

# CYBER SECURITY IN THE FINANCIAL INDUSTRY

From complying with industry regulations to meeting evolving customer demands and increasing uptime, institutions within the financial sector each face a unique set of pain points. One challenge they all share is combating the growing cybersecurity threat.

**Finance is one of the five most cyber attacked industries with losses of \$18 million per institution.<sup>1</sup> Less than half are prepared for a cybersecurity attack.<sup>2</sup>**



## Banking

Since 2015 there has been a **546% increase** in ATM skimming attacks.<sup>3</sup>

*FACT:*  
Data can be skimmed from mobile devices when a seemingly legitimate application is downloaded but is compromised.



## Trading

**30% of organizations** have experienced cyberattacks on infrastructure.<sup>4</sup>

*FACT:*  
Criminals are increasingly turning to complex multistage techniques and combining several methods in a single attack.



## Insurance

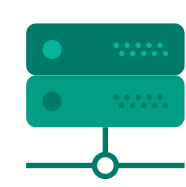
Each year, **38 out of 113 cyberattacks** are successful in causing a breach.<sup>5</sup>

*FACT:*  
DDoS attacks are becoming more powerful. 2018 was marked by two of the largest in history, reaching 1.35 and 1.7 terabits per second.<sup>6</sup>

If a breach does occur, finance organizations across the globe **rely on Opengear** for full visibility.

## EXTEND YOUR REACH

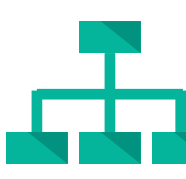
In the event of a breach, use **Lighthouse Centralized Management** to:



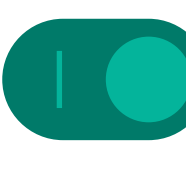
Disable access to impacted network equipment via the console port, to isolate the incident



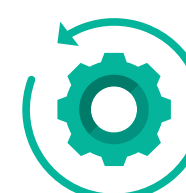
Shut down access to servers to protect private data until the breach has been remedied



Disconnect the WAN connection to isolate an affected branch; use cellular access to remediate remotely



If unable to regain control of network assets, power off via remote PDU control



Reconfigure devices to factory default, and rebuild the profiles via the console port

Make the **smart investment**, get *Smart Out-of-Band* by Opengear.