to mimic internal communications to trick employees into clicking malicious links or sharing sensitive information.

Credential-Based Phishing

Credential-based phishing attacks surged 703% in 2024, making them one of the fastest-growing threats to SMBs. These attacks use fake login pages and deceptive emails to steal usernames and passwords.

AI-Enhanced Phishing

Attackers are using generative AI to create hyper-personalized phishing campaigns that closely resemble legitimate corporate communications. This makes phishing emails more convincing and harder to identify.

Information Stealing Malware

Information-stealing malware (infostealers) became a leading driver of cyberattacks against SMBs, with detections increasing 104% year-over-year. Often through personal devices used for work, these programs steal credentials to access corporate networks.

Credential Data Leaks

In June 2025, a compilation of 16 billion leaked credentials emerged, largely sourced from infostealer infections on personal devices. These massive credential databases enable attackers to conduct credential-stuffing attacks against SMB remote access portals and cloud services.

Security Risks for Remote Workers

Remote work has expanded organizational flexibility, but it has also introduced new security challenges that are more difficult to manage outside the traditional corporate perimeter. Without proper controls, remote workers can unintentionally expose sensitive data and increase organizational risk.

- **Data Access Control**
- **Corporate Impersonation**
- **Corporate Data Loss**
- **Compromised Home Networks**
- **Uncontrolled Data Storage**

.

Because these pillars are interconnected, organizations must adopt a unified Zero Trust security strategy that continuously verifies users, devices, applications, and workloads.

@2024 eSecurity Solutions. All Rights Reserved.

Security Threats for Remote Workers

Remote employees are a common target for cybercriminals because they often work outside the protection of the traditional office environment. By exploiting human behavior through phishing, impersonation, and credential theft, attackers can often gain access to sensitive systems without needing to bypass advanced security controls. In 2025, 41% of SMB victims identified Gen AI as the root cause.

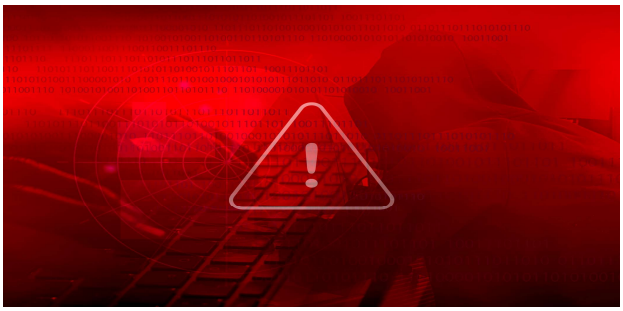
Employee Carelessness or Theft

Uncontrolled Access to Corporate Data

Lax Authentication Controls & Broad Permissions

Security Attacks on Home PC, Wi-Fi, or Networks

Insecure Communication with Corporate Infrastructure



Recent Attack Methods Targeting Remote Workers

Remote workers are a primary target for attackers seeking to infiltrate small and medium-sized businesses (SMBs), with **20% of organizations** reporting breaches directly caused by remote employees.

Remote Access Exploits

Small Law Firm Attack

Compromised RDP credentials enabled REvil ransomware deployment, with attackers threatening to release customer data.

BeyondTrust Remote Access Product Vulnerability

BeyondTrust's software was exploited to provide access to O/S commands allowing corporate date exfiltration.

Broad VPN access or Stolen Credentials

Broad VPN access or stolen credentials can give employees or **third parties unrestricted access to large portions of the corporate network**, exposing sensitive data and enabling unauthorized activities such as downloading, sharing, or storing data on remote devices or in the cloud.

Stolen Insider Provided Credentials Allowing Unfettered Remote Access

Credential Laundering

In a 2025 case, an individual was sentenced for helping a foreign operative use their credentials to log in and perform remote work for a Virginia-based government contractor, allowing an unauthorized actor full access to the company's internal programs.

Careless or Malicious Employees

Careless or malicious employees are often the cause of stolen or misused credentials. The results are the same: unfettered access to corporate data.

@2024 eSecurity Solutions. All Rights Reserved.

Infostealer Malware Attacks

The City of Mundelein Breach (Jan 2025)

The Medusa ransomware group gained access to the city's network, **stealing 118 GB of medical, health insurance, and financial data.** While the initial entry correlated with **stolen credentials found in infostealer logs.**

Pickett & Associates (Jan 2026)

This **small-to-medium engineering firm** was targeted by a threat actor known as Zestix/Sentap. The **attacker allegedly stole 77 GB of data following a compromise linked to infostealer credentials.**

AI-Enhanced Phishing & Social Engineering

North Korean Lazarus Group (2025)

Targeted European defense sector SMBs using a **social engineering campaign that sent fake job offers containing a Remote Access Trojan (RAT) to employees.**

Summary of Attack Causes & Vulnerabilities

Over-Reliance on VPNs

VPNs are an important security tool, but relying on them alone can create security gaps. Without granular access controls, strong authentication, and data protection policies, users may receive excessive access to corporate resources, increasing the risk of data exposure.

Insecure Home Networks & PCs

Remote workers often use devices and home networks that do not meet corporate security standards. Unsecured Wi-Fi, personal device usage, and malware infections can provide attackers with a path to access corporate systems and sensitive data.

Lack of Central Corporate Control of Pcs, Usage and Networks

Organizations often have limited visibility and control over remote devices, network connections, and user activity. Without centralized management and monitoring, security policies may be inconsistently enforced, creating opportunities for unauthorized access and data misuse.

Inadequate Cybersecurity Training

Employees remain a primary target for phishing, social engineering, and business email compromise attacks. Regular cybersecurity awareness training helps users recognize threats and reduce the likelihood of successful employee-driven security incidents.

Lack of Granular Data Access

Organizations must control who can access data, what actions they can perform, and where information can be stored or shared. Without Zero Trust principles and least-privilege access, sensitive data can be exposed to unnecessary risk.

Weak Authentication Controls

Organizations cannot adequately protect data if they cannot confidently verify user identities. Strong multi-factor authentication (MFA) should be required for all remote access to applications, infrastructure, and sensitive corporate resources.

@2024 eSecurity Solutions. All Rights Reserved.

Necessary Security Solutions for Companies with Remote Workers

Supporting a remote workforce requires security solutions that provide secure access, continuous protection, and centralized visibility across users, devices, networks, and applications. Together, these technologies form the foundation of a modern SASE-based security architecture.

Secure Access Service Edge (SASE)

Combines cloud-delivered networking and security services into a single framework that supports secure access from any location. It enables organizations to consistently protect users, applications, and data in the cloud regardless of where employees work.

Remote Security/ PC Security

Combines endpoint protection, secure access controls, network security, and cloud-based security services into a unified security strategy. This layered approach helps protect remote employees, devices, applications, and corporate data from evolving cyber threats.

Zero Trust Network Access

Delivers granular access controls, ensuring employees access only approved applications, data, and resources based on their specific roles.

Endpoint Detection & Response (EDR)

Protects employee devices by monitoring, detecting, and responding to malware, ransomware, and other advanced cyber threats in real time.

Firewall as a Service (FWaaS)

Provides cloud-based protection for remote users and locations, enforcing policies and blocking malicious or unauthorized network traffic.

Secure Web Gateway (SWGaaS)

Protects users from internet-borne threats by inspecting web traffic, blocking malicious content, and enforcing secure web access policies.

Cloud Access Security Broker (CASB)

Provides visibility and controls for cloud applications, helping protect sensitive data while securing access for remote and on-premises users.

Wi-Fi Network Security

Secures wireless network through strong encryption, authentication, and access controls, helping protect corporate data from breach.

Managed Detection & Response (MDR)

Global MDR Solution provides 24x7 monitoring, threat detection, investigation, and incident response across security and critical IT systems. This enables organizations to quickly identify, contain, and mitigate cyber threats before they impact business operations.

Multi-Factor Authentication (MFA)

Provides strong identity verification for all application and system access by requiring users to validate their identity through multiple authentication factors. This significantly reduces the risk of unauthorized access resulting from compromised or stolen credentials.

@2024 eSecurity Solutions. All Rights Reserved.

SASE security versus VPNs for Remote Worker Security

Feature	Typical VPN	SASE Solution
Security Offered	• Site-Site & Mobile secure tunnel • Traffic encrypted, Open to the Internet • Network-level access once authenticated.	• **Cloud Architecture Built on Zero Trust Platform** (**ZTNA**) – Granular access and usage of company data. Continuous verification of users and access • **FWaaS** – Cloud firewall protects home PC/network • **CASB** – Secure Cloud App./Data Protection • **Secure Web Gateway (SWG)** – Secure Web Access
Threats Mitigated	Mitigates eavesdropping and unauthorized modifications in data transit.	**Mitigates** • Data Exfiltration and lateral movement • Unauthorized Data Access & Usage • Unsafe Home PC & Networks • Unsafe Internet Access
Vulnerabilities Solved	Addresses insecure public Wi-Fi by encrypting data point to point	• Solves excessive implicit trust • Exposed IP addresses • Lack of Visibility
Access Control	Coarse-grained; often grants full network access to all resources.	**Granular** • Identity-based access to internal resources, but does not place them on the network, reducing lateral movement of threats • Least-privilege access limited to defined resources
Visibility	Limited; hard to track user activity outside the tunnel.	• Full Visibility • Centralized logging of all WAN traffic and cloud apps.
Infrastructure	• Perimeter-Based Design • Limited Scalability • Managed from VPN device • Relies on overall security • Data tunnel security	• Augments Perimeter-based Solutions • Highly Scalable Cloud Native design • Centrally based Network & security Mgt • Cloud delivered security, continuous monitoring • Integrated security stack for users and network
Overall ***Mitigates these Risks***	• Secure point-point data tunnel for secure access • Protects communication • Point-Point, Hub & Spoke • Secure Communication • Unauthorized Access	• Granular user Identity based security control for all corporate assets • Designed to protect distributed cloud assets • Scalable, cloud based • Data Exfiltration and lateral movement. • Unauthorized Data Access & Uncontrolled Usage • Unsafe Home PC & Networks • Unsafe Internet Access

@2024 eSecurity Solutions. All Rights Reserved.

Remote Worker Attack Summary

Attack Type	How Exploited	Attack Results
Remote Access Exploits	• Bugs in VPN solutions • Stolen or Lost Credentials • Employee Misuse of data	• Access to corporate Networks • Ransomware & Data Exfiltration • Data control is lost • 3rd parties pose as employees • CEO fraud caused financial loss • Employee data loss
Stolen Credentials	• Phishing, malware, careless employees, simple passwords…	
Infostealer Malware	• Malware designed to steal credentials. Websites phishing	
AI-Enhanced Phishing & Social Engineering	• Links in emails, Websites, weblinks, text messages, phone	

How eSecurity Solutions Can Help

Remote work creates new security challenges, but every business is different. eSecurity Solutions can help you identify the risks facing your remote workforce and recommend the right solutions to protect your users, data, and systems. Whether your priority is stronger access controls, better visibility, or improved protection against cyberattacks, we can help you find the right fit for your needs and budget.

Contact Us to Learn More
sales@esecuritysolutions.com

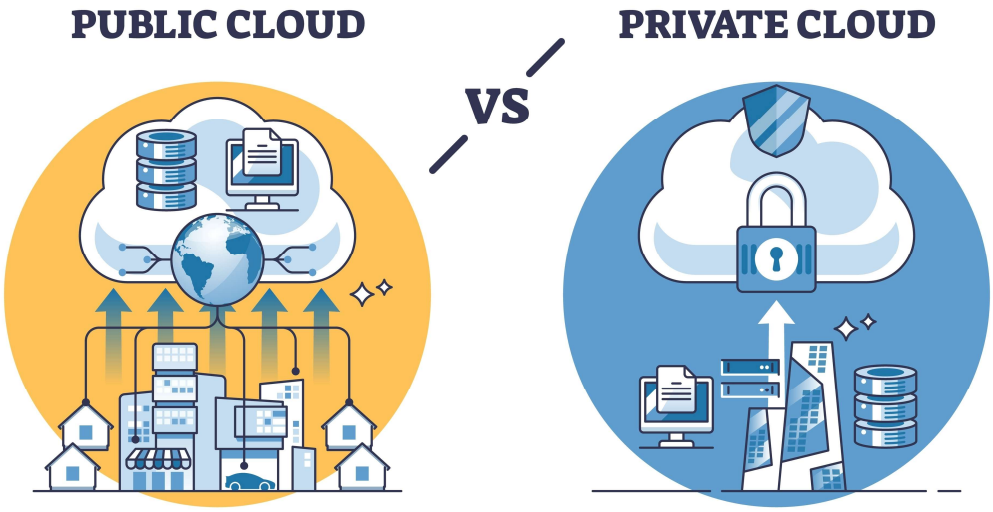
REQUEST A DEMO

GET A QUOTE

@2024 eSecurity Solutions. All Rights Reserved.

Security for Public & Private Cloud Workloads

Cloud Security Pillar #2



Moving to a public cloud introduces unique security challenges that differ from traditional on-premises environments. In 2025, over 80% of organizations reported at least one cloud security incident. Data and workloads in remote clouds present new security challenges and can only be addressed with cyber security that is designed for these environments.

Cloud Infrastructure Cybersecurity Statistics

Data Exposure

82%

of all data breaches involve data stored in the cloud (Public, Private, Multi-Cloud)

Public Cloud

27%

of data breaches are from data public cloud storage

API

31%

of cloud breaches are from insecure cloud interfaces

Compromised Identity

70%

of cloud breaches originate from compromised user identities

75% ⬆

In cloud environment intrusions in the past 3 years

Shadow Assets

32%

of cloud infrastructure sits unmonitored, carrying an average of 115 vulnerabilities

Cloud Misconfigurations

23-31%

of cloud incidents are due to misconfigurations

Phishing

73%

of businesses are subject to phishing breaches

Ransomware

78%

of companies encountered 1+ cloud-related ransomware attack in the past year

@2024 eSecurity Solutions. All Rights Reserved.

Security Risks for Public & Private Cloud Workload

As organizations increasingly host critical applications and data in private and public cloud environments, they face a range of security risks that can impact confidentiality, integrity, and operational resilience. A successful attack or misconfiguration can lead to significant business, financial, and reputational consequences.

Breached Servers & Workloads

Stolen or Destroyed Data

Loss of Control of Data

Our experts at eSecurity Solutions can help your company identify and implement the security controls needed to protect public and private cloud workloads.

Security Threats for Private & Public Cloud Workload

As cloud workloads expand, so do the security risks. The threats below highlight the most common vulnerabilities organizations face across private and public cloud environments.

Identity Attacks

Misconfigurations

Risk from Connected Apps

Public Cloud Environment Risks

Unprotected & Unmonitored Cloud Assets

.

These risks create security gaps that attackers can exploit, increasing the likelihood of data breaches, ransomware infections, and unauthorized access to critical cloud workloads.

The Growing Risk to Public and Private Cloud Workloads

As organizations expand their use of public and private cloud environments, the attack surface continues to grow. Sensitive data, applications, identities, and cloud resources must be protected against threats such as unauthorized access, misconfigurations, compromised accounts, ransomware, and shadow IT.

Without continuous visibility and consistent security controls, these risks can lead to data exposure, operational disruption, compliance violations, and significant financial and reputational damage.

@2024 eSecurity Solutions. All Rights Reserved.

Public and Private Cloud Attacks

(2023) During a decade-long misconfiguration **in Toyota's cloud environment** exposed data for 260,000 customers publicly from 2015 to 2023.

(2024) State-sponsored actors hacked **Microsoft's corporate systems** by exploiting a test account, highlighting risks in unmanaged cloud workloads.

(2024) Attackers stole credentials to breach over 160 organizations using the **Snowflake data platform,** exfiltrating massive volumes of customer data.

(2018) **Timehop's cloud environment** compromised 21 million users after social media access tokens from an unsecured account were stolen.

(2016) 57 million uber users were compromised through **Uber's AWS account** using credentials from a private GitHub repository.

(2019) 100 million Capital One customers were exposed from a **Capital One attack using Server-Side Request Forgery (SSRF)** to exploit a misconfigured WAF.

(2021) Ransomware attackers exposed thousands of **Kaseya's SMB customers** from a vulnerability in their remote management software's cloud hosted environment.

Key Takeaways from Recent Cloud Attacks

The cloud incidents above highlight several common security gaps that organizations must address to protect cloud workloads and data:

- **Compromised credentials** and identities remain one of the leading causes of cloud breaches.
- **Misconfigurations** can expose sensitive data and resources to unauthorized access.
- **Unmanaged or forgotten cloud assets** create opportunities for attackers to gain a foothold.
- **Third-party and supply chain risks** can extend vulnerabilities beyond an organization's direct control.
- **Lack of visibility and monitoring** can delay the detection and response to cloud threats.
- **Ransomware and data theft** continue to target cloud-hosted applications and data repositories.

Without a comprehensive cloud security strategy, organizations may struggle to protect critical cloud workloads.

@2024 eSecurity Solutions. All Rights Reserved.

Cloud Infrastructure Breach Causes, Risks and Vulnerabilities

Configuration & Management Errors

Configuration is the most pervasive risk, often with unsecured storage buckets (like Amazon S3 or Azure Blob) left open to the public, or improper firewall settings. 99% of cloud security failures will be due to customer-side errors in 2025.

Identity & Access Risks

Inadequate IAM

Weak IAM policies, like permissive user roles or failure to use the principle of least privilege, can lead to breach and privilege escalation.

Account Hijacking

Hackers can exploit administrative accounts through stolen credentials from phishing or brute force attacks.

Insider Threats

Current or former employees with legitimate access may intentionally or accidentally cause data breaches.

Technical Vulnerabilities

Insecure APIs

Poorly secured or unauthenticated APIs are direct entry points for attackers to extract data or disrupt cloud services.

Shared Infrastructure (Multi-Tenancy)

Failure to separate multiple tenants on the same physical hardware in public cloud infrastructure may allow one user access to another's data.

Supply Chain Attacks

Vulnerabilities in third-party library, software, or the cloud provider's vendors can compromise an entire ecosystem of users.

Operational & Compliance Risks

Lack of Visibility

Organizations often loose granular control and visibility into their network operations and data flows when moving to the cloud, making it harder to detect anomalies.

Compliance Violations

Operating across different global regions makes it difficult to maintain consistent compliance with strict regulations like GDPR, HIPAA, or PCI-DSS.

@2024 eSecurity Solutions. All Rights Reserved.

Necessary Security Solutions for Public & Private Cloud Infrastructure

Risk Category	Key Mitigation Strategy
Misconfigurations	Use **Cloud Security Posture Management (CSPM) tools** for automated cloud risk audits and compliance assessments.
Access Control	Enforce **Multi-Factor Authentication (MFA)** and Least Privilege Access.
Data Protection	Implement a **SASE (Secure Access Service Edge)** solution to provide granular access control to your cloud distributed data. Encrypt data as necessary.
Visibility	Use a global MDR solution to monitor, detect and respond to threats for your entire security and key IT infrastructure. CSPM solutions also provide visibility for all cloud environments
Network Protection	Use **Server specific endpoint detect and response protection** (EDR) to protect workloads, servers and data. Use **cloud firewalls** to provide secure networks.
Backup & Disaster Recovery	Use a robust backup and disaster recovery solution to backup all servers, workloads, data at all locations.

How eSecurity Solutions Can Help

Every cloud environment is unique, and securing it requires the right combination of technology, processes, and expertise. eSecurity Solutions helps organizations evaluate their cloud security risks and implement solutions that protect critical systems and data without adding unnecessary complexity. We work with you to build a security strategy that aligns with your business goals, compliance requirements, and budget.

Contact Us to Learn More
sales@esecuritysolutions.com

REQUEST A DEMO

GET A QUOTE

@2024 eSecurity Solutions. All Rights Reserved.

Securing Cloud Applications & Data

Cloud Security Pillar #3

Securing Business-Critical SaaS (Software as a Service) applications like Salesforce, ServiceNow, HubSpot, payroll, HR and financial apps is a unique challenge for SMBs because the security model shifts from protecting a network to protecting data access and configuration.

Cloud Application Security Statistics

Incident Frequency

75%

of organizations experienced a SaaS-related incident in the past year.

SaaS Applications

65%

of SaaS apps in use are unmanaged by IT (Shadow IT)

SMB Market Segment

16%

of SMB use cloud apps being the fastest target for credential theft

Salesforce CRM is

29.7%

of the cloud app market, contributing to misconfigurations in over 5 Salesforce components

Financial & Banking Apps

4x faster with AI

introducing AI-based attack vectors against consumers.

ITSM Service Now Market

85%

of fortune 500, but hold sensitive internal system credentials and employee PII

@2024 eSecurity Solutions. All Rights Reserved.

Security Risks for Public & Private Cloud Workload

As SMBs increasingly rely on cloud applications to support daily operations, securing these environments has become essential to business continuity and growth. Without proper security measures, a single cyber incident can have serious business consequences.

Failing to secure cloud environments can lead to devastating consequences for SMBs:

Financial Ruin

The average cost of a single breach for an SMB in 2025 is $140,000, with many businesses closing within six months of a major incident.

Reputation Damage

75% of consumers would sever ties with a brand following a cybersecurity issue.

Operational Downtime

Attacks can paralyze services, leading to lost revenue and eroded productivity

Legal & Compliance Penalties

Violations of regulations like HIPAA or GDPR can result in heavy fines.

Why SMBs Are Increasingly Vulnerable to Cloud-Based Threats

Cloud applications have become essential to small to medium-sized business operations, creating new opportunities for growth, collaboration, and efficiency.

Key challenges driving cloud security include:

- Expanding attack surfaces as more applications, users, and devices connect to cloud environments.
- Limited cybersecurity resources and expertise compared to larger enterprises.
- Increased reliance on third-party vendors, managed service providers, and interconnected cloud services.
- Greater volumes of sensitive business and customer data stored outside traditional network boundaries.

As a result, SMBs face a growing range of cloud-focused threats that can compromise data, disrupt operations, and impact business continuity.

@2024 eSecurity Solutions. All Rights Reserved.

Major Threats to Insecure Cloud Applications & Data

Cloud environments offer flexibility and efficiency, but they also introduce new security risks. As adoption grows, organizations face an expanding range of threats targeting applications, users, and sensitive data.

The primary threats targeting SMB cloud application infrastructure include:

Phishing & Social Engineering

SMB employees face **350% more** social engineering attacks than those at larger firms.

Ransomware & Multi-Extortion

Attackers encrypt cloud-hosted data and exfiltrate it first to threaten public exposure. **Ransomware accounts for 88% of SMB breaches.**

Business Email Compromise (BEC)

AI-enhanced impersonation of specific executives / vendors to trick employees into sensitive actions. This is often cited as the #1 financial threat to SMBs.

Insecure APIs

Poorly guarded "front doors" to cloud applications that allow attackers to bypass authentication and scrape sensitive data.

Supply Chain Attacks

Exploiting a trusted third-party cloud vendor or Managed Service Provider (MSP) to gain access to all its SMB clients simultaneously.

Cloud Hijacking

Unauthorized access to a business's cloud control, allowing attackers to steal data or use computing power for illicit activities like crypto mining.

These threats can have serious operational, financial, and reputational consequences. Understanding them is the first step toward strengthening cloud security and reducing risk.

@2024 eSecurity Solutions. All Rights Reserved.

Recent Actual Cloud Application Attack Exploits

(2025): Cybercriminals deployed **fake Microsoft OAuth applications** disguised as Adobe Acrobat, Adobe Drive, and DocuSign to gain access to Microsoft 365 accounts. Permissions enabled attackers to read emails, access files, and potentially deliver malware

(2025) Threat group UNC6040 impersonated internal IT staff in a **vishing attack** to convince employees at 20 organizations to install tampered versions of **Salesforce's Data Loader**, granting access to sensitive CRM data.

(2024) A Japanese game developer, made a simple Google Drive misconfiguration exposing nearly 1 million individuals for over 6 years. Files created, stored, and shared between 2017-2023 became accessible to anyone with a URL link. 935,779 individuals were exposed.

(2025): Compromised OAuth tokens allowed attackers to bypass authentication for 700+ organizations.

(2025): A supply chain breach through a **Salesforce connector** impacted a large list of customers. Attackers abused compromised **OAuth tokens from Gainsight-published applications** connected to customer Salesforce environments.

(2025) an infostealer infection on an employee's personal computer led to stolen Slack credentials and unauthorized access to **Nikkei's Slack workspace**, potentially exposing sensitive discussions and shared files involving more than 17,000 employees and partners.

(2024): Hackers breached production systems for its **Dropbox Sign eSignature platform** via a configuration tool. Hackers gained access to authentication tokens, MFA keys, hashed passwords, and customer information.

How eSecurity Solutions Can Help

Cloud applications are essential to running a modern business, but they can also create new opportunities for cyber criminals. eSecurity Solutions helps organizations secure their cloud applications and sensitive data by identifying risks, strengthening access controls, and recommending the right security solutions for their environment. Let's discuss the right cloud security strategy for your organization.

Contact Us to Learn More
sales@esecuritysolutions.com

REQUEST A DEMO

GET A QUOTE

@2024 eSecurity Solutions. All Rights Reserved.

Necessary Security Solutions for Your Cloud Applications

Risk Category	Key Mitigation Strategy
Zero Trust Network Access (ZTNA)	Implement a "never trust, always verify" framework for all users and devices. ZTNA grants application access case-by-case after verifying user identity and context, instead of giving broad network access like a legacy VPN access assumes zero trust. Can provide control over access and usage to data.
Secure Web Gateway (SWG)	Filters internet traffic to block web-based malware and enforce acceptable use policies.
Cloud Access Security Broker (CASB)	Monitors and controls the use of SaaS and cloud services, giving visibility into shadow IT and enforcing data protection policies.
Data Loss Prevention (DLP)	Prevents sensitive data from leaving the organization without authorization.
Software-Defined WAN (SD-WAN):	Optimizes and secures connectivity for branch offices and remote sites, with intelligent routing and integrated security checks.
Strong Endpoint (EDR) Solutions	Strong endpoint security to stop credential stealing or other malware that facilitates unapproved cloud application or data access or usage.
Multi-Factor Authentication (MFA)	Enforce MFA across all remote access points, including email and cloud portals.
Principle of Least Privilege (PoLP)	Limit user access rights to only what is strictly necessary for their role.
Continuous Employee Training	Regular awareness programs to help staff recognize AI-driven phishing and social engineering.
Recoverable Backups	Maintain encrypted, offline backups to ensure recovery after ransomware attacks.
Security Monitoring	Managed Detection and Response from a global MDR solution can be your early warning system and last line of defense if attacks get past your traditional security.

@2024 eSecurity Solutions. All Rights Reserved.