The State of Layered Security in 2021

The stakes of cybersecurity have never been higher, and the bar has been raised for service providers—but the right security layers can **help you meet the current moment with confidence.**

Attacks can be costly

41%
of cyberattack victims are **SMBs**[1]

280
days to **identify and contain** a breach[2]

$280,000
is the **average cost** of a cybersecurity incident[3]

Layered security can help

Multiple steps in an attack mean multiple chances to shut it down.

Start with these core layers:

INTERNET | NETWORK | PEOPLE | APPLICATION | DEVICE

Internet

- Implement a dedicated email security solution to extend the native security in email programs
- Configure email to disable macros, block password-protected documents, and scan any link extensions
- Enable proactive DNS filtering on endpoints to help block on- and off-site devices from visiting malicious web sites
- Close open internet-facing ports including remote desktop protocol

Network

- Use an endpoint firewall like Windows® Firewall to help prevent lateral spread on a network

People

- Offer regular security training to help users recognize scams, set strong passwords, and follow security policies

Application

- Schedule regular patching of both operating systems and third-party software
- Avoid using end-of-life (EOL) software as these typically are unsupported

Device

- Choose an antivirus solution that uses signature, heuristic, and behavioral scans
- Set remote monitoring and management (RMM) rules to flag services being disabled in bulk

Then add these **advanced** layers:

Device

- Swap out antivirus (AV) for endpoint detection and response (EDR) that uses artificial intelligence (AI) and machine learning
- Consider offering endpoint vulnerability scans to find such issues as missing patches, default passwords, and misconfigurations

People

- Use a password manager internally for your team and offer password-management-as-a-service to customers to further lock down user credentials
- Implement multifactor for added security, preferably using an authenticator application instead of text or email

Application

- Reduce shadow IT by limiting users from installing unsupported software via an allow/deny list application like AppLocker®
- Review cloud software by examining their security protocols published on their website (and be wary of those that don't)

Internet

- Add a next-generation firewall that offers security features like malware detection, intrusion prevention, and SSL inspection
- Look into cloud-based firewalls to further move protection outside of the perimeter

Don't forget backup

Backup isn't always considered a security technology, but it's crucial for any layered security strategy. If an attack lands, backup gets customers up and running fast. **Look for backup that offers:**

- A cloud-first architecture so you have a separate copy if ransomware or malware deletes local backup
- Automated recoverability testing to make sure backups are ready to go
- Standby systems to allow minimal disruption to business continuity

For comprehensive coverage, **partner with an MSSP**

* Some customers may need extensive security, particularly if they're regulated.

* It may help to work with a dedicated security provider.

They can help:

- Monitor network traffic around the clock
- Hunt for threats in environments
- Perform external vulnerability scans to look for additional internet-facing vulnerabilities
- Improve your own internal MSP security

Lay a strong foundation

Get the tools you need to provide strong layered security services.

Visit N-able.com

N-ABLE

N-able.com

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.

1. "VDBIR Summary of Findings." Verizon. enterprise.verizon.com/resources/reports/dbir/2019/summary-of-findings/ (Accessed December 2020).
2. "Cost of a Data Breach Report 2020." Ponemon and IBM. ibm.com/security/data-breach (Accessed December 2020).
3. Cyber Readiness Report." Hiscox. https://www.hiscox.com/documents/2019-Hiscox-Cyber-Readiness-Report.pdf (Accessed December 2020).