N-ABLE™

N-able Layered Security for IT Departments

Competitive comparisons

	N-ABLE	KASEYA	SOPHOS	FORTINET	KASPERSKY	CARBON BLACK	WEBROOT
EDR	✓	✓	✓	✓	✓	✓	✓
Patch management	✓	✓	–	✓	✓	–	–
Vulnerability scanning	✓	✓	–	✓	✓	–	–
Cloud email security	✓	–	✓	✓	✓	–	–
Web security	✓	✓	✓	✓	✓	–	✓
Password management (Business grade)	✓	✓	–	✓	–	–	–
Backup	✓	✓	–	–	–	–	✓
Disk encryption management	✓	✓	✓	✓	✓	–	–
Device monitoring	✓	✓	✓	–	–	–	–
Firewall appliance	–	–	✓	✓	–	–	–
Unified IT management console	✓	–	–	–	–	–	–

✓ Third-party integration and/or limited functionality.

Put simply, N-able layered security is far more than software. Some of its premier benefits include:

- Bolstered data security to reduces business risk overall
- Future-proofs against ever-evolving threats
- Allows staff to focus on business development vs. learning complex security tools
- Cloud-first, instant recovery reduces downtime

All of this lives on an integrated cloud console that allows you to layer on the security capabilities as you need them—without wasting time or budget.

Layered security capabilities

ENDPOINT DETECTION AND RESPONSE (EDR)

N-able EDR provides frontline technicians with the ability to detect the latest malware—including ransomware—investigate the threat and fix any damage quickly and easily. Functionality includes restoring endpoints to their healthy state and completing a threat incident response within just minutes.

PATCH MANAGEMENT

Patch management gives IT managers complete granular control over when, how, and which patches are deployed across the network, devices, or groups. Plus, it can protect multiple operating systems and third-party applications.

VULNERABILITY SCANNING

Designed to identify potential misconfiguration or open ports on the network, vulnerability scanning also provides historical reporting to allow IT departments to show security progress over time.

CLOUD-BASED EMAIL SECURITY

Required even if a business has a primary layer of security, as with Microsoft 365™, Mail Assure provides added control and an additional level of defense. Built to protect against spam, viruses, malware, phishing, ransomware, and other email-borne threats, while archiving data to protect it further.

WEB SECURITY

Web security still matters. Through the evolution of mobile workforces, web database and DNS-based filtering, web protection is essential to keep businesses, staff, and their data safe—both on and off the network.

PASSWORD MANAGEMENT

Password management significantly reduces your password risks. It allows IT managers to implement rules to generate strong passwords, eliminate re-use, and automate password rotation and routine maintenance. Encrypt, store, manage, and retrieve credentials quickly and safely.

BACKUP

In the modern security environment, businesses need more than the fast, secure, and hybrid architecture that underpins premier backup solutions; they require multi-storage and restoration capabilities that makes the chance of an effective ransomware nearly zero percent.

DISK ENCRYPTION MANAGEMENT

Volume-level disk encryption protects your customers' data from theft or accidental loss by making information on hard drives unreadable to unauthorized users. Disk encryption is best for businesses and environments where data is a critical asset or governed by compliance regulations such as GDPR, PII, and PCI DSS.

DEVICE MONITORING

Monitoring provides frontline techs, IT managers, and security specialists the real-time and historical trending to predict and seek out threats and attacks before they have a chance to escalate. Monitoring identifies and alerts you to abnormal trends—a critical early indicator of potential attacks.

FIREWALL APPLIANCE

Firewall is a system built to protect private networks from unauthorized and unverified access through an internet connection. Firewalls can be either in the form of hardware or software—or a combination of the two.

Learn more about N-able Layered Security for IT Departments