eBook

Top 10 Network Security Best Practices

Extreme networks

Table of Contents

Introduction

While no company is immune from suffering a security breach, there is no one-size-fits-all strategy. What's right for you is going to be affected by the industry you are in; what data you need, and when and where you need it; expectations of customers, employees, and other stakeholders; regulatory requirements; your existing infrastructure; and many other factors.

At Extreme Networks, we believe that a good network security strategy is one that is multilevel: designed for the needs you have today and able to be adapted to the changing circumstances you will inevitably face tomorrow.

Here are the Top 10 Network Security Best Practices, based on decades of experience implementing smart, cost-effective security capabilities for the world's leading enterprises.

*Cybersecurity is the **number one priority** when it comes to 2020 strategies, policies and management processes*

Source: NASCIO

***$133B** Worldwide Spend on Cybersecurity by 2022.*

Source: Gartner

***68%** of business leaders feel their cybersecurity risks are increasing.*

Source: Accenture

***52%** of breaches featured hacking, **28%** involved malware and **32–33%** included phishing or social engineering, respectively.*

Source:Verizon

*The average cost of a data breach is **$3.92** million as of 2019.*

Source: Security Intelligence

Best Practice

1

Risk Assessment

Best Practice #1: Risk Assessment

Identify Vulnerabilities

Security risks are different for every industry: a health clinic bombarded with ransomware attacks has very different needs from a school protecting the online safety and data privacy of its students. The pharmaceutical manufacturer on guard against theft of its intellectual property has very different needs from the retailer fighting off credit card fraud.

It's not only that different businesses in different vertical markets have different security needs, but it's also the changing role of the network. The network perimeter continues to expand; services and infrastructure are migrating to the cloud, IoT and ransomware are colliding. The landscape is dynamic with emerging security threats, such as the adversarial attacks on Machine Learning, that are only adding to the complexity.

Starting with a Risk Assessment is essential in order to level set where your business is at, and to determine your network security goals.

- Identify what is most critical to your business
- Consider your IT, OT and IoT environment
- Prioritize
- Consider hiring a penetration expert

15% of breaches involve Healthcare organizations, 10% in the Financial industry and 16% in the Public Sector.

Source: Verizon

The Healthcare Industry has the highest number of ransomware attacks. Attacks will quadruple by 2020.

Source: CSO Online

Financial and Manufacturing Services have the highest percent of exposed sensitive files at 21%.

Source: Varonis

Supply chain attacks are up 78% in 2019.

Source: Symantec

43% of breach victims were small businesses.

Source: Verizon

Best Practice

2

Zero Trust Approach

Best Practice #2: Zero Trust Approach

Secure Outside and Within Organizations

With over 30% of security breaches originating inside organizations, more enterprises are adopting a 'Zero Trust' approach. The philosophy behind a zero trust network assumes that there are attackers (intentional and non-intentional) both within and outside of the network, so no users or machines should be automatically trusted. Firewalls alone are not enough and the cloud has redefined any networks border.

Zero Trust Security is an IT Security Model that requires strict identity verification for every person and device trying to access resources on a private network, regardless of whether they are sitting within or outside of the network perimeter. No single specific technology is associated with zero trust; it is a holistic approach to network security that incorporates several different principles and technologies.

Adopt a Zero Trust Approach to Network Security:

- Start from the vantage point that no one/device is trusted
- Educate staff and end users about Proper Security Practices
- Strictly enforce those practices

34% of data breaches involved internal actors.

Source: Verizon

61% of companies have over 500 accounts with non-expiring passwords.

Source: Varonis

94% of malware was delivered by email.

Source: Verizon

Best Practice 3

Network Visibility

Best Practice #3: Network Visibility

Invest in Analytics

Not only are many businesses unaware of the endpoints connected to their networks, but they also lack the in-depth visibility to know what, where, and with who devices may be communicating. It is impossible to secure what you do not know about, which is why investing in analytics is essential.

Fortunately, analytics has evolved over the past decade from descriptive (the most basic form) to predictive (capable of modeling future behavior) to prescriptive (capable of optimizing future actions). Business can now leverage not only network and application analytics, but emerging technologies such as security analytics to greatly improve the security posture of networks.

Increase network visibility:

- Invest in advanced analytics, including security analytics that can provide a comprehensive view of the traffic traversing your network by linking diverse types of security event info
- Consider application telemetry as a critical piece of securing the infrastructure
- Ensure visibility of traffic flow (East/West and North/South)

61% of networking professionals had low to no confidence that they knew every device connected to their network.

Source: ZK Research

***Less than half** of all businesses are able to detect IoT breaches.*

Source: 2019 Gemalto study

Best Practice

4

Policy-Based Access Control

Best Practice #4: Policy-Based Access Control

Control Who and What Gets on the Network

Policy-based Access Control creates a centralized place to implement and manage the profiles and policies that control network access. As each person and device seeks access to the network, it makes it possible to check their identity against an identity store, perform a device health check (to make sure the device is compliant), and then, based on the predetermined role, provide access to a certain portion of the network.

Instead of an overly simplistic binary "you are in, or you are out" approach, enterprise networks require highly granular policies based on user, device type, location, time of day, connection type and more.

Deploy strong policy-based network access control:

- Tailored to your environment (on-premise/cloud)
- Role based policy
- Consistency across wired and wireless

*Almost **20%** of IT professionals onboard and secure corporate, guest and BYOD devices the same way.*

Source: Extreme Survey

*The top reasons for unsuccessful NAC implementations are a lack of qualified IT personnel (**37%**), too much maintenance cost/effort (**29%**) and implementation complexity (**19%**).*

Source: Extreme Survey

Best Practice

Network Segmentation

Best Practice #5: Network Segmentation

Contain Breaches and Isolate Hackers

It is widely acknowledged that one of the most overlooked security strategies is network segmentation and isolation. It's critical to strengthen the most sensitive parts of your network, making them accessible only to those within the organization with a particular need. A key way to accomplish this is through network segmentation.

Segmenting a network creates dead ends: someone who gets access to one part of the network can't go elsewhere on the network. If that person has a malicious or criminal intent, the potential for damage can be contained.

As a National Security Agency expert aptly stated "In the event of a breach, segmentation is the difference between an incident and a catastrophe."

Consider network segmentation solutions that provide:

- IT and IoT Isolation
- Strong Access Controls
- Tiered environment
- Strong monitoring of user systems both into and out of segments using firewalls

*Today only **1%** of companies have a segmentation strategy. By 2023, **30%** will have one.*

Source: Gartner 2019

*Customers who segment will experience **25% fewer** successful cyber attacks.*

Source: Gartner 2019

***53%** of companies had over 1,000 sensitive files open to every employee.*

Source: Varonis


Best Practice
6
Automate Compliance

Best Practice #6: Automate Compliance

Importance of Data Privacy Increasing

Whether it is HIPAA in healthcare, PCI in retail, FIPS in government, or GDPR in the EU, compliance regulations help establish the security requirements for vertical industries or enterprises conducting business in certain countries.

Keeping data classification and governance up to date is instrumental to maintaining compliance with data privacy legislation, and avoiding hefty fines, such as the $57 billion fine that Google faced for GDPR violations in 2019.

Pay close attention to compliance mandates:

- Ensure compliance with industry standards and regulations
- Automate Network Configuration Compliance where possible
- Automate Compliance Reporting
- Eliminate Manual Audits and Errors

69% of companies see compliance mandates driving spending.

Source: CSO Online

Companies spent $9 billion on preparing for GRPR.

Source: Forbes

64% of respondents around the world— and 74% of those in the U.S.— feel that adhering to compliance requirements is a 'very' or 'extremely' effective way to keep data secure.

Source: Thales Survey


Best Practice
7
IoT Security

Best Practice #7: IoT Security

Careful Consideration of IoT and OT Environment

With the number of IoT devices expected to surpass 20.4 billion in 2020, the attack surface continues to expand. From vulnerable healthcare devices to video cameras involved in DDoS attacks, to self-driving cars taken over by hackers, the implication of IoT breaches have far-reaching effects into every aspect of our lives. 5G deployments will only exacerbate the problem as it will lead to more widespread outdoor deployments of IoT, such as dense sensor networks for agriculture optimization.

Addressing IoT security involves adopting many of the best practices in this eBook with specific refinement for IoT:

- **Policy:** The best practice for IoT and OT devices is to deny all traffic to and from the device UNLESS it is to an authorized host AND using an authorized protocol/application.
- **Segmentation:** Ensure groups of IoT devices (e.g. healthcare infusion pumps, surveillance cameras, HVAC systems) are isolated in their own secure network segment. Different IoT device categories carry different security risks so do not lump all IoT devices together in a single network segment

61% of organizations have experienced an IoT security incident.

Source: CSO Online

*IoT devices experience an average of **5,200 attacks** per month.*

Source: Symantec

*It takes **3 minutes** to hack an IoT device but **6 months** to discover the breach.*

Source: Gartner

***5% of IoT devices** deployed today are segmented; however, by 2021 **60%** will be.*

Source: Gartner

Best Practice

8

AI/ML and Emerging Technologies

Best Practice #8: AI/ML and Emerging Technologies

New Frontier in Tackling CyberSecurity

As the sheer volume and frequency of cyberattacks increase, emerging technologies, such as artificial intelligence and machine learning (AI/ML) offer a glimmer of hope.

Unlike humans who find it challenging to process and act upon vast quantities of data, ML/AI can process, identify and respond to security breaches faster and more efficiently. Machines can also automate processes and pro-actively help find anomalies before they become major issues, unlike humans who can only react to problems once they have occurred. By gathering and analyzing data in real time, machines can correlate information, identify patterns, learn to predict what may happen next, and act on that information. For example, AI-powered security analytics can remove the constant burden for security analysts by quickly gathering the necessary data and prioritizing the alert based on the risk profile of the threat.

Leverage emerging technologies to:

- Accelerate early identification of and response to threats
- Better process and act on vast amounts of data

Be cautious however for hackers leveraging AI/ML technology (e.g. AI-modeled malware that evades sandboxing or AI-enabled spear phishing that further increases attacks at scale) and always be vigilant in protecting the integrity of data that your AI/ML solution is based on.

*By 2024, AI will be integral to every part of the business, resulting in **25% of the overall spend**.*

Source: IDC

*By 2025, **at least 90%** of new enterprise application releases will include embedded AI functionality.*

Source: IDC

*Humans Plus AI **20X More Effective** in Cybersecurity Defense Than Traditional Methods.*

Source: Forbes

Best Practice

Cloud Security

Best Practice #9: Cloud Security

Multi-Level Approach

As the mass migration to the Cloud continues (business processes, application software, infrastructure software and system infrastructure) so too do security concerns rise – questions regarding unauthorized access, cloud data loss, encryption, cloud backup and more.

The approach to cloud security is no different to that of on-premise security – a layered approach is critical.

Multi-level Cloud Security:

- Extends across Public/Private/Hybrid Cloud
- Ensures data compliance
- Meets Regulatory requirements (e.g. ISO 27001)
- Comprehensive business continuity and disaster recovery plan – including off line backups
- No Continuous Data Protection or mirroring

83% of enterprise workloads will move to the cloud by the year 2020.

Source: Forbes

93% of organizations are moderately to extremely concerned about cloud security CyberSecurity Insiders.

Source: 2019 Cloud Security Report

70% prefer cloud-based NACs where some/all functionality is in the cloud; only 28% of respondents prefer on-premises deployments.

Source: Extreme Survey


Best Practice
10
Security Ecosystem

Best Practice #10: Security Ecosystem

Open Solutions That Interwork With Existing Security Solutions

One of the biggest oversights businesses can make is not recognizing the enormity of the network security challenge or believing they can address it alone. Every year more money is spent on cybersecurity solutions and every year there are more cybersecurity breaches.

A layered approach to network security, one that involves working in conjunction and collaboration with the existing security solutions in your network (firewalls, virus detection, etc.), is essential. Any business investing in network security should ensure that they can integrate seamlessly with their existing security solutions and work with the leading threat intelligence feeds.

Adopt an open ecosystem approach

- Ensure your network is an active participant in the ecosystem
- Where possible deploy integrated and automated threat detection, intelligence, and mitigation
- Avoid proprietary security solutions

*A typical enterprise is evaluating or deploying as many as **75 different** security products to cover the many different aspects of security.*

Source: CSO Online

Conclusion

Network security issues are here to stay. As we become more connected, more mobile, and more cloud-driven, they are only going to increase. The huge security breaches that have hit so many leading companies are clear evidence that the ground rules are changing.

Being a victim of a security breach is never desirable. However what is worse is to be victimized and know that practical, affordable steps could have been taken to either prevent it or contain the damage .

Leverage these Top 10 Network Security Best Practices to bolster your network security.

And reach out to Extreme to learn how our industry leading network security solutions can help.

*It's predicted that by 2021, **100%** of large companies globally will have a CISO position Cybersecurity.*

Source: Ventures

*The cybersecurity unemployment rate is **0%** and is projected to remain there through 2021.*

Source: CSO Online

Advance Your Network Security With Extreme

Extreme Fabric Connect

Hyper-Segmentation

Not a single breach in Numerous Hackathons

ExtremeCloud Security

Only Cloud Vendor with ISO/EIC 27001 Certification

Extreme Control

Secure Network Access

On-Premise

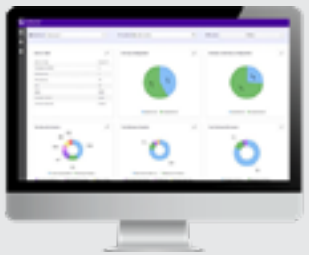
Enhanced Wi-Fi Security

Private Pre-Shared Key for Enhanced Encryption and Data Privacy

Extreme Defender for IoT

Edison Award Winner for IoT Security

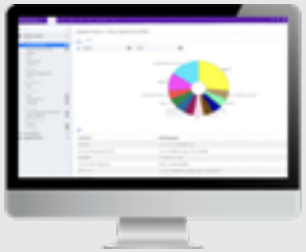
Extreme AirDefense



Advanced Wireless Intrusion Prevention with

2x Signature Library

ExtremeCloud A3



Secure Network Access in the Cloud

Compliance and GDPR

Committed to the Protection and Privacy of Data

Appendix 1: Get the Basics Right

Access controls, password controls, patch management, training, and off-line back-ups all qualify as table-stakes security measures. If you are not doing them, you are increasing your exposure.

- ***Access Controls:*** Firewalls and anti-virus protections are like locks and keys – they may have their limitations however without them, you open the door to increased breaches at a faster rate.
- ***Password Controls:*** Brute force attempts to break passwords —along with phishing—continues to be a prime way that hackers steal data. Stopping repeat attempts and requiring double authentication are proven methods that strengthen security.
- ***Patch Management:*** Regular patch deployment may not halt the backdoor vulnerability discovered 5 minutes ago, but it can help stop upwards of 70% of the attacks you are likely to see on any given day.
- ***Training:*** The "Human", besides representing the target, is also the unaware carrier of cyber-attacks. Many cyber-attacks use social engineering techniques, and cyber criminals adopt increasingly complex methods to bypass the ''Human Firewall'', with the aim of convincing users to perform an action that causes an infection or the dissemination of valuable information. Effective awareness and training not only reduce the number of people that fall victim to attacks but also builds up institutional knowledge that can result in faster detection and remediation.
- ***Off-line Back-ups:*** when ransomware hits, this may be the one security measure, above all others, that you may be thankful for in ensuring business continuity.

Appendix 2: The Mitre Att&ck Defense Framework

The **MITRE ATT&CK** knowledgebase describes cyber adversary behavior and provides a common taxonomy for both offense and defense. It has become a useful tool across many cyber security disciplines to convey threat intelligence, perform testing through red teaming or adversary emulation, and improve network and system defenses against intrusions. The process MITRE used to create ATT&CK, and the philosophy that has developed for curating new content, are critical aspects of the work and are useful for other efforts that strive to create similar adversary models and information repositories. https://attack.mitre.org

18 Indicators of Compromise

A Handy List to Use and Compare With Mitre Att&ck!

1. Unusual outbound traffic patterns
2. Anomalies in privileged account behavior
3. Geographical irregularities
4. Login red flags (failures, unusual time/location)
5. Swells in database read volume
6. HTML response sizes (SQL injection, etc.)
7. Large numbers of requests for the same file
8. Mismatched port/application traffic
9. Suspicious registry or system file changes
10. DNS request anomalies
11. Unexpected patching
12. Mobile device profile changes
13. Bundles of data in wrong locations
14. Compressed archive formats
15. Executable files in/tmp
16. Web traffic with ‘unhuman’ behaviors
17. Web scraping
18. Signs of DDOS activity

Appendix 3: DNS Risks and Vulnerabilities

1. Lock down systems to prevent changes to local DNS settings
2. Lock down systems to prevent the installation and use of 3rd party VPNs
   - Particularly no-split tunnel behaviors
3. Lock down your firewalls to allow DNS queries from local DNS systems only
   - Block outbound port 53 unless it comes from a trusted source (i.e. DNS forwarder)
4. Look for questionable patterns in your DNS logs
   - Queries outside of normal hours
   - Queries that use non-standard naming conventions
   - Long Tail log queries
5. Separate traffic! i.e. IoT, Users, Data Centers
6. Beware of TOR activity! (The Dark Web)
7. Leverage DNS blocking based on known bad hostname lists (e.g. the Steve Black list on github)


Extreme®
networks
WWW.EXTREMENETWORKS.COM