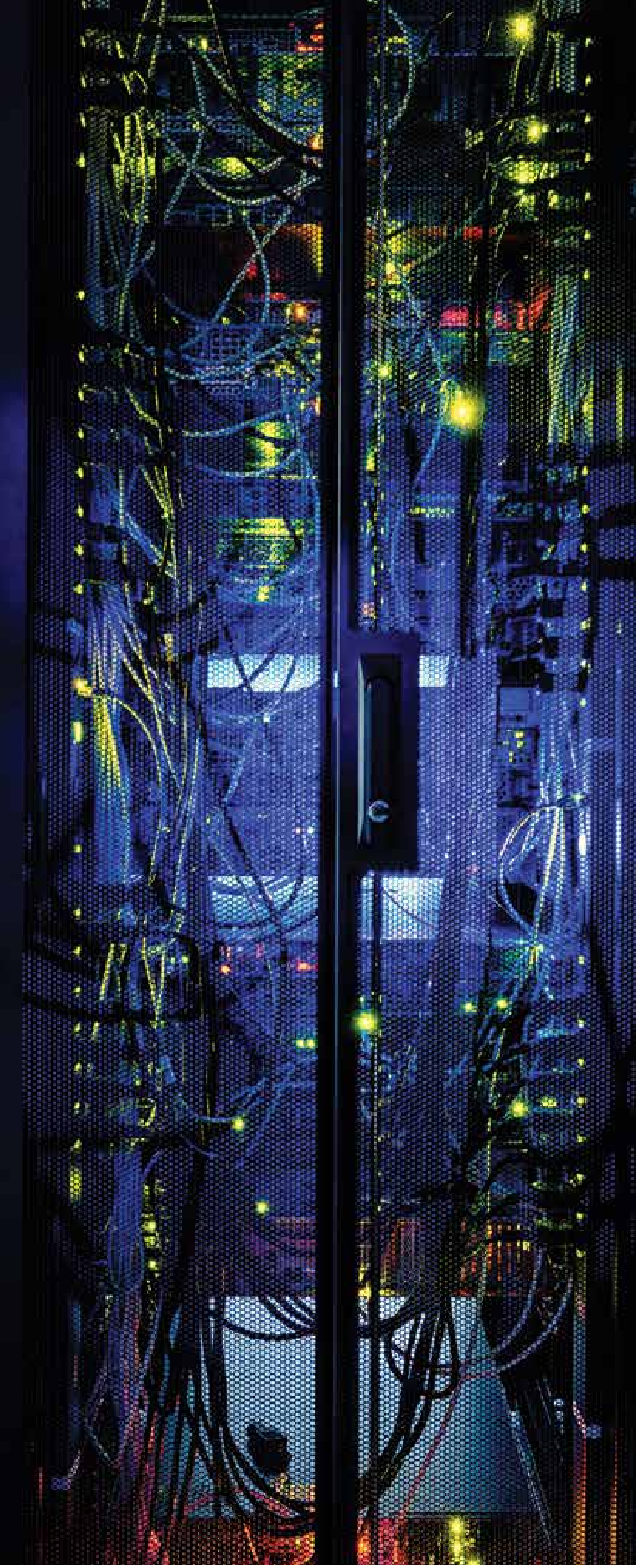
# BLACK BOX WHITEPAPER: UNDERSTANDING FIBER TO THE DESKTOP

LEAVE THE TECH TO US



## SECURITY IS THE KEY TO THIS ARCHITECTURE

As we explore the advantages of Fiber to the Desktop (FTTD),it is also important to focus on the significant upgrade in levels of security that it provides. While many standards bodies focus on data and cyber security, there is not an obvious and pervasive standard on FTTD networks and physical security. Black Box believes that our "four levels of security" describe the contribution FTTD can provide in both physical and network security.

At Black Box, this has been our first goal with FTTD architectures. How can we provide consistent and universal security representing physical, networking and data integrity? Our position is unique in that we supply products in all of these areas: cabling, infrastructure, networking and customer premises equipment (CPE). The idea is to define these security levels in an easy to understand way, and validate that peace of mind is well worth the total cost of ownership. FTTD can provide this.

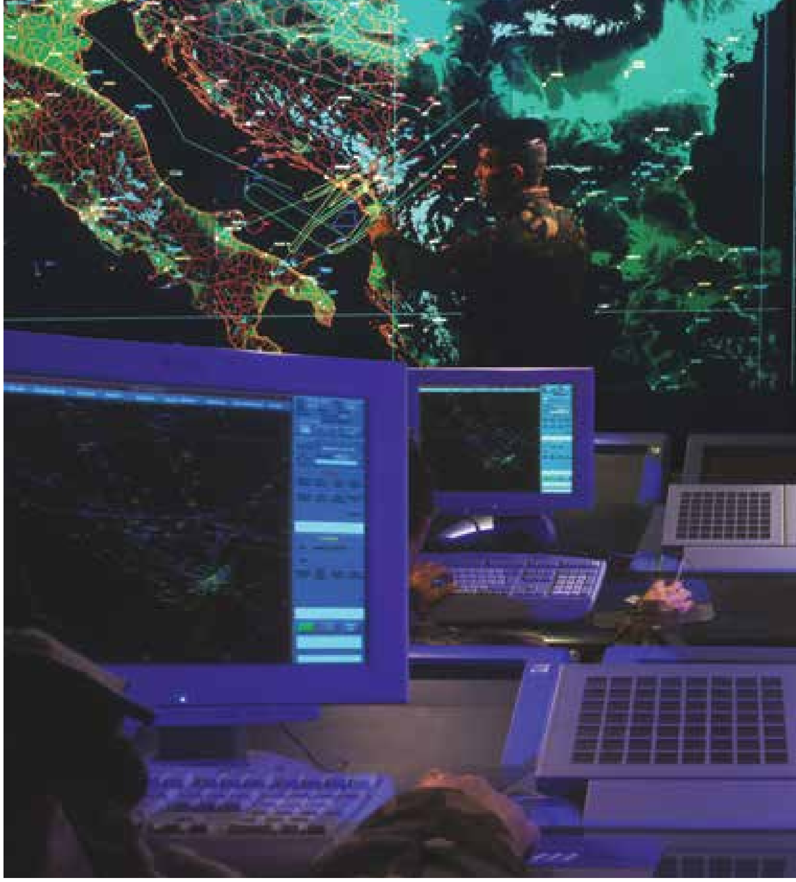
### SECURITY LEVEL 1

Security level 1 is the consideration of removing copper cable from the LAN/WAN network and replacing it with fiber optics. LANs using copper transport data streams as electronic transmissions that can only travel relatively short distances (100 meters or less) before re-transmission. What this means is that the data is relatively easy to snoop electronically. It also means copper has multiple access points within the office, such as in telecom rooms on each floor. Fiber optic cable solves both of these problems. Fiber converts the electronic data streams to light, which is much harder to snoop. Fiber optic transmission can also go long distances, allowing all cables to be homerun back to a secure location, without physical disruption. Security level 1 is simple ensuring that fiber optic technology eliminates the copper-based vulnerabilities from the network.

### SECURITY LEVEL 2

Security level 2 is the next level of security aimed at preventing the physical theft of data. This involves the placement of locking connectors at every physical interconnection point. Both copper and fiber cables present thousands of physical connection points that are typically left unsecure. For example, if an individual walks into an office, unplugs a copper patch cable from a computer terminal and plugs it into their unauthorized laptop. Perhaps not a threat, but visually, this is easy and many people have done it. By investing in locking connectors at all copper and fiber termination points, this type of threat is eliminated. The only way that these cables can be unplugged is with a specific locking tool.

From the IT manager, system integrator or technician perspective, Security level 2 ensures that installed connections remain in place. The only way changes can be made is when the authorized technician unlocks the connection.



## SECURITY LEVEL 3

Security level 3 is particularly relevant in defense, healthcare and financial industry networks. This level specifies that all access points for the network are secured within locked cabinets. Main cabinets in the data centers are locked, and all ingress equipment is secured. Furthermore, these cabinets have very specific features that add to the security of tamper-proof cable management. Other security factors including separation between networks, data processing/server equipment, specific environmental protections and redundant power are just a few considerations that are important. As fiber optic to the floor or office occurs, a wall-mount lock-box or a co-location style locked cabinet should be used. Each office, each tenant and/or each work group's fiber hub points should be physically locked and separated as a theft control measure. Another measure is to ensure each fiber office cable is properly labeled and documented. Doing this not only puts the access points behind lock and key, but the network design also ensures that only limited exposure will occur should the security levels be defeated.

Finally, at the desktop or fiber riser location, all electronics and network connections should be secured within a compact, locked enclosure. The only remaining connection or electronic that can be manipulated is the end terminal, end personal computer or end access point. Every other part of the network is locked and secured.

## SECURITY LEVEL 4

Security level 4 eliminates the desktop computer altogether. In this scenario, high-performance KVM (keyboard, video, mouse) extends the FTTD network to only provide end user keyboard, display and mouse access. The actual personal computer resides back in a secure central facility. This means that the computer, all of its data, and any physical terminal manipulation is eliminated completely. This type of security can be provided by Black Box in two formats:

- **HIGH-PERFORMANCE KVM PROVIDES POINT-TO-POINT EXTENSION, ACROSS SPECIFIC DATA LINKS, TO PERIPHERAL DEVICES (KVM) FROM THE SECURE LOCATION WHERE THE PERSONAL COMPUTERS ARE LOCKED AWAY.**

- **KVM OVER IP PROVIDES POINT-TO-POINT EXTENSION, ACROSS COMMON ETHERNET/IP NETWORKS, TO PERIPHERAL DEVICES (KVM) FROM THE SECURE LOCATION WHERE THE PERSONAL COMPUTERS ARE LOCKED AWAY.**

These security levels represent the Black Box FTTD solution. The illustration below shows that each successive level of security represents an additional level of protection. This can be very important in defense, healthcare, finance and retail environments. More importantly, the ability to migrate from Fiber to the Floor to FTTD/KVM Level 4 is realizable with Black Box. This is a unique part of our solution: the ability to view security and fiber optic networking based upon the budget available, now and in the future.

Black Box FTTD System Integrators are available to help with these decisions, construct budgets, and ultimately execute on a phased fiber optic architecture. Arguably, secondary security standards such as Sarbanes-Oxley Act (SOx), the Gramm-Leach-Bliley Act (GLB), compliance with Federal Financial Institutions Examination Council (FFIEC) Information Security Booklet, compliance with NIST 800 series, ISO/IEC 27002 and HIPAA regulations are important. Black Box FTTD is complementary and constructive to all of these security-based standards.

| FTTD TYPE | WAN SECURITY THROUGH FIBER OPTICS | DESKTOP SECURITY THROUGH FIBER OPTICS | LOCKING CONNECTORS SECURE ACCESS POINTS | ACCESS POINTS SECURED IN LOCKED CABINETS | PERSONAL COMPUTERS REMOVED FROM DESKTOP | L2/3 IP SECURITY OF THE PERIPHERAL DEVICES |
|---|---|---|---|---|---|---|
| FIBER TO THE FLOOR | YES | NO | NO | NO | NO | NO |
| FTTD LEVEL 1 | YES | YES | NO | NO | NO | NO |
| FTTD LEVEL 2 | YES | YES | YES | NO | NO | NO |
| FTTD LEVEL 3 | YES | YES | YES | YES | NO | NO |
| FTTD/KVM-LEVEL 4 | YES | YES | YES | YES | YES | YES |