Layered Security:

Essential for Protecting Business Growth

Networks have grown more complex. Businesses are moving their services to multiple cloud vendors, and even though cloud services are generally secure, nothing is perfect. Companies should adopt a multifaceted, layered security strategy to defend against cyberattacks and protect their growth.

Business Growth Depends on Secure Environments

90% of c-level executives feel public trust in the security of the internet is essential for businesses growth.[1]

As dependency on the internet grows, so do security risks. You are at risk even if you think:

- You don't have a lot of assets or valuable information anyone wants
- You don't have a large amount of money to steal
- You aren't a big enough company to be a prime target

Keeping businesses secure online builds a foundation for growth by:

- Boosting uptime
- Increasing productivity
- Reducing costs from time and resources spent mitigating cyberthreats and dealing with breaches
- Demonstrating compliance
- Protecting intellectual property and business data
- Maintaining good business and brand reputation
- Reducing customer churn

Your Customers Are Prime Targets

67% of SMBs have faced a cyberattack, and **58%** experienced a data breach.[2]

The consequences can be dire: The average time to detect and contain a breach is estimated at **279 days**.[3]

40% of companies are down more than 8 hours after a breach.[4]

A Strong Security Foundation Can Help Reduce Your Customers' Risks

Secure Your Own MSP

- Practice the fundamentals by patching, putting up firewalls, running backup, and employing professional email security in house
- Understand what applications are in use and who should have access
- Invest in advanced endpoint protection solutions for your own machines
- Monitor for threats to your network with security information and event management (SIEM) tools
- Use a password management tool to maintain strong password security

Mitigate Risk with Layered Security

- Assess your customers' risks.
- Implement the right layers to mitigate risks including:
  - Patch management
  - Endpoint detection and response
  - Disk encryption
  - Network protection
  - Firewall management
  - Backup
  - Web protection
  - Mail protection
  - Password management
  - Identity management
  - SIEM
  - Vulnerability scanning

Educate Your Customers

- Establish and maintain a culture of security for your customers with regular training and awareness
- If needed, team up with third parties to help with security awareness training
- Teach users to spot malicious emails or other social engineering attempts, with examples
- Retrain users on an on-going basis—security training should be regular and frequent to get the results you need

Strong Security Requires Multiple Layers

Protecting your customers and your own revenue requires you to fight cybercriminals on multiple fronts. Key technology in your arsenal should include:

Patch management

Unpatched vulnerabilities contribute to **34%** of breaches.[5]

Backup and data protection

Ransomware causes an average of **16.2 business days** of downtime.[6]

Email protection

Spam makes up **53%** of all email traffic.[7]

Endpoint protection

Fileless malware attacks increased by **more than 250%** in H1 2019.[8]

Use N-able RMM to Help Prevent Cyberthreats from Stopping Growth

N-able™ RMM is built to help MSPs keep their customers safe from cyberthreats. From a single solution, you can provide customers with multiple layers of security, including patch management, integrated backup and recovery, email protection, web protection, and even AI-driven endpoint protection to help defend against fileless attacks. Try it free.

Start free trial

1"Securing the Digital Economy: Reinventing the Internet for Trust," Accenture. accenture.com/_acnmedia/Thought-Leadership-Assets/PDF/Accenture-Securing-the-Digital-Economy-Reinventing-the-Internet-for-Trust.pdf#zoom=50 (Accessed January 2020).
2"2018 State of Cybersecurity in Small & Medium Size Businesses," Ponemon Institute. keepersecurity.com/assets/pdf/Keeper-2018-Ponemon-Report.pdf (Accessed January 2020).
3"Cost of a Data Breach Report: 2019," IBM. databreachcalculator.mybluemix.net/ (Accessed January 2020).
4"Cisco 2018 Cybersecurity Report: Special Edition SMB," Cisco. cisco.com/c/dam/en/us/products/collateral/security/small-mighty-threat.pdf (Accessed January 2020).
5"Cybersecurity: One in Three Breaches Are Caused by Unpatched Vulnerabilities," ZDnet. zdnet.com/article/cybersecurity-one-in-three-breaches-are-caused-by-unpatched-vulnerabilities/ (Accessed May 2020).
6"Ransomware Costs Double in Q4 as Ryuk, Sodinokibi Proliferate," Coveware. coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate (Accessed May 2020).
7"'Abuse Emails:' What They Are and How They Impact Your Email Marketing," Entrepreneur. www.entrepreneur.com/article/335272 (Accessed May 2020).
8"Top Cybersecurity Facts, Figures, and Statistics for 2020," CSO. csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html (Accessed May 2020.)

About N-able

N-able empowers managed services providers (MSPs) to help small and medium enterprises navigate the digital evolution. With a flexible technology platform and powerful integrations, we make it easy for MSPs to monitor, manage, and protect their end customer systems, data, and networks. Our growing portfolio of security, automation, and backup and recovery solutions is built for IT services management professionals. N-able simplifies complex ecosystems and enables customers to solve their most pressing challenges. We provide extensive, proactive support—through enriching partner programs, hands-on training, and growth resources—to help MSPs deliver exceptional value and achieve success at scale.

n-able.com