Extreme™
Customer-Driven Networking

9 Enterprise Networking Imperatives for 2018 and Beyond

WHITE PAPER

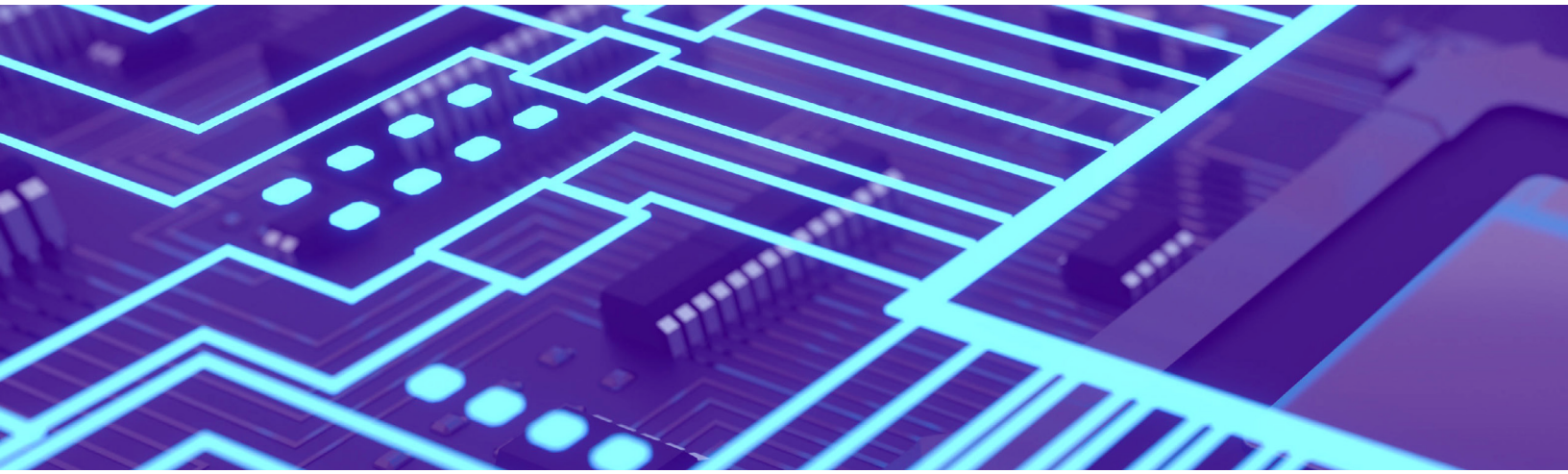

Table of Contents

Network Focuses for the Digital Age

Digital business is here, and networking is fundamental to its success. The modern enterprise demands agility and unending connectivity, and the network is the foundation. As advanced technologies such as automation, machine learning and IoT continue to gain significant traction, staying on top of these trends, and others, will help you make the right strategic decisions around your network to enable digital growth while remaining stable and secure.

1. Network as a Strategic Enabler of Digital Technology

Digital transformation positions enterprises to innovate faster, become more agile and gain competitive advantage in their respective markets.

- Organizations that have embraced digital transformation have seen an average 55% growth in gross margin over a three-year period.
- Organizations that weren't prepared to embrace digital transformation had significantly less margin growth (just 37%) during the same period (Harvard Business School, CIO from IDG)[1].

Digital transformation, driven by the demands to improve customer and user experience, will ultimately redefine networking. To keep pace, networks are going to need to improve with respect to resiliency and dynamism in order to support the speed of business while meeting the demands of end users and customers (Forbes)[2].

Extreme Digital Transformation Perspective for 2018	
✓	Business transformation is intertwined with IT and network transformation. A holistic approach must be considered.
✓	As networking grows more critical to the business, new, simple and agile network architectures will be deployed that don't force trade-offs with security and resiliency.
✓	Machine learning and advanced orchestration systems will ultimately emerge to create a more automated, self-learning and self-healing network environment.

"A well segmented network means that if a breach occurs, it can be contained… the difference between a contained and uncontained breach is the difference between an incident and a catastrophe."

Rob Joyce, Chief of Tailored Access Operations, US National Security Agency

2. Security

Today's network security environment is a virulent one, and high profile breaches are on the rise. No business is safe, as shown by the increasing frequency of major brand name attacks. Here's what the landscape looks like:

- Cybercrime damages worldwide are predicted to cost $6 trillion per year by 2021.
- Hackers are attacking computers and networks nearly constantly, with an average of one attack every 39 seconds.
- The World Economic Forum predicts that cyberattacks will constitute the third largest global threat in 2018[3] (Comparitech).

While malicious actors and their attack methods multiply in frequency and sophistication, the impacts of digital transformation are also creating security implications for the enterprise. In fact, 69% of senior IT and security leaders report that digital transformation is forcing them to make major changes to their security strategy[4] (Forbes and BMC). With increased IoT connectivity, this wider attack surface creates more ways for threat actors to gain access to data, finances and other assets.

This year, uncharted threats are looming, promising new dangers and the resulting security technology challenges. An adversarial machine learning "arms race" is on between attackers and defenders. As more enterprises look to get into the AI and machine learning space, malicious actors will use machine learning themselves to support their own attacks. Threats on critical infrastructure are also on the rise – requiring much more vigilence from governments and corporations who manage this infrastructure. It's also predicted that ransomware will make its way into IoT, penetrating high net-worth users and causing large-scale corporate disruption[5] (CSO from IDG).

Extreme Security Perspective for 2018	
✓	Security compliance will get serious. GDPR is one such example; expect other regulatory bodies to follow suit.
✓	Segmentation of applications and the network is increasingly critical. Properly implemented, end to end segmentation is proven to contain breaches, protect critical data, and prevent lateral movement.
✓	Security should be viewed as an ecosystem and should encompass coordinated multi-layer threat detection, intelligence and mitigation. No one product or vendor can solve the security challenge – it requires coordinated effort.
✓	Security analytics are becoming more sophisticated. The use of machine learning can assist with anticipating and blocking threats more efficiently than humans alone.

3. Analytics and Machine Learning

As networks continue to grow in complexity, lack of visibility and insight into their operations persist. Many vendors offer tools to troubleshoot individual products only in specific parts of the network, compounding the issue of disparate components and limited visibility. A holistic view is critical, but often difficult to achieve with countless devices, applications and services attached to the enterprise network. This is evidenced by the fact that today, 27% of network engineers or architects say they spend most of their time responding to high-priority or emergency issues[6] (McAfee and ESG).

But there's hope. The use of analytics and machine learning to predict and prevent network failures is on the rise. Guesswork is becoming a thing of the past as greater effort is made to develop highly effective predictive analytics tools to allow staff to remedy specific issues before the network is affected[7] (CIO from IDG).

By 2021, over 50% of enterprise infrastructure will use some form of cognitive and artificial intelligence to reduce costs, enhance efficiency and manage risk[8] (Network Computing). Security software solutions continue to incorporate machine learning to a greater degree, while log analytics tools regularly make use of machine learning, both to enhance troubleshooting capabilities and prevent security problems before they come to pass.

Extreme Machine Learning and Analytics Perspective for 2018	
✓	• **The use of machine learning to predict and prevent security breaches is becoming more prevalent**. • 12% of organizations have deployed machine learning technology for security analytics and operations extensively, while 27% have done so on a limited basis[6], and the adoption rate will continue to increase.
✓	• **The use of machine learning intelligence targeted directly at IT operations and support is also emerging to assist over-tasked IT professionals.** • One particular use case to keep an eye on is RF management in wireless networks.

4. Automation

Network operations are often executed manually, device by device, using the command line interface. This manual entry of commands by humans often results in outages as a result of misconfigured network devices. Further, it can take weeks to make network configuration changes in order to support new applications.

- By 2021, over 25% of infrastructure services will include autonomous, self-managing capabilities to expedite business outcomes and reduce the risk of human error.[9]

The objective behind automation is really to generate autonomous processes, allowing the network to execute on essential activities without human intervention. Now that the technology components needed to make automation possible have reached high levels of maturity, the sky is the limit[10] (Light Reading). Integrating automation tools into network operations can accelerate workflows and automate manual processes, helping your networking team focus on more strategic projects.

- Two-thirds of organizations report that the automation of security analytics and network operations is a major priority.[6]

Extreme Automation Perspective for 2018	
✓	• **Network fabrics are proving to be effective components of network-wide automation, reducing manual provisioning and simplifying network operations.** • ...and they're being used more broadly within the network. Network Fabrics started out in the data center, but they're emerging with increasing frequency in the campus network to deal with the complexity driven by IoT.
✓	**Comprehensive management and orchestration platforms will continue to get more sophisticated and will be integrated with machine learning technologies to provide automated remediation based analytics and insights.**

5. IoT Security and Management

IoT growth is exploding across most industries, particularly in retail, healthcare and industrial/supply chain[11] (Forbes).

- 54% of organizations have somewhat incorporated IoT into business operations
- 13.8% of organizations have incorporated IoT into business operations to a significant degree

Retail is an obvious fit for IoT, with most retailers aiming to increase direct connections with customers, expand branding efforts and personalize the customer journey. Healthcare and manufacturing are following retail closely, with their sights set on connecting with patients using wearable devices, or tracking products from factory to floor.

It's important to note, advanced analytics and machine learning are well poised to help manage the fragmentation and widespread adoption of IoT, as well as potential security concerns. Much of the difficulty with IoT lies in finding a systematic method for collecting, storing and analyzing the data it generates, whether to improve processes or achieve other business goals[12] (SAS).

When it comes to IoT security, the problem spans a number of areas. First, there's sheer volume. At present, there are more IoT devices on the planet than there are people. Second, mass production of low cost IoT devices is taking place daily, but many of these devices lack inherent security. And to make matters worse, there's no central body of authority for regulating IoT security. But that's not to say that zero efforts are being made—the Open Connectivity Foundation, an industry group focused on developing IoT standards was founded in 2016, and the technology community at large certainly recognizes the problem, but it's a long way from being solved.

These initial issues lead to the business implications: IoT devices create endpoints, which means more avenues for access into your network, and we've already seen the consequences:

- In September 2017, multiple major DDoS attacks were delivered using the Mirai worm that infected IoT devices, including the website of security journalist Brian Krebs, who suffered a 600+Gbps DDoS attack. Only two days later, OVH, a French hosting company, reported a 1Tb Gbps DDoS attack[13] (Verizon).
- Additional IoT DDoS malware attacks took place in October and November of 2017, targeting DNS provider DYN and Deutsche Telekom a little over a month later.

Extreme IoT Security and Management Perspective for 2018	
✓	• **A marked increase in spend on IoT management and security products will take place.** • As more IoT devices are manufactured and connected, the need for management and security products increases.
✓	• **Solutions that automate secure IoT device on-boarding and then use segmentation to isolate IoT devices should be evaluated.** • Businesses using IoT devices need to focus on reducing the attack surface by placing IoT traffic and devices into isolated zones. Centralized management and policy-based control is also key in order to deploy IoT devices faster and more securely.
✓	• **Enabling analytics to gather data on IoT devices bring invaluable business opportunities.** • Monitoring asset usage, location and performance can help you make decisions that optimize capital investments.

6. Wireless

Given that all businesses rely on uninterrupted, unending connectivity, wireless is everywhere today, and it's increasing as a form of access at an unprecedented rate. IoT is a major contributor to wireless growth as the vast majority of IoT devices are connecting via wireless.

Historically, we've relied on 802.11ac, the most recent standard for Wi-Fi. However, 802.11ax (High-Efficiency Wireless), the next evolution of wireless, is fast approaching, expected to be finalized in early 2019. The 802.11ax standard will deliver a projected fourfold increase in average throughput per user[14] (Network World), designed for high-density public environments. This will extend an increase in programmability, automation and even machine learning capabilities that can be applied to wireless networks to help simplify operations.

But why are simplified operations needed? 60% of participants in a ZK Research study said they spend at least a quarter of their time doing nothing but troubleshooting Wi-Fi issues. Consider a typical 40-hour work week: that adds up to 10 hours of time dedicated to finding and fixing Wi-Fi problems[15] (Network World).

The other major shift taking place in the wireless space is the evolution to cloud. Hybrid strategies will quickly become the norm, which allow a combination of private cloud/on-premise solution and public cloud solutions. An example being a healthcare provider that has an on-premise solution for its main hospitals but wants to leverage the public cloud to interconnect their remote clinics and doctors offices.

Extreme Wireless Perspective for 2018	
✓	Oganizations should start evaluating 802.11ax solutions, especially those expecting growth in WiFi traffic.
✓	Organizations should consider investing in WiFi solutions that provide investment protection and common hardware for on-premise, cloud and hybrid cloud implementations.
✓	WiFi solutions that leverage machine learning capabilities to automate user experience and/ or back end operations should be investigated to reduce amount of time spent troubleshooting.

7. Edge Computing

Edge computing is a major development on the rise due to the growth of IoT and sensors. Essentially, edge computing can be described as a the migration of compute to the pheriphery of the network, away from centralized points, to decrease the volume of data that must travel from the device/sensor to the server, as well as, the distance that data must travel. This in turn reduces transmission costs, shrinks latency, and improves QoS[16]. Ultimately, the speed of gathering and sharing large amounts of data is expedited significantly.

45% of all data created by IoT devices will be stored, processed, analyzed and acted upon close to or at the edge of a network by 2020 (IDC)[17].

Extreme Edge Computing Perspective for 2018	
✓	As compute becomes more dispersed across the organization, organizations must evaluate networking technologies optimized for east/west traffic flows and/or meshed communications.
✓	As edge computing becomes common-place – many of the network functions such as firewalls, IDS/IPS, etc. Typically housed in enterprise Data Centers – will also move closer to the network edge.

8. Cloud, Multi-Cloud, and Infrastructure as a Service

The dominance of the cloud, hybrid IT strategies and multi-cloud services certainly aren't going anywhere, and they're heavily influencing the way the enterprise network is delivered. While trends like edge computing and digital transformation continue, cloud and hybrid IT make more sense than ever.

Infrastructure as a Service is becoming the preferred method for delivering IT resources such as compute, storage and networking given the benefit of unmatched scalability. Users are able to demand resources as needed, making it easy to provision temporary or unpredictable workloads. IaaS is also further enabling automation capabilities.

Multi-cloud connectivity offers customers the flexibility to mix and match cloud technologies and services from different vendors to suit their exact needs. These can be multiple public clouds, multiple virtual or on-premise private clouds, multiple managed or unmanaged clouds, or a mix of them all. Ultimately, enterprises' applications and data are becoming more and more spread between in-house platforms, IaaS, SaaS and edge IoT (The Enterprises Project).[18]

Extreme Cloud Perspective for 2018	
✓	Hybrid cloud deployments will increase rapidly and become more common.
✓	Solutions that can support on-premise, cloud-managed or any mix with a common hardware will help enterprises with their hybrid IT goals.
✓	Connectivity to multiple cloud providers will be commonplace; therefore, APIs and integration with multiple cloud service providers will be increasingly important.

9. Virtual Network Operating Systems and Containers

Containerized applications will be front and center this year as their use cases continue to expand.

Virtualization largely paved the way for container technology, based on the concept of decoupling applications from underlying hardware (InfoWorld from IDG)[19]. Container technology providers greater deployment flexibility overall beyond the fundamentals of virtualization.

In comparison to Virtual Machines, Containers are a significantly lighter weight method for running applications and services since multiple containers can share a single OS. Therefore, it is possible to run six to eight times as many containers as VMs on the same hardware. Due to the cost savings and efficiency advantages, many enterprises are investing in container technology.

- **44% of IT professionals** rank containers as the most important technology priority today.
- **38% of IT professionals** rank containers as the most important technology priority three to five years from now (SolarWinds)[20].

What's changing is where container technology is being deployed. While containers have been used within the Data Center for hosting applications as well as Virtualized Network Functions (NFV) – the technology is now making its way closer to the edge of the network in support of the emerging edge computing paradigm.

Extreme Virtual Network Operating Systems and Containers Perspective for 2018	
✓	Networking vendors will move to ensure that their network operating system can run within a container based framework.
✓	Standard hardware (white-box, brite-box or even compute platforms) capable of running the Network Operating System as well Virtualized Network Functions (ie. firewalls, IDS/ IPS, etc) will emerge in the enterprise network.

Conclusion: Stay Ahead of the Networking Imperatives of 2018

With the enterprise network becoming more and more critical to the success of your business, there's no better time to be prepared to evaluate the technologies that will set you up for success as digital transformation continues to progress.

Where are you in your digital transformation, and what have you done to modernize and optimize your network? We can help.

Interested in exploring how to improve the strength and efficiency of your network? Let's chat. Visit https://www.extremenetworks.com/contact/ or call (888) 257-3000 to speak to a networking solutions expert today.

References

1. Boulton, C. (2016, September 21). 'Digital laggards' must harness data or get left behind. Retrieved April 12, 2018, from https://www.cio.com/article/3122806/it-industry/digital-laggards-must-harness-data-or-get-left-behind.html?nsdr=true
2. Bae, H. (2017, December 18). Digital Transformation And The Future Of The Network. Retrieved April 12, 2018, from https://www.forbes.com/sites/forbestechcouncil/2017/12/18/digital-transformation-and-the-future-of-the-network/#1c1e65ed524c
3. "100 Terrifying Cybercrime and Cybersecurity Statistics & Trends [2018 EDITION]." Comparitech. Accessed April 11, 2018. https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/
4. Industry report: Enterprises Re-engineer Security in the Age of Digital Transformation. Forbes Insights & BMC. Retrieved March 29, 2018, from http://www.bmc.com/forms/DCA-SecOps-ForbesSecOpsReport-Q3FY17.html
5. Garside, Debbie, and IDG Contributor Network. "Cybersecurity Trends for 2018." CSO Online. December 08, 2017. Accessed April 11, 2018. https://www.csoonline.com/article/3241122/cyber-attacks-espionage/cybersecurity-trends-for-2018.html
6. Industry report: Automation and Analytics versus the Chaos of Cybersecurity Operations. Enterprise Strategy Group & McAfee. Retrieved March 29, 2018, from https://www.mcafee.com/us/resources/reports/rp-esg-security-ops-and-analytics.pdf
7. Edwards, J. (2017, July 17). Predictive analytics: Your key to preventing network failures. Retrieved March 29, 2018, from https://www.cio.com/article/3207569/predictive-analytics/predictive-analytics-your-key-to-preventing-network-failures.html
8. 6 Hot Tech Trends That Will Impact the Enterprise in 2018." Network Computing. January 02, 2018. Accessed April 11, 2018. https://www.networkcomputing.com/data-centers/6-hot-tech-trends-will-impact-enterprise-2018/755072649
9. Industry report: IDC Futurescape: Worldwide Enterprise Infrastructure 2018 Predictions. November 30th, 2017. Accessed April 11, 2018 from http://technodocbox.com/Data_Centers/71927796-Idc-futurescape-worldwide-enterprise-infrastructure-2018-predictions.html
10. The Autonomous Network Is the Endgame for Telecom. (n.d.). Retrieved April 11, 2018, from https://www.lightreading.com/automation/the-autonomous-network-is-the-endgame-for-telecom/a/d-id/735860
11. Newman, Daniel. "The Top 8 IoT Trends For 2018." Forbes. January 29, 2018. Accessed April 11, 2018. https://www.forbes.com/sites/danielnewman/2017/12/19/the-top-8-iot-trends-for-2018/#4f829b1267f7
12. Applying Machine Learning to IoT Data." SAS. Accessed April 12, 2018. https://www.sas.com/en_us/insights/articles/big-data/machine-learning-brings-concrete-aspect-to-iot.html
13. Industry report: Verizon's 2017 Data Breach Investigations Report. Verizon. Retrieved March 27, 2018, from http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/
14. Kerravala, Zeus, and Network Intelligence. "AI Can Be a Game Changer for WI-Fi Management." Network World. March 27, 2018. Accessed April 11, 2018. https://www.networkworld.com/article/3266585/wi-fi/ai-can-be-a-game-changer-for-wi-fi-management.html
15. Gold, Jon. "Wi-Fi 2018: What Does the Future Look Like?" Network World. November 29, 2017. Accessed April 12, 2018. https://www.networkworld.com/article/3237146/lan-wan/wi-fi-2018-what-does-the-future-look-like.html
16. Christ, Andre "Built to Last: Laying a Framework for IoT with Enterprise Architecture" Datanami. April 3, 2018 https://www.datanami.com/2018/04/03/built-to-last-laying-a-framework-for-iot-with-enterprise-architecture/
17. IDC.com IDC Table of Contents. (n.d.). Retrieved April 12, 2018, from https://www.idc.com/research/viewtoc.jsp?containerId=US40755816
18. 5 cloud computing trends for 2018. (2017, December 28). Retrieved April 14, 2018, from https://enterprisersproject.com/article/2017/12/5-cloud-computing-trends-2018
19. Wang, C. (2017, June 29). What is Docker? Linux containers explained. Retrieved April 12, 2018, from https://www.infoworld.com/article/3204171/linux/what-is-docker-linux-containers-explained.html
20. Industry report: IT Trends Report 2018: The Intersection of Hype and Performance. SolarWinds. Retrieved April 11, 2018, from https://www.solarwinds.com/company/press-releases/2018-q2/solarwinds-study-of-it-professionals-finds-cloud-computing-is-top-transformative-technology-and-main-cause-of-mounting-performance-challenges