Ensuring Information Security in a Digital World
How to Choose the Right Solutions for Your Business
## Table of Contents

<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Introduction</td>
</tr>
<tr>
<td>4</td>
<td>Chapter 1: What does a secure, digital-ready IT network look like?</td>
</tr>
<tr>
<td>7</td>
<td>Chapter 2: What should a digital-ready security solution offer?</td>
</tr>
<tr>
<td>10</td>
<td>Chapter 3: What should I look for in a solution provider?</td>
</tr>
<tr>
<td>15</td>
<td>Conclusion</td>
</tr>
</tbody>
</table>
Introduction

Companies today depend on technology and data to drive everything from decision-making to customer service. As more and more employees rely on laptops, smartphones, and tablets to stay productive in or out of the office, the demands for secure mobile access are higher than ever. At the same time, machines, processes, sensors, and systems also require uninterrupted access to data to support everyday business operations.

With collaboration on the rise, organizations need to rethink information security. The need to share data across the public Internet—combined with inadequate visibility, poor control of end-user devices, and recurring threats like phishing and ransomware—have created some serious security challenges for companies everywhere. While digital transformation is reshaping business, it is also expanding the attack surface across IT networks. According to a recent study, nearly one out of three IT leaders remains unconvinced that their security regimes are adequate.1

Faced with limited IT staff and lean budgets, mid-sized businesses in particular need simple and cost-effective ways to protect their company and assets. They need security solutions that gather comprehensive insights across the network—insights that inform a course of action based on analysis, identification, and packaging of threats. With these security solutions in place, IT pros can access real-time data to quickly analyze and act on security incidents in their network environments, before customer experience or company reputation is negatively impacted.

In this guide, we explain how the right security solutions enable organizations to better protect their networks and reduce the burden on in-house security management teams. Choosing a partner with a security-first approach helps companies protect their networks, become proactive in a complex threat landscape, and drive their digital future.
What does a secure, digital-ready IT network look like?
In a digital-first world, IT pros are expected to enable organizations to embrace new technologies like the Internet of Things (IoT), artificial intelligence, and big data.

While strapped for time and resources, they need to monitor multiple layers of network protection and prepare for emerging threats like cryptocurrency attacks and software supply chain attacks. This job becomes even more challenging as companies shift workloads to the cloud and uncover new things that need to be secured—web gateways, hosted email, and identity and access management.

A snapshot of today’s threat landscape:

- **Total ransomware** grew 56% in the past year.\(^2\)
- **176 new cyber threats** occur every minute, almost three every second.\(^3\)
- The number of **new malware samples** grew to 638 million, while total mobile malware grew 99%.\(^3\)

With organizations sharing reams of data and deeply personalized content with end-users across multiple platforms, the level of anxiety around potential exposure and the risk of a data breach is rising. And with the digital economy dramatically increasing the types and sources of digital requests from APIs, mobile apps, cloud, and customer and partner ecosystems, companies need to rethink their security strategies. A homogenous approach to security, where all information is protected and shared in the same way, can no longer sufficiently address the unique needs of each business operation.

As a result, companies today need security solutions that enable complete visibility across networks and allow risk management and response decisions to be made in real time. In a data-saturated world, security policy monitoring and enforcement strategies need to move closer to the digital edge, allowing you to more effectively mitigate user errors, threats, and hacking attempts. For IT pros, it’s critical to ensure that security policies are applied in a programmable fashion so that threats can be captured, analyzed, and removed within the packet flow before users are impacted.
As network environments get more interconnected and maintenance demands become more complex, IT pros are looking to avoid the hassle of managing a range of security products from numerous vendors. By choosing security-focused solutions from a single provider—with uninterrupted visibility across the network—they can use things like localized boundary control and packet inspection to avert potential security disasters before they begin. Plus, they can implement security strategies in a way that can’t be circumvented, making their network truly digital-ready.

The best security solutions help a business:

- **Ensure business resiliency**: Help them stay operational, even when disaster strikes; a data breach can often drive a company out of business. The average cost of a business data breach totals around $3.6 million.\(^4\)

- **Gain complete visibility**: Provide a clear view into their security environment through a streamlined portal or management console.

- **Reduce the exposure of multiple potential intrusion points**: Stay secure with solutions from a single vendor, because juggling solutions from multiple vendors creates gaps where attacks can be launched.
What should a digital-ready security solution offer?
Companies today spend considerable time and resources improving their IT security measures, trying to prevent the kind of attacks that can set a business back months or years, if not drive it into the ground.

Most IT and business decision-makers wrestle with multiple challenges on an everyday basis. How can you better manage your network and infrastructure? How can you spend less time managing your network security? How can you spend more time building your business?

The answers lie in deploying security solutions that can efficiently and effectively manage ongoing security tasks so you can use your resources for more important projects.

Mid-sized businesses in particular often have fewer resources to devote to combating cyber threats, making them an increasingly attractive target for bad actors. When these companies try to speed up their growth trajectory by adding offices or locations, upgrading bandwidth, or migrating to hybrid environments, they can avoid the additional security concerns that come with physical and virtual expansion by partnering with a full-service network security solutions vendor.

In today’s threat landscape, effectively fighting malicious attacks requires continuously monitoring all the elements of your infrastructure, correlating security events for meaning, and analyzing the outcomes to extract key data and prioritize action. When mid-sized companies train their sights on embracing newer technologies such as IoT devices—which are notoriously vulnerable and encompass a multitude of network endpoints that are susceptible to attack—IT pros need to be constantly vigilant that every device across the network remains secure.

Mid-sized businesses can avoid additional security concerns by partnering with a full-service network security solutions vendor.
To make life easier for them, IT pros can hugely benefit by relying on an experienced solutions vendor like CenturyLink to provide integrated approaches for managing and monitoring infrastructure and to make sure that no security loopholes remain. The best security-focused solutions are those that leverage automation in combination with rigorous human review by security experts, so that organizations can stay ahead of security threats while simplifying management. By choosing solutions that enable comprehensive visibility and 24x7 network monitoring, in-house IT teams at mid-sized companies can free themselves from day-to-day network monitoring tasks and focus on core business initiatives and growth.

**What are the must-haves for digital-ready security?**

The right security solutions should be designed to handle the entire attack lifecycle, from preventive services, proactive detection, containment, and incident response services to global threat intelligence and deep analytics. Make sure the solutions offer:

**Expertise:** Look for a solution that offers individualized consulting expertise to evaluate your regulatory environment, risk profiles, and business priorities to build an optimal security program. With CenturyLink, a team of proven security experts will work closely with you to uncover areas of high risk in your organization, identify security gaps, and prioritize your network security efforts.

**Visibility:** Look for dashboards that enable organizations to easily visualize their security postures, gain insight into threat patterns, and enable more accurate decision-making for faster incident response. CenturyLink monitors over 114 billion NetFlow sessions and 1.3 billion security events every day, responding to and mitigating roughly 120 DDoS attacks daily and removing approximately 35 command and control (C2) networks per month. This heightened visibility enables customers to better anticipate and protect against threats.

**Monitoring:** Look for a solution with 24x7 security operations centers to provide always-on monitoring and incident response. CenturyLink® Security Log Monitoring collects and tracks incidents in real time around the clock, applies advanced analytics, categorizes them, and sends them to an expert team for review. Teams then investigate the potential threats and prioritize events into the top incidents that require greater analysis or immediate action.
What should I look for in a solution provider?
For most mid-sized companies, it just makes better sense to find a partner who can support you across all your network security needs, instead of dealing with the expense and inconvenience of implementing those solutions on your own.

From the complexity of configuring disparate solutions to the time commitment and expertise needed to monitor them for vulnerabilities, you can avoid a lot of headaches by letting a reputable network security solutions provider keep your business protected and running.

It’s important to know that the provider can:

- **Deploy holistic solutions:** Deliver protection through both hosted and network-based security measures along with specific consulting disciplines.

- **Provide continuous network monitoring:** Support proactive and real-time notifications to keep your business protected at all times.

- **Offer customizable management:** Provide co-managed, fully-managed, or custom solutions based on your business needs and risk tolerance, all delivered by a single provider.

- **Enable a streamlined network security environment:** Give IT pros the tools and visibility they need to simplify network management and move from a reactive to proactive security stance.
Lean on the security experts at CenturyLink

CenturyLink’s solutions are designed with security in mind, so businesses like yours can stay ahead of ever-evolving cyber threats. Our experts will work with your team to find the right solutions for your specific needs. With CenturyLink, you can lower your cybersecurity risks and protect your critical business assets with flexible IT security solutions that maximize your time and budget.

CenturyLink allows customers to:

- **Rely on CenturyLink’s experts rather than finding and training specialized in-house security professionals.**
- **Benefit from continuous monitoring and real-time incident response through CenturyLink’s 24x7 security operations centers.**
- **Leverage CenturyLink’s investment in costly and sophisticated tools so they don’t have to.**
- **Use fully integrated security solutions from a single source for multiple technology endpoints.**
- **Provide the foundation for a holistic and secure IT ecosystem.**
What can CenturyLink offer my business?

CenturyLink offers a range of network and infrastructure security solutions, based on the size of the organization.

Organizations with less than 250 employees:

Smaller organizations—or those struggling with limited budgets and/or in-house security expertise—may want to consider:

- **Cisco Meraki Cloud-Managed Security**: A comprehensive Unified Threat Management (UTM) solution that simplifies protection of your entire business through a suite of tools that provide cloud-based management and enhanced reporting. Since the solution is 100% cloud managed, installation and remote management is simple.

- **WorkWise**: Cybersecurity awareness training and phishing simulation that empowers employees to become your organization’s strongest line of defense.

- **SD-WAN**: An SD-WAN solution that makes it easy to keep your network secure, whether you have one location or multiple branches, by providing consistent security measures across your business. CenturyLink has the capabilities to fully manage and monitor your networks and save IT time.

- **Fiber+**: A reliable, high-performance internet connection that maintains availability of your network-based security solutions. Fiber is typically more secure than the competition.

- **Managed Office (MO)**: Bundled data, voice, and business applications with end-to-end management for companies of all sizes.
Larger organizations—or those needing stronger data protection, network management, and/or compliance—may want to consider Cisco Meraki Cloud-Managed Security, SD-WAN, and Managed Office (MO) as well as:

- **Cisco Meraki Cloud-Managed Security**: A comprehensive Unified Threat Management (UTM) solution that simplifies protection of your entire business through a suite of network services that provide cloud-based management and enhanced reporting. Ideal for larger organizations with distributed sites, campuses, or data center VPN concentrations. Since the solution is 100% cloud managed, installation and remote management is simple. Also includes anti-malware, content filtering, web search filtering, and geo-IP-based firewalling.

- **Managed Security Service**: Integrated security monitoring and analysis services on a fully managed platform, allowing access to real-time data for identifying security incidents.

- **Security Log Monitoring**: Services that go beyond monitoring, including collecting incidents, categorizing them by severity, and prioritizing events that require action. CenturyLink Security Log Monitoring provides insight into our findings via our customer portal, enabling immediate analysis and response. Dig deeper into log data with intelligence from community feeds, social media, dark web, honey pot infection records, and third-party research—all with no additional equipment or licensing fee requirements.

- **SD-WAN**: Gain insight and control of all of your network connections and protect your customer and employee applications with granular, automated policies for access control, redundant failover, and end-to-end packet monitoring.

- **Ethernet**: A natural extension of your office network across town, or across the globe via private, dedicated connectivity to your locations, data centers, and cloud-based services. Experience dynamic bandwidth scalability up to 3x your current capacity and an enhanced portal that provides full network analytics and software-defined control. Customers may automate, schedule, or ‘activate now’ when needed, scheduled or ad-hoc, to adapt network resources to changing demands.

- **Managed Office (MO)**: Bundled data, voice, and business applications with end-to-end management for companies of all sizes, though frequently used by larger organizations with more to manage. Also provides enhanced protection via DDoS mitigation, managed firewall, and network-based security.

---

**Organizations with 250 or more employees:**

Larger organizations—or those needing stronger data protection, network management, and/or compliance—may want to consider Cisco Meraki Cloud-Managed Security, SD-WAN, and Managed Office (MO) as well as:

- **Cisco Meraki Cloud-Managed Security**: A comprehensive Unified Threat Management (UTM) solution that simplifies protection of your entire business through a suite of network services that provide cloud-based management and enhanced reporting. Ideal for larger organizations with distributed sites, campuses, or data center VPN concentrations. Since the solution is 100% cloud managed, installation and remote management is simple. Also includes anti-malware, content filtering, web search filtering, and geo-IP-based firewalling.

- **Managed Security Service**: Integrated security monitoring and analysis services on a fully managed platform, allowing access to real-time data for identifying security incidents.

- **Security Log Monitoring**: Services that go beyond monitoring, including collecting incidents, categorizing them by severity, and prioritizing events that require action. CenturyLink Security Log Monitoring provides insight into our findings via our customer portal, enabling immediate analysis and response. Dig deeper into log data with intelligence from community feeds, social media, dark web, honey pot infection records, and third-party research—all with no additional equipment or licensing fee requirements.

- **SD-WAN**: Gain insight and control of all of your network connections and protect your customer and employee applications with granular, automated policies for access control, redundant failover, and end-to-end packet monitoring.

- **Ethernet**: A natural extension of your office network across town, or across the globe via private, dedicated connectivity to your locations, data centers, and cloud-based services. Experience dynamic bandwidth scalability up to 3x your current capacity and an enhanced portal that provides full network analytics and software-defined control. Customers may automate, schedule, or ‘activate now’ when needed, scheduled or ad-hoc, to adapt network resources to changing demands.

- **Managed Office (MO)**: Bundled data, voice, and business applications with end-to-end management for companies of all sizes, though frequently used by larger organizations with more to manage. Also provides enhanced protection via DDoS mitigation, managed firewall, and network-based security.
Conclusion

Your business can’t afford a security breach. What are you doing to help your cybersecurity teams— who are already stretched thin—mitigate the billions of emerging security threats? You need a partner who’s solely invested in ramping up your company’s digital capabilities and strengthening its security infrastructure.

Let CenturyLink take care of all your network security needs with solutions that are designed for your organization, so that your in-house IT team can focus on helping your business adapt to a digital future.

Ready to take the next step?
Go to the CenturyLink Business Home Page to find the Security and Network Solutions that are right for your organization.