FORTINET

4 Best Practices for Efficient Network and Security Management



Table of Contents

Executive Summary	3
1: Network Security Management Requires a Consolidated View	5
2: Device Management Requires a Micro View	7
3: Configuration Backup Is Essential	9
4: Log Retention Is Critical	11
Improve Security and Help IT Teams	13

Executive Summary

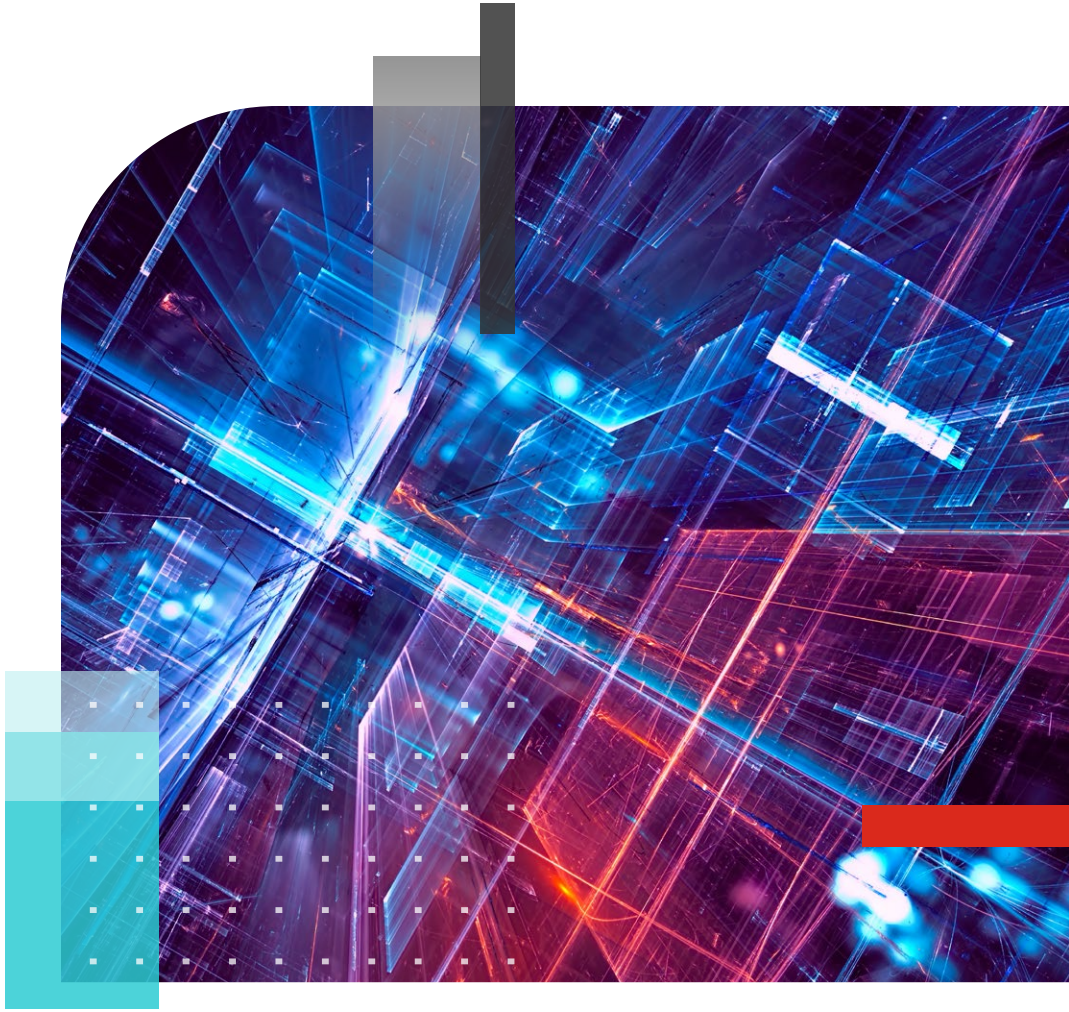
As organizations embrace the flexibility of hybrid work, cloud applications, and smart devices, keeping networks up and running with consistent user experience has become increasingly complex. Every new user, device, application, and branch expands a potential attack surface, creating more opportunities for bad actors to exploit vulnerabilities. IT teams are expected to secure these dynamic environments while maintaining business continuity at scale with limited resources.

To address these challenges, organizations need a secure, well-managed network with centralized control and visibility to easily deploy devices, enforce security, and respond to threats before they enter their networks. A next-generation firewall (NGFW) is the first line of defense. It provides the foundation for protecting edge and cloud environments against evolving cyberthreats while enabling secure connectivity for users, devices, and applications. Only with unified cloud-based management, can organizations centrally monitor, configure, and maintain firewalls and connected network devices from a single interface. This simplifies operations, expands visibility, and ensures consistent protection across offices, branches, and remote locations.



The number of connected IoT devices is estimated to reach 39 billion in 2030, reflecting a CAGR of 13.2% from 2025.[1]

1: Network Security Management Requires a Consolidated View



Organizations, especially small and midsized businesses (SMBs), need a holistic but easy-to-digest view of their networks. With different users and a range of devices like network firewalls, Ethernet switches, and wireless access points, IT teams need full visibility in one solution that includes device configurations, log files, audit trails, security event tracking, traffic analysis, and accessed websites.

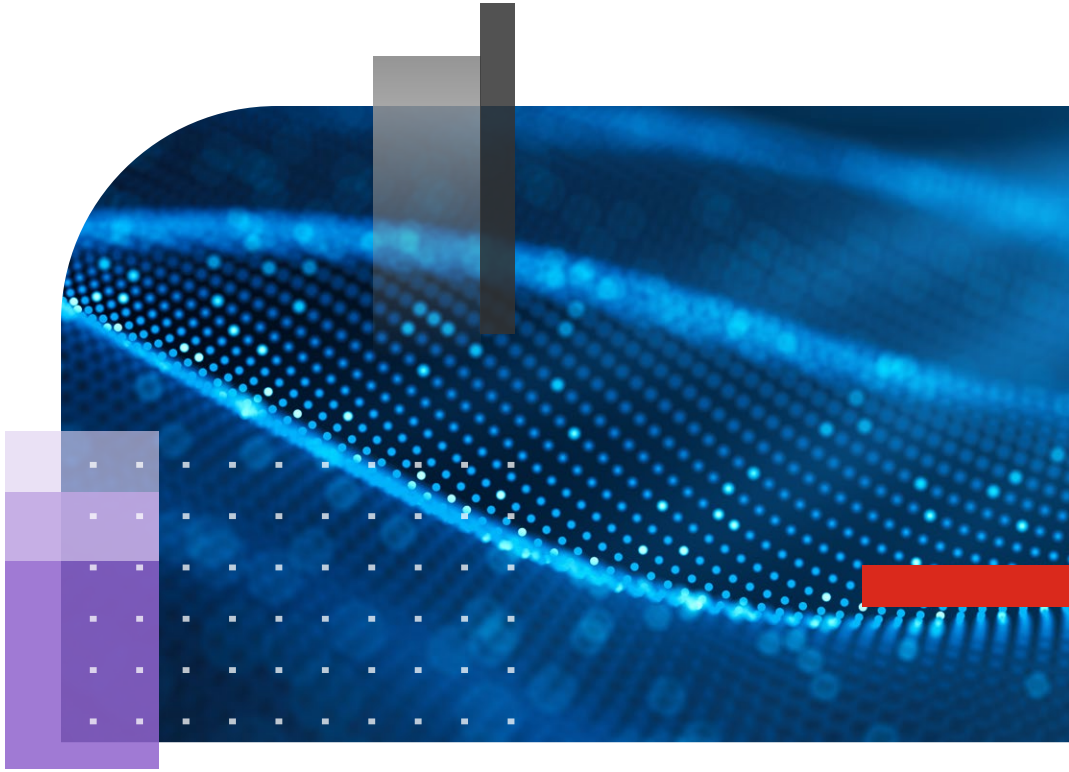
A holistic view of network performance and threat activities also allows IT teams to see top threats, application traffic, websites, and other pertinent information immediately. A networkwide dashboard is also critical, providing visualization of real-time and historical data to help teams troubleshoot issues quickly and make better decisions for optimizing network performance and user experience. For example, this macro view shows how applications accessed by users may be contributing to risk factors and performance slowdowns.

In a nutshell, this consolidated view should provide insights into everything happening on the network and empower IT managers to discover, interpret, and prioritize security risks. Additionally, it should highlight the deployment's security score in comparison to the industry average and range, to help teams improve security and performance.



86% of organizations report one or more breaches in the past 12 months. Fifty-two percent say breaches cost them more than $1 million—up from 38% in 2021.[2]

2: Device Management Requires a Micro View



Although a unified view is essential to see how all the pieces of network security fit together, IT teams also need the ability to drill down into the details of a particular device. They should be able to easily access information, including access policies, configuration settings, and device health. And that information should be visible within the framework of the broader network context, such as segments or zones, routers, switches, and wireless access points.

Equally important is presenting this information in an intuitive, role-based interface that provides the right level of access for each administrator. With centralized visibility, IT teams can streamline policy management, simplify role administration, and quickly identify configuration issues. For example, administrators should be able to block or limit access by application, view, and violation of these access policies, plus verify that the same policies are applied across their networks.

Manually logging into individual devices for routine reviews is impractical and inefficient in today's distributed environments. As the number of devices grows, infrequent review of device configurations puts network security and compliance at risk. Cloud-based unified management can eliminate these challenges by providing a macro view with consistent policy enforcement and automated monitoring. This helps ensure compliance and consistency and reduces the burden on IT resources.



IT leaders cite lack of cybersecurity skills as a top cause of security breaches (56%). Fifty-one percent say that they need senior-level cybersecurity skills most of all, yet 49% struggle to get approval for additional cybersecurity talent.[3]

3: Configuration Backup Is Essential



Once a network is secured and compliant, organizations need a reliable and automated method to back up network and device configurations to ensure high availability and business continuity. A minor error in configuration changes can disrupt operations or introduce a potential vulnerability. A secure configuration backup system allows IT teams to automatically store previous configurations of managed firewall and network devices, making it easy to roll back the configuration to the last known good state.

The ability to roll back to a previously verified configuration minimizes downtime. It enables IT teams to recover operations and gain time to troubleshoot configuration changes that may have caused unintended consequences. A configuration backup system also reduces operational risks by ensuring that trusted configurations are always available for recovering, making it a crucial requirement for building a resilient network.

For example, when a new firewall configuration change unintentionally creates an unauthorized access path to unclassified services, IT teams can quickly restore the previous configurations to eliminate the risks. Additionally, configuration backups can be used to recover operations from device failures or outages caused by incorrect configuration changes. This helps organizations maintain continuous operations while reducing the impact of human errors.



Like any device, firewalls are not immune to hardware failures, configuration issues, or even disasters. Being able to recover quickly is essential to maintaining a secure and stable network environment. This is where automated backups for firewalls come into play, acting as your safety net in times of crisis.[4]

4: Log Retention Is Critical



Security needs to be considered a process of continuous improvement. This requires visibility into network and user behavior, the status of security devices, and detailed logs of security events and changes. However, log retention, an integral part of any security and compliance program, is often an afterthought.

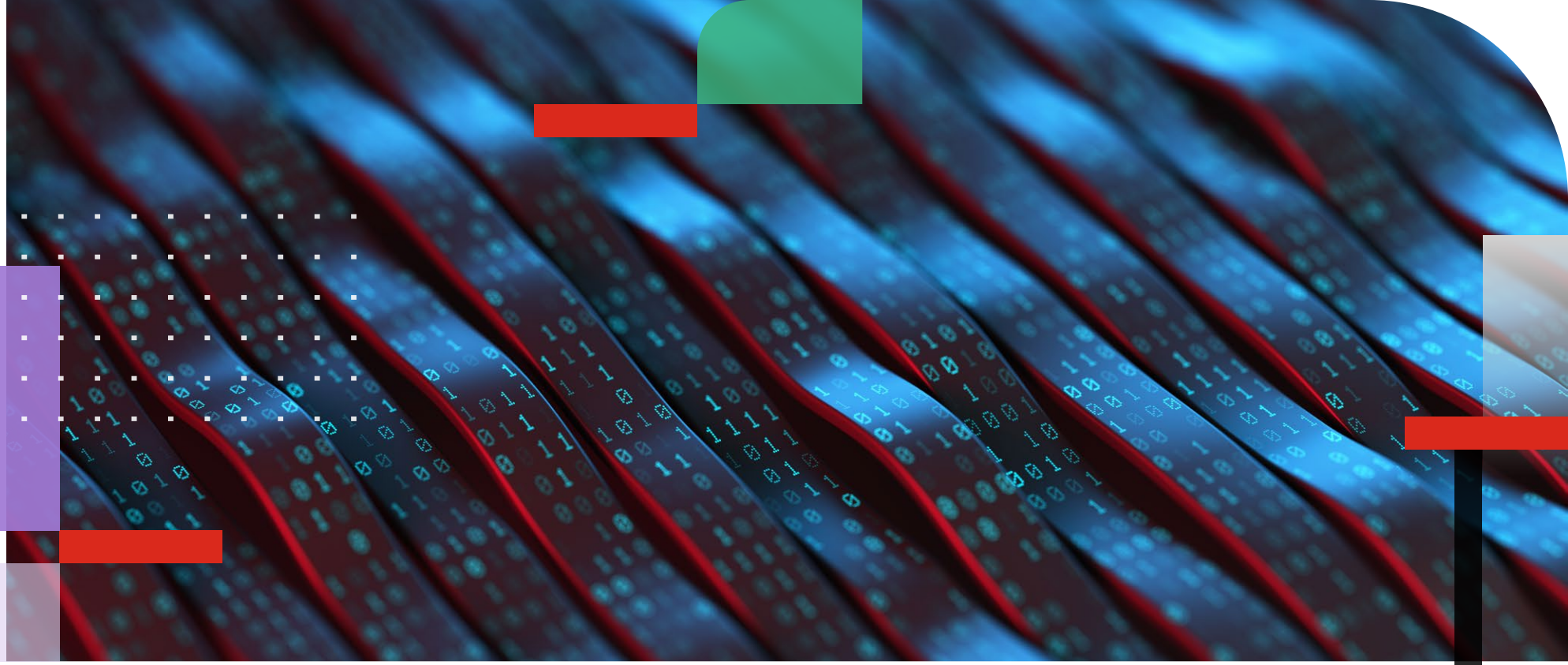
Security logs can grow rapidly and administering a separate storage system is expensive, can impact network and application performance, and requires trained staff. An effective security management system should automatically retain logs of all security events.

In many industries, retaining this information is required for compliance purposes. Whether log retention is required or not, it is always a good idea. If a security incident occurs, investigators, insurance companies, and internal procedures will require a forensic examination of the incident. In the event of a forensic investigation, security logs will serve as the primary source of evidence, and the investigation will likely fail if logs are not retained.

Any security management system should retain logs for at least a year and should have the ability to archive logs for far longer.



The significance of maintaining security logs cannot be overstated in the intricate web of digital security. Beyond streamlining incident response, which enables organizations to diagnose and mitigate the impact of security breaches swiftly, security log retention is increasingly becoming a determining factor in acquiring cyber insurance policies.[5]



Improve Security and Help IT Teams

Efficient network and security management is essential for protecting businesses without overburdening constrained IT resources. By adopting these four best practices and leveraging the advantage of a unified cloud-based management solution like FortiManagement Cloud, SMB organizations can unify management, automate routine tasks, improve visibility, strengthen security, and free up IT teams to focus on supporting business growth.

[1] Global IoT Market Forecast, IoT Analytic, October 2025.

[2] Fortinet Report Reveals Cybersecurity Hiring Stalls as Nearly Half of IT Leaders Face Corporate Pushback, Fortinet, April 28, 2026.

[3] Ibid.

[4] The Benefits of Setting Up Automated Backups for Firewalls, Sikich, May 16, 2025.

[5] Mastering Log Retention Policy: A Guide to Securing Your Data, Cribl, accessed August 5, 2026.

FORTINET

www.fortinet.com

Copyright © 2026 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's SVP Legal and above, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

August 11, 2026 2:25 PM / MKTG-4014-0-0-EN