Kaseya 365 USER

KASEYA 365 USER BUSINESS CASE

REDEFINING USER PROTECTION FOR THE MODERN WORKFORCE

eBook

The hybrid work model and increasing reliance on Software-as-a-Service (SaaS) applications are reshaping the cybersecurity landscape. Although hybrid work and SaaS apps offer multiple benefits, they also introduce new cybersecurity challenges. With end users accessing sensitive business information from various devices and locations — from outside the secure perimeter of an organization's network — the attack surface continues to expand, providing cybercriminals with more opportunities to exploit vulnerabilities.

Cyberthreats, such as phishing, ransomware, account takeover (ATO) and business email compromise (BEC), are rapidly evolving and becoming more complex and prevalent. In 2023, the FBI reported 21,489 BEC complaints, resulting in losses exceeding $2.9 billion.[1] According to the Kaseya Cybersecurity Survey Report 2024, phishing continues to be a leading threat, affecting 50% of businesses in the past 12 months.[2]

When a cyberattack, such as phishing, occurs — and it's a matter of when, not if — your organization must be equipped to detect, respond and recover quickly. Without proactive measures, a single compromised user can jeopardize the entire system with cascading threats. The Kaseya Cybersecurity Report also revealed that human error accounts for over 35% of cybersecurity incidents, emphasizing the critical need for end-user protection.

This is where Kaseya 365 User, a ground-breaking subscription, steps in as a comprehensive solution. In this eBook, we will explore the perils of leaving your users unprotected and how Kaseya 365 User can help bolster user protection against evolving threats while saving you significant time, effort and costs.

The cost and danger of not protecting users

Stolen credentials and compromised logins aren't just theoretical; they are real-world risks that can have devastating consequences. The harsh truth is that many of these credentials are already circulating on the dark web, readily available to cybercriminals looking to exploit vulnerable systems.

Did you know the average requested transfer in a BEC attack is $84,059?[3] However, the impact of user-related breaches extends beyond financial losses. Apart from direct costs, including the expense of mitigating breaches, indirect costs, such as downtime, lost productivity, tarnished reputation, diminished customer trust and regulatory penalties, amplify the damage further. Reputational harm can linger for years, eroding relationships with clients and partners who lose confidence in your organization's ability to safeguard sensitive information.

Here are some examples of businesses facing data loss incidents or falling victim to cyberattacks where end users played a direct or indirect role.

Threat actors exploited Windows Quick Assist through social engineering

In April 2024, cybercriminals exploited Windows Quick Assist, a remote support tool, using social engineering tactics.[4] The attackers, known as Storm-1811, impersonated IT support staff to deceive victims into granting device access through vishing (voice phishing). After gaining entry, they deployed malicious software, including Black Basta ransomware. This allowed them to take control of the victim's device, move laterally across networks, steal sensitive data and carry out additional malicious actions.

DarkBeam data breach: 3.8 billion records exposed

In September 2023, an unprotected interface led to a significant data breach at U.S.-based cybersecurity firm DarkBeam, exposing over 3.8 billion records.[5] The breach occurred due to an unprotected Elasticsearch and Kibana interface, allowing cybercriminals to access sensitive data. This included email and password combinations, names, phone numbers and other personal details. DarkBeam attributed the attack to a cybercriminal group known as "DarkSide," which exploited the interface vulnerability to steal the data.

The 2024 Data Breach Investigations Report revealed that almost 70% of security incidents were tied to non-malicious human factors, including errors and falling victim to social engineering tactics.[6] Ignoring the risks of not protecting your end users could prove to be a costly gamble. Your business must adopt proactive strategies that go beyond traditional security measures to overcome the challenges posed by modern threats.

Introducing Kaseya 365 User
Comprehensive user protection beyond the endpoint

Kaseya 365 User is a revolutionary subscription designed to maximize user protection while minimizing complexity and costs. Built with a modern, user-first approach, it seamlessly integrates multiple layers of protection into a single solution, enabling you to prevent attacks, respond swiftly to incidents and recover effortlessly from user-based threats.

This innovative solution covers every aspect of user security, extending protection beyond endpoints to secure users and data. What sets Kaseya 365 User apart is its flawless integration, eliminating the need for multiple standalone tools. Each component works in harmony, streamlining security management and maximizing IT efficiency and productivity. The Kaseya 365 User solution gives you access to essential security tools to preserve critical data and identities, ensuring business resilience in the face of inevitable cyberthreats.

Key components of Kaseya 365 User

Listed below are the key components of Kaseya 365 User and the impact they have on businesses.

Prevention

With cyberthreats rapidly evolving and becoming more sophisticated, safeguarding end users demands proactive and flexible defenses. Kaseya 365 User proactively identifies and neutralizes threats, reducing risks from phishing and credential theft. Its cutting-edge solutions enhance user awareness, address high-risk behaviors and enforce cybersecurity best practices, strengthening defenses at every level while improving long-term security.

Graphus: This AI-powered solution defends against phishing, BEC, malware and ransomware by intercepting threats before they reach your employees. Malicious emails are quarantined automatically, reducing exposure to potential threats and minimizing IT workload.

"We were impressed by the AI feature set. And what really sparked it is the AI learning — how Graphus learns about the communication between internal email users and how it's capable of detecting that a message really didn't come into our mail system from inside the network."

— Luis Figueroa, General Manager of EC Group

Dark Web ID: The industry-leading dark web monitoring solution protects your organization by detecting stolen credentials and personally identifiable information (PII) on the dark web via 24/7/365 human and machine-powered monitoring. It helps protect against data breaches and cyber fraud with real-time alerts, enabling you to act swiftly to prevent unauthorized access to sensitive data.

"The proactive approach to threat detection that Dark Web ID provides is one of its biggest benefits. We can keep ahead of possible attacks by constantly scanning the dark web for credentials that have been compromised. The real-time alerts are very helpful as they allow for quick incident response. Dark web ID assists in quantifying the disclosure of sensitive data which enables us to efficiently prioritize mitigation efforts."

— Luis Figueroa, General Manager of EC Group

BullPhish ID: This security awareness training and phishing simulation solution equips your users with essential cybersecurity skills. Through engaging training programs and realistic phishing simulations, it improves vigilance and identifies high-risk behaviors for targeted improvement. It reduces the chances of human error, instills secure habits and enables your team to confidently defend against cyberthreats while complying with industry regulations.

"In the first quarter, before training, we had 77 people click a bad link, and 30 people submit personal information. After training, by the third quarter, 11 people clicked a bad link, and nobody submitted personal information."

— John Masci, System Administrator, Canisius High School

Response

During a cyberattack or a data disaster incident, rapid response is key to mitigating the damage and securing user accounts. Kaseya 365 User's advanced security solution enables you to respond to threats quickly and efficiently, reducing downtime while freeing your IT team to focus on other priorities.

SaaS Alerts: The cloud detection and response platform uses advanced machine learning to detect suspicious activity, alerts IT teams when potential threats are detected and provides automatic remediation. Equipped with robust features like cloud detection, SaaS event monitoring and instant account locking, SaaS Alerts streamlines incident management. It provides full visibility into cloud activities and protects compromised accounts within seconds.

"In our first month after deploying, we caught 15 account compromises, allowing us to respond and remediate before suffering any negative impacts."

— Buddy Pitt, Logically

Recovery

In an era where organizations operate 24/7/365, downtime is not an option. The ability to quickly recover from a disruptive incident is critical to ensuring business continuity and data integrity. Kaseya 365 User gives you access to an advanced SaaS backup solution that seamlessly restores business-critical SaaS data following an incident, minimizing business disruptions.

SaaS Backup: Kaseya 365 User provides SaaS backup options like Spanning or Backupify. Our cutting-edge SaaS backup solutions automate point-in-time backups for Microsoft 365 and Google Workspace, ensuring rapid recovery of lost or damaged data. With granular, non-destructive restore options, it minimizes downtime while maintaining compliance. These solutions secure independent backups outside SaaS servers, providing an extra layer of protection.

"Every time I check, the backup is going perfectly. The data is always 100% backed up."

— Dave Medicott, Senior Manager, Dell EMC

Quantifying the business value of Kaseya 365 User

Kaseya 365 User is more than a security solution; it's a purpose-driven, strategically developed subscription that maximizes the value of your investment by enhancing efficiency, reducing costs and helping you achieve and maintain compliance. The innovative solution brings together powerful security and data protection solutions, enabling businesses like yours to stay ahead in an increasingly complex cybersecurity landscape.

Reduce IT time and effort

According to the IBM Cost of a Data Breach Report 2024, breaches caused by stolen or compromised credentials took the longest to detect and resolve, averaging 292 days.[7] Phishing-related downtime affects 33% of businesses for two or more days.[8] Kaseya 365 User's suite of automated tools and streamlined processes significantly reduces the time required to identify and address security incidents. By automating threat detection, response and backups, your organization can free up valuable IT resources to focus on strategic priorities rather than grappling with downtime or manually resolving issues during crises.

Build resilience and stay compliant

Non-compliance with the Health Insurance Portability and Accountability Act (HIPAA) can result in fines of up to $250,000 and imprisonment for up to 10 years.[9] Similarly, violating the General Data Protection Regulation (GDPR) may lead to fines of up to €20 million or 4% of the previous year's global turnover, whichever is higher.[10]

For industries operating under strict regulatory requirements, such as healthcare (HIPAA) or those in Europe bound by GDPR, Kaseya 365 User offers additional compliance benefits. Our SaaS backup solution meets a wide range of compliance standards, including SSAE16, HIPAA and GDPR. It combines comprehensive protection, backup automation, flexible recovery options and multilayered security, ensuring your data is secure and compliant. Our solution also comes equipped with intrusion detection and data encryption for maximum security.

Achieve significant cost savings

The IBM Cost of a Data Breach Report 2024 also found that employee training reduced the average breach cost by $232,867. BullPhish ID, one of the key components of Kaseya 365 User, enables end users to build a strong defense against phishing scams and social engineering attacks through security awareness training and phishing simulation.

Additionally, Kaseya 365 User proactively mitigates risks, such as phishing attacks, credential theft and ransomware, minimizing the financial burden of breach recovery, downtime and lost productivity. Preventing security incidents not only reduces immediate costs but also protects your business against long-term reputational damage and customer churn.

Qualify for cybersecurity insurance

According to the IBM Cost of a Data Breach 2024 report, the average cost of a data breach reached $4.88 million, while the cost of a ransomware attack averaged $4.91 million. With cyberattacks becoming more pervasive, a cyber liability policy is no longer a good-to-have but a must-have for businesses of all sizes. However, cyber liability insurance is increasingly expensive, complex and more difficult to obtain than ever before. That's where Kaseya 365 User is a lifesaver for your business.

Organizations using Kaseya 365 Endpoint Pro and Kaseya 365 User gain comprehensive security and easy access to the Cyber Insurance Fast Track program — a first-of-its-kind offering that provides pre-qualified cyber liability coverage for businesses below market rates.

The Kaseya 365 User advantage

Kaseya 365 User offers a comprehensive suite of tools designed to address modern cybersecurity challenges while delivering exceptional value. Here's what sets it apart:

Ease of use

Gain centralized visibility into user activities across critical SaaS platforms like Microsoft 365 and Google Workspace. Kaseya 365 User simplifies monitoring by providing real-time alerts for suspicious behavior, policy violations and potential vulnerabilities. This streamlined approach enables IT teams to quickly identify and address risks, enhancing security posture and minimizing blind spots across your SaaS environment.

Comprehensive user protection

A single subscription protects every aspect of your business' users — valuable data, SaaS applications and email inboxes. Kaseya 365 User offers all the essential user security and data protection solutions in one platform, removing the need for multiple standalone tools and reducing costs and complexity. Kaseya 365 User enhances organizational resilience by offering a layered, proactive approach that addresses prevention, response and recovery.

Powerful automation

Boost IT efficiency and productivity while minimizing errors by automating critical tasks, such as threat detection, data backups and mitigation. IT teams are instantly notified of harmful activities, enabling them to act quickly to contain threats. Powerful automation, driven by machine learning, identifies suspicious patterns, secures compromised accounts and consistently backs up your data for complete peace of mind.

Scalability

As your business grows, your users, data and applications will also grow. Kaseya 365 User is designed to evolve alongside your business, seamlessly accommodating your business needs. With its flexible, subscription-based model, it's perfectly suited for organizations of any size, making it easier than ever to scale. This adaptable solution not only provides reliable security but also eliminates the burden of expensive upgrades, future-proofing your business.

Incredible value

Kaseya 365 User helps you save up to 70% compared to using multiple standalone solutions. Enjoy cutting-edge security, seamless automation and advanced integration without breaking your IT budget. Our cost-effective solution combines powerful tools with versatile capabilities that deliver proactive prevention, rapid response and swift recovery. With Kaseya 365 User, you get everything you need to protect your users and data while bolstering your organization's security posture.

Build a holistic user protection strategy with Kaseya 365 User

Your users are often the first target in cyberattacks, making their protection against threats like phishing, BEC, ATO, credential theft and ransomware crucial. To combat these threats and ensure the security of your users, you need a holistic approach that focuses on preventing, responding to and recovering from user-based threats.

Kaseya 365 User equips your end users with the right knowledge and tools, ensuring they remain a strong line of defense rather than a vulnerability. It prevents compromised accounts from exploitation and reduces the risk of unauthorized access, empowering your users to work securely and confidentially in SaaS environments. Kaseya 365 User offers advanced threat prevention tools, real-time alerts and automated responses that proactively block potential threats. It also enables your IT team to respond to security incidents quickly, mitigating risks before they escalate.

Kaseya 365 User's robust backup and recovery capabilities enable your IT team to restore data and operations seamlessly in the event of a disaster. This significantly reduces the IT burden and frees up time to focus on other strategic initiatives that drive your business.

1. https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf
2. https://www.idagent.com/resources/kaseya-cybersecurity-survey-report-2024/
3. https://docs.apwg.org/reports/apwg_trends_report_q1_2024.pdf
4. https://www.microsoft.com/en-us/security/blog/2024/05/15/threat-actors-misusing-quick-assist-in-social-engineering-attacks-leading-to-ransomware/
5. https://www.twingate.com/blog/tips/Darkbeam-data-breach
6. https://www.verizon.com/business/resources/reports/dbir/
7. https://www.ibm.com/reports/data-breach
8. https://www.idagent.com/resources/kaseya-security-survey-report-2023/
9. https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/
10. https://gdpr-info.eu/issues/fines-penalties/#:~:text=83(4)%20GDPR%20sets%20forth,to%20that%20used%20in%20Art.

See Kaseya 365 User in action to discover how this game-changing solution can transform the way you manage and protect your end users.

LEARN MORE

Kaseya 365 USER