Kaseya 365 USER

MODERN USER PROTECTION BUYER'S GUIDE

eBook

People are both an organization's greatest asset and the most vulnerable link in the cybersecurity chain. According to Verizon's 2024 Data Breach Investigations Report, a non-malicious human factor was involved in nearly 70% of security breaches.[1] With the human factor now the most targeted and exploited entry point for malicious actors, robust, people-focused defense mechanisms are critical for end-user security.

The unprecedented rise in remote/hybrid work and increasing reliance on cloud-based applications have expanded the attack surface like never before, exposing your users to sophisticated threats, such as phishing, ransomware and business email compromise (BEC).

While critical for productivity and collaboration, Software-as-a-Service (SaaS) applications introduce unique vulnerabilities, such as unauthorized access, data leakage and misconfigurations. Meanwhile, dark web markets are teeming with stolen credentials and sensitive data, heightening the urgency of protecting user identities.

Security breaches of any magnitude can have far-reaching consequences, extending well beyond data loss or business disruptions. They can result in heavy financial losses, reputational damage, regulatory penalties, customer dissatisfaction and more.

Therefore, a truly effective end-user protection solution must be multifaceted, empowering you to tackle user-related risks efficiently.

Our Modern User Protection Buyer's Guide is designed to help simplify the process of selecting the right end-user protection solution for your business. This guide will help you identify the key features to look for in a security solution that will enable you to prevent, respond and recover from threats targeting users.

Prevention — Safeguard users from emerging threats

In an era where cyberthreats are evolving rapidly, protecting your end users requires proactive and adaptable defenses. You must implement preventive security measures that not only block malicious attacks from reaching end users but also build awareness and resilience among them.

Key considerations for preventive solutions:

- Anti-phishing solutions are critical for blocking email-based attacks before they reach users' inboxes. They drastically reduce the risk of users accidentally clicking on malicious links or downloading malware-infected attachments.
- Security awareness training can improve vigilance by helping users recognize suspicious activities and avoid common pitfalls, such as phishing or social engineering schemes.
- User susceptibility testing helps to assess and address risky user behaviors proactively. Simulated attacks and assessments reveal user vulnerabilities, enabling targeted education in areas prone to errors.
- Dark web monitoring solutions are vital for the early detection of compromised credentials. They enable your IT team to take swift action if user information is exposed.

Features to look for:

- Many phishing simulation solutions struggle with tedious whitelisting requirements and ensuring guaranteed simulation delivery. Look for security solutions with integrated anti-phishing and security awareness training to streamline the delivery of phishing simulations. Boost your team's efficiency and productivity by removing tedious, busy work and ensuring the end-user properly receives the phishing simulation.
- Your end-user security solution should have built-in email protection that filters and flags potentially harmful messages, catching suspicious content before it hits your users' inboxes.
- Your solution should allow easy deployment of user training programs across the organization, enabling consistent training with minimal disruption to daily operations.
- It is important that your solution has robust reporting capabilities to monitor user improvements and vulnerability trends. This helps to identify improvement areas and adapt training strategies based on actual data.

Response — Rapid action when a threat is detected

Every minute counts when dealing with cybersecurity incidents. When a threat is detected, rapid response capabilities are critical to preventing damage and protecting user accounts and data without delay. A comprehensive response strategy paired with the right tools enables you to take immediate action to address potential breaches.

Key considerations for responding to user threats

- Effective SaaS management ensures that user permissions and access levels are tightly controlled, reducing the risk of unauthorized access and preventing compromised accounts from further exploiting sensitive applications.
- Advanced security solutions with real-time alerting capability help notify IT teams when unusual or potentially harmful activity is detected, allowing for quicker assessments and responses to mitigate threats.
- Modern solutions equipped with automated mechanisms that lock accounts when suspicious behavior is detected prevent attackers from further exploiting compromised credentials.

Features to look for:

- Choose a security solution that offers centralized management for all user accounts across multiple SaaS platforms. This unified approach improves efficiency by enabling IT teams to monitor, update and manage user accounts from a single interface and reduces the risk of overlooked vulnerabilities across platforms.
- Your user security solution should have a real-time alerting feature that keeps IT teams informed of suspicious activities as they occur, enabling them to take immediate action to contain potential risks before they escalate into major issues.
- Opt for a robust solution with flexible automation that can initiate pre-approved remediation actions. This feature is critical to respond to threats swiftly by executing predefined actions, such as account locking, without manual intervention.

Recovery — Ensure business continuity and data integrity

In today's always-on business landscape where downtime and data loss can severely disrupt operations, the ability to quickly recover from a disaster is crucial.

Key considerations for recovery solutions:

- Leverage advanced backup solutions for essential SaaS applications, such as Google Workspace or Microsoft 365, to ensure your mission-critical data can be quickly retrieved and restored in the event of a disaster.
- Backup solutions with seamless recovery processes are critical to reducing downtime and ensuring business continuity. They allow you to resume business operations without extended interruptions, preventing productivity loss.
- Your recovery solution should align with data protection laws and industry standards to ensure compliance with regulations and minimize legal risks.

Features to look for:

- Look for an advanced backup and recovery solution that offers automated SaaS backups and easy data recovery. Automated backups simplify data protection efforts, reducing the chance of errors and freeing up IT time. Quick recovery minimizes data loss and downtime, providing peace of mind and operational resilience.
- Your recovery solution should allow you to configure the frequency of backups to suit your business's needs. Flexible backup scheduling ensures your critical data is always current and readily accessible.
- Detailed backup reports verify your backups are up to date and operational, enabling your IT team to proactively address issues before they impact recovery efforts. Opt for a recovery solution with powerful reporting capabilities to confirm backup health and readiness.

Building a holistic user protection strategy

A comprehensive user protection strategy is crucial in today's unpredictable threat landscape, where safeguarding users requires prevention, rapid response and seamless recovery. A holistic approach to user protection ensures your business can not only identify and block potential threats but also respond to and recover from unexpected cyber incidents efficiently. Choosing a reliable solution that addresses these multiple layers of protection is key to building resilience and minimizing security risks.

Questions to ask before choosing a user protection solution:

Does it provide visibility into user-related risks and incidents?

The ideal user protection solution should offer clear insights into user activities, threats and vulnerabilities, enabling your IT team to identify and respond to issues promptly. Having clear visibility into user-related risks and incidents is critical for understanding patterns, anticipating risks and making informed decisions to improve user security.

Is the solution scalable for future business needs and growth?

Your security solution should be able to grow with your business to support additional users, data and applications. A scalable solution helps avoid costly upgrades and ensures reliable security as your business grows.

Can it integrate smoothly with your existing SaaS tools and workflows?

Your security solution should effortlessly integrate with the SaaS applications you are subscribed to so you can detect and respond to SaaS-related security threats efficiently. Seamless integration with your current SaaS tools and processes is vital for maximizing efficiency and minimizing disruption.

Does it support both prevention and response measures efficiently?

A robust solution should support both proactive and reactive measures to address user-related security challenges effectively. It must offer the tools to prevent disruptive incidents while providing rapid response capabilities when threats are detected.

Introducing Kaseya 365 User
Comprehensive user protection beyond the endpoint

With the digital landscape becoming increasingly interconnected and end users accessing sensitive data across diverse cloud platforms, applications and devices, **your end-user protection strategy must extend beyond endpoint security.**

Kaseya 365 User brings together key elements for a modern, user-focused security approach. Our solution is designed to strengthen security at every stage, empowering you to prevent attacks, respond to incidents effectively and recover quickly to maintain business continuity and data integrity. Kaseya 365 User focuses on protection beyond the endpoint, allowing you to comprehensively protect end users, data and workflows without breaking a sweat.

Prevention

Kaseya 365 User's prevention tools are designed to take a proactive stance against threats, identifying and mitigating risks before they escalate. By equipping your organization with tools that fortify defenses at every level, Kaseya 365 User works to reduce susceptibility to common attack vectors, like phishing and credential theft, and improve user awareness and responsiveness to potential threats. These tools not only defend against immediate threats but also strengthen long-term security by identifying high-risk behaviors and enforcing cybersecurity best practices across the board.

Anti-phishing: AI-powered phishing defense blocks malicious emails in Google Workspace and Microsoft 365 before they reach your end users, reducing exposure to potential threats.

User awareness training: Delivers comprehensive training programs to educate users on cybersecurity best practices, enhancing their vigilance.

User susceptibility testing: Conducts phishing simulation exercises and identifies high-risk behaviors, enabling targeted training to solidify secure habits.

Dark web monitoring: Detects compromised credentials early, allowing for immediate action to prevent unauthorized access to sensitive data.

Response

Kaseya 365 User boasts cloud detection and response (CDR) that enables swift response to SaaS threats, reducing potential damage and securing at-risk accounts. These features are designed to handle incidents without the need for extensive manual intervention so your team can focus on other priorities. Advanced tools like SaaS event alerting and automated threat response utilize machine learning to identify suspicious patterns and secure compromised accounts quickly. Kaseya 365 User's automation empowers organizations to manage security events with minimal downtime and maximum efficiency.

SaaS application management: Provides oversight of SaaS application activity, ensuring fast action when suspicious activity is detected.

SaaS event alerting: Delivers alerts and immediate remediation steps in response to malicious activity, with automated actions to secure accounts instantly.

Automated threat response: Leverages machine learning for pattern detection and can lock compromised accounts in seconds, granting valuable time to mitigate threats effectively.

Recovery

Ensuring continuity and resilience is essential to minimizing the impact of any cyber incident on users and your organization. Kaseya 365 User's recovery tools provide robust options to secure and restore SaaS data following an incident, minimizing business disruptions and keeping operations on track. By offering advanced backup automation and versatile recovery methods, such as point-in-time, granular and non-destructive restore options, Kaseya 365 User ensures data can be quickly restored with minimal or no data loss. This recovery layer provides peace of mind that, even in the face of an incident, essential information is protected, and business can continue.

Automated SaaS backups: Creates automated, point-in-time backups across Microsoft 365 and Google Workspace, ensuring a full capture of relevant data changes.

Independent backup copy: Maintains a secure, independent backup copy outside SaaS provider servers, adding an extra layer of protection.

Flexible restore options: Offers point-in-time, granular and non-destructive restore options, allowing quick data recovery to resume operations with minimal downtime.

Why Kaseya 365 User?

Here are three key reasons why Kaseya 365 User can be a game changer for your business:

- Kaseya 365 User provides integrated user protection without needing multiple standalone products. A Kaseya 365 User subscription provides all the essential tools to protect and preserve the critical data and identities of SaaS users in Microsoft 365 and Google Workspace environments. With seamlessly integrated components, Kaseya 365 User works proactively to prevent, respond to and recover from user threats.
- By addressing prevention, response and recovery with a single, integrated solution, Kaseya 365 User simplifies security management, making it easier to maintain strong defenses across all stages of user protection.
- Kaseya 365 User extends security beyond the endpoint, safeguarding the most valuable part of any business: its people. It combines essential components for core IT and security functions, delivering unified tools for threat prevention, detection, response and recovery in a single consolidated platform. Kaseya 365 User is thoughtfully designed to protect your end users, their identities, data, privacy and work.

Discover how Kaseya 365 User can help you prevent, respond to and recover from any threat your users face effortlessly and cost-effectively.

LEARN MORE

[1] https://www.verizon.com/business/resources/reports/dbir/

Kaseya 365 USER