Kaseya® WHITE PAPER

# Protect Your Company's Data and Infrastructure with Layered Security


Kaseya®

Kaspersky Lab recently published an eBook, Cybercriminals: Unmasking the Villain, which provides insight into cybercriminals' evolving strategies and tactics. Here are three items that point to the specific dangers for SMBs:

- "31% of all cyberattacks are directed at businesses with less than 250 employees"
- "42% of confidential data loss is caused by employees" often due to well-meaning employees "opening unauthorized email attachments, forwarding sensitive information or storing data insecurely"
- "Hacking a small business to get into a larger business is now standard operating procedure for cybercriminals."

These evolving cybercriminal practices underscore the reality that proper, up-to-date security practices are more vital than ever to the health and well-being of every company, no matter its size. The risks are too high, and the incidence of exposure and breaches is only increasing. For SMBs, the best way to gain proper protection is through managed security services. Today's security threats require a consistent and layered security approach to ensure your company's data and infrastructure are hardened and protected from external attacks.

Today's security threats require a consistent and layered security approach to ensure your company's data and infrastructure are hardened and protected from external attacks.

## Better Protection through Layered Security

Even better, taking a more inclusive approach can—with the right technology solutions and automation—improve security while freeing up time and resources for other projects. What is included in this layered approach for an MSP?

### Full 360° visibility

You can't manage what you can't see. You need a solution that easily and continually discovers all devices on your network, including servers, laptops, kiosks, mobile devices, scanners, and peripherals. It also needs to constantly collect real-time status on all operating details for these devices to keep systems up to date.

### Consistent anti-virus and anti-malware (AV/AM)

Once all devices are visible, you need to ensure that they are protected with AV/AM software. Installing is just the beginning—you need to update systems to ensure they are always running the latest versions. So get a solution that makes this easy and automatic.

### Keeping patches current

All devices need to be up-to-date on Microsoft and other third-party patches. Patches and updates can be tested centrally then pushed out to all machines or select groups once they are proven safe. Again, with the right type of automation, you can be confident that all patch updates are successful—and that you'll get an alert if they aren't.

### Policy-based configurations

Look for solutions that enable multiple sets of policies to be applied automatically based on any set of groupings you want—by device type, user role, or even location type—and that can check that each device is in compliance with its assigned policies. This way, you can standardize and update all infrastructure under your care with confidence. Of course, doing this successfully depends on powerful and flexible automation to keep up with multiple policies and update many devices by simply changing a policy once.

### Regular, routine backup and recovery

Routine, reliable (and encrypted) backup and recovery is a vital component of any complete layered security approach. In addition, complete and regular backups are also a defense against CryptoLocker and other ransomware attacks.

Kaseya®

### Complete Identity and Access Management (IAM)

You already know you can't use vendor-supplied defaults for system passwords. IAM takes this further by including multi-factor authentication, which is a requirement for some compliance regulations. IAM also includes centralized credential management, policy-based rules, and Single Sign On for end users (including partners—remember how Target was breached!) to keep internal systems protected.

### Policy-based access

You need to be able to create as many policies about access as for device configurations. With these policies in place, you can quickly and completely delimit access to systems and data based on staff's functionality and job requirements. In addition, you can create policies to require password changes after so many days and/or lockout rules after so many failed login attempts. Location-based rules would control when and where users can sign in—limiting user access, for example, by location such as building, city, country, etc.

### Deprovisioning users

Statistically, admins enable more users than they disable. While outside attacks lead the list of retail breaches, it's only prudent to make sure you have a way to quickly and completely deprovision a user—whether employee, sysadmin, or partner—from any and all systems under your care.

### Alerts on usage patterns

You need to be alerted of any potential security breach beyond viruses and malware, including unusual patterns of user behavior or access or suspicious spikes in bandwidth utilization.

### App blocking

Disallowing certain apps—say peer-to-peer apps or Flash—can help keep systems clean and running strong. This also provides another security dimensions since apps that are more vulnerable can be blacklisted to prevent users from installing and inadvertently creating an enticing entry point for hackers.

### Web filtering

Blocking websites sites known to host spyware, viruses or malware limits vectors of attack opened by unwitting users. Filtering is usually accomplished through many tactics, including a database of black-listed websites, policy-based content filtering, and scanning and inspecting SSL-encrypted traffic.

### Real-time tracking alerts

If a device, laptop or even server idea leaves a company site, you should know instantly where it is once it's back online.

### Securing/destroying data

Once you know a device has gone out of corporate control, you need to be able to ensure the data on the system is not accessible to malicious players. You need the ability to remotely disable the device, encrypt the data, or even destroy the OS on that device.

## Learn more

If you're interested in learning how Kaseya VSA and Kaseya AuthAnvil can enable you to implement an inclusive layered security approach, download our "**Automation Cheat Sheet: IT Compliance, Audits and Security.**"



Rev 012017

Kaseya®