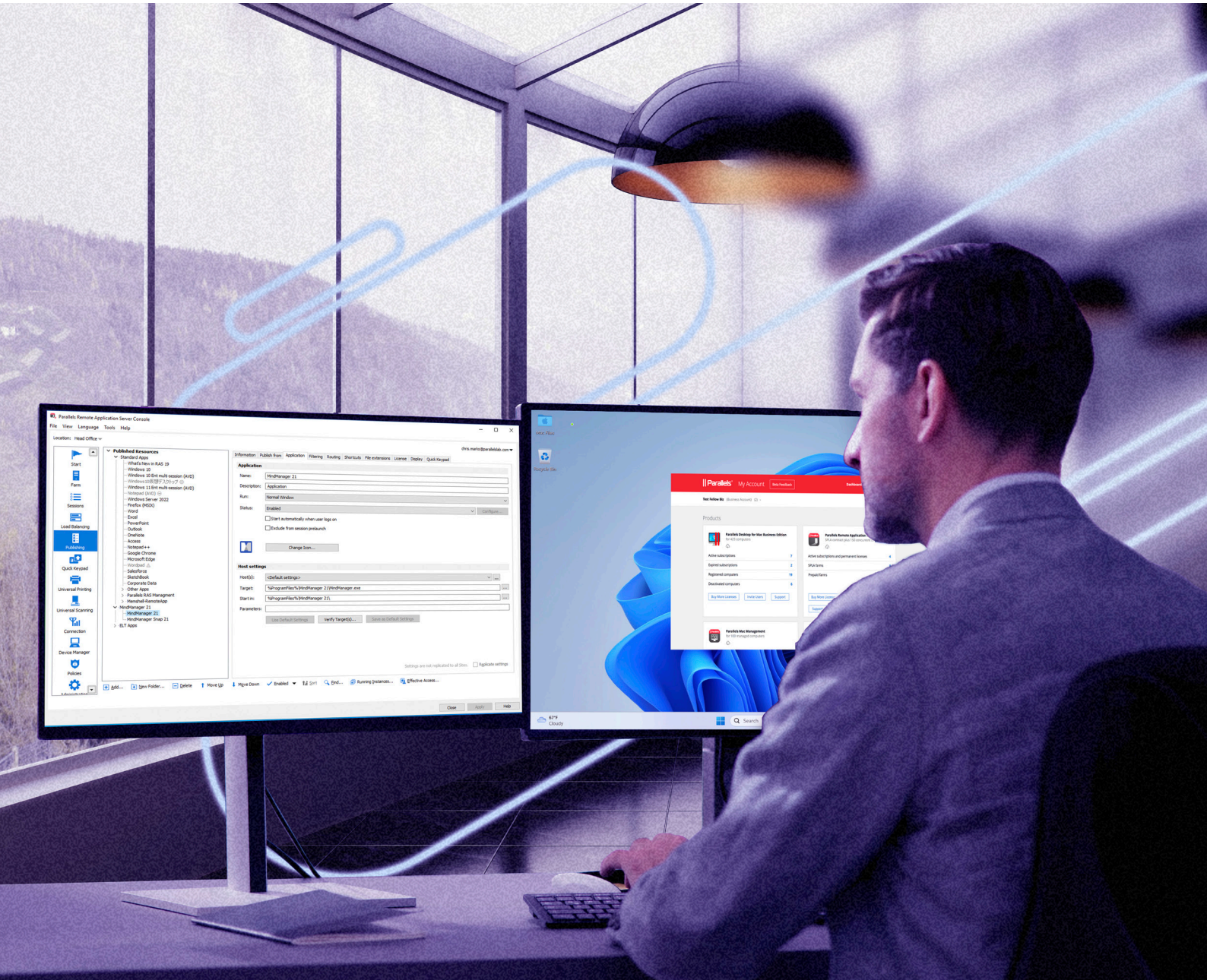
Parallels® RAS

Parallels®

WHITEPAPER

MSP Best Practices Guide: Implementing cybersecurity solutions and security management



What's covered:

Parallels®

Introduction

Organizations place immense trust in their managed service providers (MSPs) to safeguard their data and applications from cyber threats, unauthorized access, and data loss.

This trust is rooted in the expectation that MSPs will implement strong security measures, including advanced encryption, multi-factor authentication, regular system updates, and robust disaster recovery policies.

While MSPs often offer dedicated cybersecurity solutions that shield clients from an array of cyber threats, it is equally important to ensure that their solutions are also equipped with built-in security measures, helping to guarantee that client data remains fully protected.

Due to the nature of their operations, MSPs host client' data across multiple environments, including customer sites, private and public clouds, and hybrid or multi-cloud platforms.

Ensuring the protection of client data, regardless of its location, requires robust cybersecurity measures. The multiple-tenant nature of MSP operations adds to the responsibility of safeguarding data across multiple environments.

Implementing comprehensive cybersecurity and robust security measures across managed service offerings fortifies the overall defense posture and provides a more comprehensive layer of protection.

This integration helps MSPs mitigate risks more effectively and uphold their commitment to safeguarding sensitive information across all platforms and environments.

This e-book explores the importance, strategies, and best practices for MSPs to implement more effective security measures and threat management.

The importance of security management in managed IT services

1. Increasing cyber threats: Cyber threats are becoming more sophisticated and frequent. Organizations face risks from malware, ransomware, phishing, and advanced persistent threats (APTs). Without proper security management, these threats can lead to significant financial losses, reputational damage, and legal consequences.

2. Regulatory compliance: Various industries are subject to strict regulatory requirements concerning data protection and privacy. Compliance with standards such as GDPR, HIPAA, and PCI DSS is mandatory within some industries. MSPs must ensure that their services adhere to these regulations through robust security management.

3. Protecting business continuity: Security incidents can disrupt business operations, leading to downtime and loss of productivity. Effective security management ensures business continuity by proactively identifying and mitigating security risks.

4. Client trust and confidence: Clients expect MSPs to provide secure IT environments. Implementing strong security measures helps build trust and confidence, fostering long-term client relationships.

Critical components of implementing a cyber security plan

1. Risk assessment and management: Conduct regular risk assessments to identify vulnerabilities and potential threats across solutions and environments. This assessment process involves evaluating the likelihood and impact of different risks and implementing appropriate mitigation strategies.

2. Endpoint protection: Ensuring the security of client and internal devices within the organization. This process includes deploying antivirus software, firewalls, and intrusion detection systems and regularly updating and patching devices.

3. Network security: Implementing measures to protect the integrity, confidentiality, and availability of network data. These measures include secure network design, segmentation, and monitoring.

4. Data protection: Safeguard sensitive data through encryption, secure storage solutions, regular backups, and implementing disaster recovery solutions. Ensure that data is air-gapped and protected both at rest and in transit.

5. Identity and access management (IAM): Implementing IAM solutions ensures that only authorized individuals can access critical systems and data. IAM solutions include multi-factor authentication (MFA), role-based access control (RBAC), and regular access reviews.

Parallels®

6. Security awareness training: Educating clients and employees on security best practices, social engineering tactics, and recognizing and responding to potential security incidents.

7. Incident response and management: Developing and maintaining an incident response plan to quickly detect, respond to, and recover from security incidents. These plans should include incident detection, containment, eradication, recovery, and post-incident analysis.

8. Compliance management: Ensuring all security practices comply with relevant laws, regulations, and industry standards. Conduct regular audits and assessments to maintain compliance.

Best practices for implementing proactive security policies

By implementing comprehensive security management practices, MSPs can help organizations identify and address security risks, protecting their assets, data, and reputation. Adopting a proactive and layered security approach, leveraging advanced technologies, and fostering a culture of security awareness are key strategies for MSPs to safeguard their clients against cyber threats.

Here are of the key best practices for implementing a proactive security policy

1. Develop a comprehensive security policy: Establish a clear and comprehensive security policy outlining the security measures, responsibilities, and procedures forthe MSP and their clients.

2. Adopt a layered security approach: Implement multiple layers of security controls to provide a robust defense against various threats. This approach includes physical security, network security, endpoint security, application security, and data security.

3. Leverage advanced security technologies: Utilize advanced security technologies such as artificial intelligence (AI), machine learning (ML), and behavioral analytics to enhance threat detection and response capabilities.

4. Regularly update and patch systems: Ensure all systems, applications, and devices are regularly updated and patched to protect against known vulnerabilities and exploits.

5. Perform regular security audits and assessments: Conduct regular security audits and vulnerability assessments to identify and address potential security weaknesses.

6. Foster a security-first culture: Encourage a culture of security awareness within the organization and among clients. Security should be a top priority and integrated into all business processes and decisions.

7. Collaborate with trusted security partners: Partner with reputable security vendors to stay updated on the latest threats and security solutions. This collaboration can also provide additional expertise and resources.

Challenges of cybersecurity across multi-cloud and hybrid

The complexity of managing and securing client data grows as MSPs increasingly adopt multi-cloud and hybrid environments to leverage the benefits of diverse cloud services and on-premises infrastructure. MSPs now have the critical responsibility of ensuring robust cybersecurity across these varied landscapes for multiple clients.

The growing adoption of multi-cloud and hybrid environments

Multi-cloud environments

A multi-cloud strategy involves using services from multiple cloud providers (such as AWS, Microsoft Azure, and Google Cloud Platform) to optimize performance, cost, and flexibility. This approach allows MSPs and organizations to avoid vendor lock-in and leverage the best services from each provider. However, it also introduces an increased risk of cyber threats and attacks, necessitating vigilant security measures to protect data and applications across diverse platforms.

Hybrid environments

A hybrid environment combines on-premises infrastructure with cloud services, allowing organizations to maintain critical data and applications on-site while leveraging the scalability and flexibility of cloud platforms.

Importance of cybersecurity in multi-cloud and hybrid environments

1. Increased attack surface: Multi-cloud and hybrid environments expand the potential attack surface. Each cloud service and on-premises system can present unique vulnerabilities.

2. Data security and privacy: Protecting sensitive data across various platforms is crucial. Ensuring data integrity, confidentiality, and compliance with regulations such as GDPR, HIPAA, and CCPA is a significant concern.

3. Complex access management: Managing user access across multiple environments requires robust identity and access management (IAM) solutions. Ensuring that only authorized users can access specific resources is essential to prevent unauthorized access.

4. Compliance requirements: Organizations must comply with various regulatory standards that often mandate specific security measures. MSPs need to ensure that multi-cloud and hybrid deployments meet these compliance requirements.

5. Disaster recovery and business continuity: Ensuring business continuity in the event of a security breach or disaster is vital. This function involves having robust backup and recovery solutions that can function seamlessly across multi-cloud and hybrid environments.

Challenges in securing multi-cloud and hybrid environments

1. Visibility and control: It's challenging to gain complete visibility and control over all assets across multiple environments. With this visibility, it's easier to monitor, detect, and respond to security threats effectively.

2. Inconsistent security policies: Different cloud providers have varied security policies and practices. Ensuring consistent security policies and controls across all environments can be complex.

3. Integration issues: Integrating security tools and practices across on-premises systems and multiple cloud platforms can be difficult, often requiring custom solutions.

4. Skill gaps: Managing cybersecurity in complex environments requires specialized skills and knowledge. MSPs may face challenges in recruiting and retaining skilled security professionals.

Enhancing cybersecurity across multiple environments

MSPs should adopt robust best practices for enhancing cybersecurity to protect client data across multiple environments, including on-premises, cloud, hybrid, and multi-cloud setups.

1. Unified security management: Implement a unified security management platform that provides comprehensive visibility and control across all environments. This platform should include centralized logging, monitoring, and threat detection capabilities.

2. Consistent security policies: Establish and enforce consistent security policies across all environments. Utilize automation tools to ensure these policies are applied uniformly.

3. Data encryption: Ensure data is encrypted in transit and at rest across all platforms. Use strong encryption standards and manage encryption keys securely.

4. Regular audits and assessments: Conduct regular security audits and vulnerability assessments to identify and address potential security weaknesses. This process includes penetration testing and compliance audits.

5. Advanced threat protection: Leverage advanced threat protection solutions, like AI and machine learning, to detect and respond to threats in real- time. This protection includes intrusion detection and prevention systems (IDPS) and endpoint detection and response (EDR) tools.

6. Centralized consoles: Centralize configurations and monitoring through a unified management console, ensuring comprehensive data protection across all client environments.

By adopting best practices such as unified security management, consistent security policies, and advanced threat protection, MSPs can provide their clients with the necessary security to protect their assets and data in these complex environments.

Advantages of integrated security solutions

To protect their clients against cyber threats effectively, MSPs should implement solutions with built-in security that are easy to manage and administer.

These solutions provide comprehensive protection, streamline management tasks, and build client trust, enabling MSPs to deliver superior service and safeguard their clients' digital assets.

As cyber threats continue to grow in sophistication and frequency, integrating robust, manageable security solutions will remain a cornerstone of effective managed services.

The importance of built-in security solutions

Organizations face an increasing array of cyber threats and data security risks. MSPs play a crucial role in safeguarding their client's IT infrastructure, making the implementation of solutions with built-in security essential.

Solutions that inherently integrate robust security features offer several advantages that help MSPs provide comprehensive protection against cyber threats.

Comprehensive protection against cyber threats

Built-in security solutions ensure that security measures are not an afterthought but a fundamental component of the IT environment. These solutions offer a holistic approach to threat management by incorporating encryption, multi-factor authentication, and SSO features.

By adopting solutions with these security capabilities integrated from the outset, MSPs can provide their clients with a fortified defense against cyber threats. This proactive stance reduces vulnerabilities and mitigates the risk of data breaches, malware infections, and other malicious activities.

Ease of management and administration

Another significant advantage of built-in security solutions is their ease of management and administration. MSPs can benefit from centralized consoles that streamline the deployment, monitoring, and management of security measures across all client systems.

This centralized approach not only simplifies administrative tasks but also enhances the efficiency and effectiveness of security operations.

Enhanced client trust and confidence

When MSPs implement robust, easy-to-manage security solutions, they enhance client trust and confidence. Clients rely on their MSPs to deliver managed services and safeguard critical data and systems.

By delivering security as an integral part of their service offerings, MSPs demonstrate a commitment to protecting their clients' assets. This commitment fosters stronger client relationships and can be a significant differentiator in a competitive market, attracting organizations that prioritize data security and compliance.

Parallels®

Protecting virtual desktops and applications

MSPs play a crucial role in delivering secure virtual desktop and application services (VDI) to their clients. They ensure that sensitive data and applications are protected as employees access systems from anywhere. Organizations rely heavily on VDI solutions to maintain business continuity and operational efficiency, especially in remote and hybrid work environments.

Selecting a VDI solution with robust built-in security features is essential to effectively meet these challenges, protecting against evolving cyber threats while simplifying setup, management, and updates.

Comprehensive data and application protection

Built-in security features in a VDI solution provide MSPs with a foundational layer of defense against cyber threats. These features typically include encryption of data in transit and at rest, multi-factor authentication (MFA), and secure SSO access gateways.

By integrating these capabilities into the VDI infrastructure, MSPs can ensure that client data and applications are shielded from unauthorized access and data breaches. This proactive approach mitigates risks and helps MSPs maintain compliance with regulatory requirements such as GDPR, HIPAA, and PCI DSS.

Simplified setup, management, and updates

Ease of setup, management, and regular updates are equally crucial factors for MSPs when selecting a VDI vendor. Solutions that are easy to deploy and maintain allow MSPs to optimize their operational efficiency and focus on delivering value-added services to their clients. Built-in security features seamlessly integrated into the VDI platform simplify the configuration of security policies, monitoring of security events, and implementing patches and updates.

Protection against the latest cyber threats and attacks

Cyber threats are constantly evolving, requiring MSPs to stay vigilant and proactive in their security measures. A VDI vendor that prioritizes ongoing security updates and enhancements ensures that MSPs can effectively protect their clients against the latest cyber threats and attacks. Regular updates to security protocols, threat intelligence integration, and vulnerability assessments enable MSPs to pre-emptively address potential security risks and maintain a robust defense posture.

Centralized security and compliance with Parallels RAS

Parallels RAS enhances data security and ensures compliance with regulatory requirements by integrating additional layers of protection and rigorous security measures.

Supporting MSPs in delivering secure applications and desktops to clients across on-premises, cloud, and multi-cloud environments, Parallels RAS reinforces asset protection through stringent system hardening and comprehensive data access lockdown protocols.

All security configurations and monitoring can be managed efficiently from a centralized single console, providing administrators with a cohesive and streamlined approach to maintaining compliance and protecting organizational assets.

Multi-factor authentication

Enhance protection with multiple multi-factor authentication (MFA) services. Ensure high-level data security by integrating RADIUS, Deepnet, Gemalto, smartcard authentication, Google Authenticator, and other time-based one-time password (TOTP) authenticators.

Parallels®

Data segregation

Parallels RAS ensures data segregation in a multi-tenancy environment by allowing the creation of unlimited independent sites within the same farm. This setup prevents the sharing of applications, desktops, or data between sites, thereby enhancing data protection.

SAML SSO authentication

Simplify the management of user identities from various organizations with single sign-on (SSO) capabilities. Allow users to seamlessly switch between hosted Windows, web, and Software as a Service (SaaS) applications without needing to re-enter credentials.

Certificate management and Let's Encrypt

Enhance secure user access with built-in SSL certificate creation through Let's Encrypt. Parallels RAS automates the renewal process and allows you to manage certificates directly from the Parallels RAS Console.

Encryption protocols and compliance

Parallels RAS reinforces security by centralizing and managing data access. The Parallels RAS Secure Client Gateway encrypts end-user connections using SSL/TLS and FIPS 140-2-compliant encryption. This encryption ensures adherence to data compliance policies, including PCI DSS, HIPAA, and GDPR. Customized policies enable organizations to tailor their security protocols to meet specific compliance mandates, thus streamlining adherence and reducing the risk of data breaches.

Parallels RAS reporting engine

The Parallels RAS reporting engine provides detailed reports that identify suspicious activity and offer valuable insights into server health, application usage, connected devices, and user activities. It generates detailed reports on server usage, device access, application utilization, and more. Additionally, these reports play a crucial role in business continuity and disaster recovery (BCDR) planning.

Centralized single console for comprehensive control

Ensuring the protection of client data across multiple environments, including private and public clouds, as well as hybrid or multi-cloud platforms, is paramount. Parallels RAS simplifies this process by offering a single console for all tasks, streamlining the deployment, monitoring, and management of security measures across all client systems.

This unified console handles app and desktop management, image handling, reporting, gateway, load balancing, access control, authentication, and authorization. It enables effortless management of users and workloads across multiple sites and data centers without the need to switch consoles, enhancing efficiency and security.

Featuring a multi-tenant architecture and a concurrent usage-based SPLA license model with monthly billing reports, Parallels RAS enables MSPs to deliver secure managed services seamlessly.

Experience Parallels RAS and discover how effortless it is to deliver secure applications and desktops to your clients from anywhere, at any time, across any device or operating system.

Try now: Get started with your free trial

Parallels