WHITE PAPER

# Security-only networks help limit exposure

Cyberattacks are one of the greatest threats facing global businesses today. Hardly a day goes by that there is not a report of hackers breaching company networks and stealing sensitive customer or personal data.

ADT® Commercial

## Data breaches are on the rise

According to Identity Theft Resource Center (ITRC), there were 1,579 known data breaches in 2017, an increase of more than 44.7 percent over 2016. Cybercriminals are not discerning in where they attack, targeting everything from retailers to financial services to healthcare.[1]

The risk is real for all types of public and private organizations. In just the first half of 2018, companies disclosing data breaches included Exactis (340 million records breached), Under Armour (150 million records breached), MyHeritage (92 million records breached), Facebook (87 million records breached), Panera (37 million records breached), Ticketfly (27 million records breached), Sacramento Bee (19.5 million records breached) and Saks Fifth Avenue and Lord & Taylor (5 million records breached). The diversity in this small sampling drives home the fact that no organization is beyond the reach of cybercriminals.

**1,579**

known data breaches

in 2017

**44.7%**

increase from 2016

### A national problem

To emphasize just how serious the threat of cyberattacks are becoming, presidential executive orders have been signed urging companies to share cybersecurity threat information with one another and the federal government.[2] Industry trade associations have also joined the fight against cybercrime, with the Retail Industry Leaders Association (RILA) Board of Directors recently supporting a comprehensive, collaborative and sustainable plan. This effort will address challenges which include enhancing existing cybersecurity and privacy efforts, as well as opening a dialogue with the general public to build and maintain consumer trust.

[1] Verizon 2017 Data Breach Investigations Report.

[2] Former President Barack Obama signed the executive order in 2015.

## Emerging trend: separate networks

In response to the threats presented by cybercriminals, many organizations are physically separating their IT infrastructure from their networks based on their primary usage in order to limit exposure. A prime example is creating a separate network to run physical security applications—a network apart from those used for other critical business processes. A physical security-only network is typically used to host a company's security devices such as intrusion detection, video, access control devices and related infrastructure.

Separate networks

### Benefits of a separate security-only network

The benefits of a dedicated security-only network are multi-faceted: a security-only network delivers a high level of protection and offers faster speeds, more bandwidth with easier access for loss prevention and security teams—while not impacting business critical systems. Deploying a standardized implementation across multiple locations can often be a lower cost alternative to traditional networks.

Further benefits to a security-only network include nearly unlimited access for applications, such as the remote monitoring of video or conducting remote investigations. This provides investigators with immediate access to video and supporting data to reduce travel, associated expenses, and the overall time it takes to conduct investigations.

When the security-only network is monitored by a certified third-party provider, added benefits include advanced alerts of potential system failure or attempted breach of the network. The monitoring company can also ensure that the network has the latest network security protocols and anti-virus software at all times.

## Should you consider a security-only network?

Any type of organization looking to provide a safer and more secure physical environment for its employees, guests and assets while maintaining a higher level of security is a candidate for a dedicated security-only network. When determining if this type of network is a viable option, it is important to consider a company's internal IT resources in the evaluation and assessment of needs and requirements including security.

### Selecting a third-party provider

When considering a third-party provider for security-only networks, traditional IT companies that plan and implement standard networks may not be your best option. Selecting a company that has the proper certifications for customizing networks as well as deep industry knowledge of the security devices running on the network and how they need to work together will greatly enhance the overall end result.

Certifications such as Cisco Cloud and Managed Services Express Partner, Meraki, Sonicwall and security product-specific certifications will help to ensure successful system integration. Cisco Cloud and Managed Services Express Partner Certification recognizes companies that have attained the expertise in the planning, implementing and supporting of cloud or managed services based on Cisco platforms.

**ADT Commercial is a certified security professional**

CISCO Premier Partner

CISCO Meraki
Cloud & Managed Services Express

paloalto NETWORKS
MSSP Silver

FORTINET
Platinum MSSP

Certified SONICWALL
Platinum MSSP

## Steps to consider when customizing a security-only network

One of the first steps is to identify the circuit requirements for the security-only network. Understanding what type of applications are going to be running on the network and how much bandwidth and speed are necessary to support the applications is key. Security-only networks are often based on commodity broadband, so it is important to ensure that the carrier can deliver reliable service and speed at any given location. It can be a challenging task trying to determine which carrier provides the best and most cost-effective solution. Your third-party provider can help identify the best solution among the available options in your area as well as procure and provision the circuit for optimum throughout.

Bandwidth and broadband speed

VPN access availability

Once the network parameters of adequate circuit bandwidth are determined, additional considerations that should be incorporated into the system include remote (VPN) access, appropriate security measure and rules. At a minimum, there should be a strict password update rule for the duration of password life and passwords re-used from the past. Ideally a consolidated security identification system should be established to ensure continuous monitoring of access with biometric or other proven security solutions as part of any access to the network.

Appropriate security measures and rules

Rules for password lifespans

Consolidate security identification system

If any part of the network is wireless enabled, appropriate security for network access and ongoing traffic monitoring are essential. If they are not part of the system, monitoring is needed to make sure that no additional devices with wireless capability are installed on the system.

Firewall protection is essential. With the advent of IPv6 and its inclusion in networks, there is potential for a security breach when tools designed for IPv4 are faced with IPv6 calls.

Firewall protection

Continuous monitoring should be undertaken for abnormal network traffic, behavior or attempted unauthorized access. When discovered, rules for appropriate notification and/or lockout must be determined and then enforced.

Ongoing traffic monitoring

## ADT Commercial security-only networks

ADT Commercial operates two Network Operations Centers (NOCs) as part of our Integrated Solutions Division. The centers employ a team of Cisco Meraki Certified professionals. This team also holds the Cisco Cloud and Managed Services Express Partner Certification, making ADT Commercial one of the few security system integrators to hold this designation. In addition, our team also holds the following designations: Fortinet Platinum MSSP, Palo Alto Silver MSSP and Sonicwall Platinum MSSP.

Our NOCs are primarily focused on providing real-time monitoring of IT-sensitive systems, including up/down status and network performance metrics. In addition to monitoring systems for performance and potential problems, the NOCs also plan, install and commission LAN/WAN networks for companies that either do not have the internal resources to accomplish this in-house or for those who want a dedicated security-only network. The addition with Cisco Cloud and Managed Services Express Partner Certification delivers a new level of capabilities and expertise to the NOCs in this growing outsourced services market.

“ADT Commercial’s ongoing investments in technology and the skill sets of our team members give us the ability to deliver more than just security integration to our customers,” said Christopher BenVau, Regional Vice President–West, ADT Commercial.

“We are seeing more of our customers implementing networks that are separate from their customer data and POS networks to ensure a higher level of security due to recent data breaches. This trend makes the services provided by the NOCs even more important as our customers’ needs evolve.”

The ADT Commercial NOC teams can help plan and deploy a company’s network, implement and manage broadband connections. The NOCs can notify a customer if their IP camera is out before they even realize it. With the large storage arrays in use today, one unknown failed hard drive could bring down an entire system, potentially destroying all archived video. The NOCs can monitor the health of hard drives and immediately notify customers of a failed drive while scheduling a service call to remedy the situation and help minimize loss. Cloud-based services managed from the NOCs include a web-based dashboard that allows the management and reporting of all IT environments, including networks and security, along with cloud backup and disaster recovery services.

> “ADT Commercial’s ongoing investments in technology and the skill sets of our team members give us the ability to deliver more than just security integration to our customers”
>
> **Christopher BenVau**
>
> Regional Vice President–West,
> ADT Commercial

## Conclusion

The growing threat of cybercrime and the high cost of remediating the aftermath of an attack, both in terms of hard dollars and brand reputation, can be devastating to an organization. In Target's 2016 annual financial report, they reported the total cost of their breach was over $290 million.

New and innovative approaches to elevating the protection of sensitive data has never been more pressing. Whether organizations choose to implement changes to their networks internally or through a third-party partner to make them more secure, it is a process that is worth heavy consideration.

The cost of implementing a security-only network pales in comparison to the potential cost of an actual breach. If an organization or company has not yet considered the possibility of implementing a higher level of security to protect their business and their customers, it is probably time to do so.

Cybercrime rates are escalating as cybercriminals will continue to grow more sophisticated in their approach. Now is the time to ensure your business is protected.

**$290 Million**

total cost of Target's data breach

# Our commitment to customers

These guiding principles are the foundation of ADT Commercial. They drive our success as we strive to deliver customer service excellence at every point of interaction.

### Customers are Our True North

We know that our reputation is based on how we serve our customers.

### Our People are the Difference

We strive to be the best technically-trained team in the business.

### Dedicated to Commercial

We are 100% focused on our commercial customers.

### One Ideal Partner

We are the premier holistic solutions partner—a full-service national company with nimble local delivery teams.

# Let’s start a conversation.

We make it easy to switch providers, and our onboarding process is predictable, dependable and painless. You will be assigned a dedicated team to help with recommending and implementing the solutions that fit your needs.

**833.238.5224**

adtcommercial.com

ADT® Commercial

Powered by Experience. Driven by Excellence.™

**SSI**
Integrated Installation
(Multi-Site) 2018

**SSI**
Installer of the Year
2018

**SDM**
Dealer of the Year
2017

**TMA**
Five Diamond
Certification

**A+ BBB Rating**
Accredited
Business

This document, materials or presentation, whether offered online or presented in hard copy (“ADT Commercial Information Tools”) is for information purposes only. ADT COMMERCIAL PROVIDES THESE ADT COMMERCIAL INFORMATIONAL TOOLS “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

The ADT Commercial Information Tools contain ADT Commercial proprietary and confidential materials. No part of the ADT Commercial Informational Tools may be modified, altered, reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), without the prior written permission of ADT Commercial, except as otherwise permitted by law. Prior to publication, reasonable effort was made to validate this information. The ADT Commercial Information Tools may include technical inaccuracies or typographical errors. Actual savings or results achieved may be different from those outlined in the ADT Commercial Informational Tools. The recipient shall not alter or remove any part of this statement.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. ADT Commercial products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective in ensuring network security and regulatory compliance.