White paper

Blended security

Using smart technology to keep higher education institutions safe—online and on campus

verizon

Table of contents

Executive summary

Many higher education institutions have adopted blended learning, a model that combines on-campus learning with online learning. This flexible approach enables colleges and universities to shift agilely from one pedagogy to another in response to changing conditions. In this white paper, we explore the benefits of blended security, which helps keep the academic community safe while on campus—while also protecting the institution online, including its network and vital data.

Protecting all aspects of an academic institution

Keeping people and data safe under all conditions can be a daunting challenge for higher education institutions still recovering from the many disruptions created by COVID-19. At the pandemic's onset, IT departments within educational institutions found themselves focusing their attention and resources on meeting the surging demand for remote services from all constituents—students, faculty, administrators and researchers. Meanwhile, they faced a corresponding surge in security risk, thanks in part to these remote users signing in from home, coffee shops, or other less-than-secure locations. Juggling learning demands with an increased need for health and safety is no small feat. Here are some insights gained so far.

> **"Education technology leaders can apply lessons they have learned from the pandemic—and the shift to remote learning—to long-term security strategies."**
>
> **—Chris Novak, Director**
> Verizon Threat Research Advisory Center

During a recent EdScoop podcast, Chris Novak, director of Verizon's Threat Research Advisory Center spoke on how security strategies can be developed through lessons learned through the pandemic. These strategies include implementing effective security in both contexts—online and on campus—with equal commitment and proficiency. After all, students, faculty, administrators and parents all need to stay connected and safe online without interrupting learning or compromising their data—or their school's network. For example, a recent ransomware attack forced Central Piedmont Community College in Charlotte, North Carolina to cancel classes.[1] And it's far from the only interruption of education caused by cybersecurity issues. On campus, the community needs to be able to focus on education in a safe environment, without the threat of personal injury or other dangers.

The challenges: Combating threats, staying safe and ensuring educational continuity

Colleges and universities hold a special place in the imagination as idyllic settings for learning and personal growth among a supportive, safe community. But no matter where they're located—small towns or urban areas—institutions of higher learning face the same crime risks as any community. In fact, higher ed institutions are often considered soft targets by criminals, because of security gaps, trusting students and the presence of high-value items, from laptops and cell phones to bicycles and cars. Common crimes include burglaries (38%), sex offenses (36%) and motor vehicle theft (12%).[2] Is campus crime on the rise? The answer is largely dependent on the location and size of the institution, with wide variance among campuses. However, most on-campus crime tends to mirror trends in surrounding communities, particularly those adjacent to urban areas.[3]

Online, higher education is equally attractive to criminals. Sensitive information—including institutional financial data, student and faculty data, intellectual property and sensitive research—make higher-ed institutions a veritable candy store for hackers. Research shows that the education sector is the least-prepared to fend off cyberattacks.[4] Security at these institutions may not be as strong as in the private sector. Less vigilant users may be more likely to fall for phishing attacks and other scams. The growing use of remote learning has opened up new avenues of vulnerabilities as administrators, teachers and students all moved beyond the traditional network and began to connect via potentially less secure endpoints.

Also, new avenues of attack and vulnerabilities appear regularly. For example, when cybercriminals (thought to be Russian intelligence) hacked SolarWinds, a major software vendor to government and education, they gained access to up to 18,000 institutions in what has been called "cyber Pearl Harbor."[5] Monitoring and ensuring the security of vendors creates yet another layer of security issues, one that requires rigorous and ongoing vendor security assessment.

It's clear that the security challenges faced by higher education institutions are significant, both on campus and online. Here are just a few:

Campus challenges

Growing complexity
Protecting an entire campus has become much more complicated than it was in the days of campus security guards walking around the quad with walkie-talkies. Labs, dorms and administrative buildings all require advanced technology to ensure safety from break-ins and thefts. Less tangible assets—including data and intellectual property—must also be protected. Partners, vendors and others who access the campus need to be vetted and monitored. The line between town and gown—the institution and its surrounding community—is often blurry, making the work of protecting the physical campus more complicated.

Economic uncertainty
Difficult economic conditions and rising crime increase the traditional attraction of campuses as easy targets.

Fiscal pressures
Many higher education institutions face significant financial challenges (most due to COVID-19), including declining and delayed enrollment, cuts in programs that brought in revenue and decreases in alumni giving. New investment in bricks-and-mortar campus security must vie with other priorities for funding.

Varying student populations
In the past, the academic calendar was set. Students started arriving in late summer and departed in spring. Now, a more unpredictable flow of students, teachers, administrators and others pose significant challenges (staffing and otherwise) to the security personnel charged with protecting the campus. While fewer students can mean less crime, it can also create new opportunities for crime, due to less vigilance and more isolation, as well as empty buildings and under-used areas.[6]

The challenges: Combating threats, staying safe and ensuring educational continuity

Online challenges

Escalating breaches and threats
Growing security concerns had already propelled information security to the top of the EDUCAUSE list of IT issues early in 2020.[7] The COVID-19 pandemic made security all the more critical. The statistics support this trend:

24.5 million
records lost by U.S. schools in breaches since 2005[8]

>50%
of UK universities suffered a data breach in 2020[9]

The growth of ransomware
The rate of ransomware attacks within the education sector has increased dramatically, with ransomware accounting for approximately 80% of malware infections, according to the 2020 Verizon Data Breach Investigations Report (DBIR).[10] As just one recent example, in June, 2020, the University of California, San Francisco paid hackers $1.14M to recover data from its School of Medicine's servers, which had been encrypted with Netwalker virus—one of the largest ransomware payouts to date.[11] And experts say that more (and more sophisticated) cyber extortion is on the way for higher education.[12]

Significant losses
Financial loss, reputational damage, interruption of educational continuity and other threats keep higher ed administrators awake at night. The personal and financial data of students, faculty, researchers, administrators, alumni, donors and others is at risk of being stolen, revealed, or ransomed.

The expansion of remote learning
It's clear that remote learning isn't going away. "A lot of students are reconsidering their education choices—and some may not choose to come back to campus," says Novak. "Educational institutions are having to extend their remote learning offerings even when the urgent need and requirement for remote learning has passed. If they don't, they risk alienating a certain population that may not be able to return to campus, for whatever reason. As a result, these schools have to continue to maintain and expand their cybersecurity capabilities."

Remote learning's most obvious benefit is that it enables higher education institutions to continue to function even when their physical locations must be shut down. But remote learning also offers an opportunity to expand the curriculum and attract new students. As remote learning continues to grow, its inherent vulnerabilities—including inexperienced users signing in from home, coffee shops, or other less-than-secure locations—expands as well. After all, a network is only as strong as its weakest link.[13]

The shortage of cybersecurity professionals
Combating online threats requires sophisticated skills. Before the pandemic, higher-ed institutions already had difficulty attracting talented IT staff, since security professionals were in high demand. But COVID-19 made it even harder for public colleges and universities to compete with private sector organizations for talent, leaving them struggling to address critical security issues.

The strategies: Similar approaches for strengthening security

While online and on-campus life may seem worlds apart, they have parallel security needs. In short, protecting a campus and its community isn't markedly different from protecting a network and its data. And in some cases—such as a lab break-in involving stolen research—on campus and online security must work hand in hand.

Here are some of the general strategies that higher education institutions implement to ensure safety and security, online and on campus.

Identify all risks and vulnerabilities.
An on-campus vulnerability could be a high-crime area, a certain event or time period (e.g., school holidays), or a specific building or buildings with less modern security (e.g., lacking keycards or security cameras). Online, any action or technology that puts the network or its users at risk must be identified. Identifying risks requires proactive thinking that helps stop incidents before they happen.

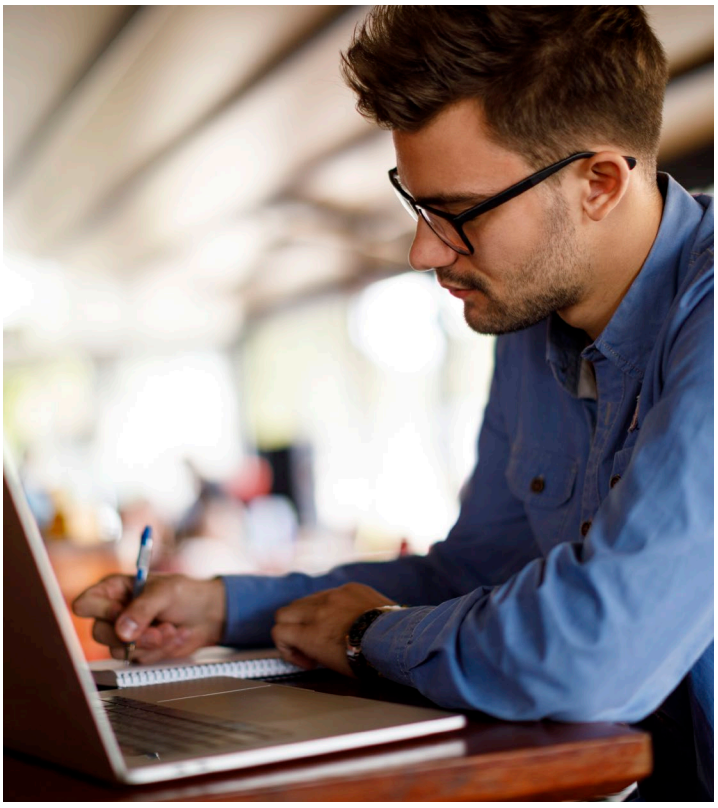
Protect all assets—human and digital.
Investing in, implementing and continually strengthening the security infrastructure helps protect the academic community, online and on campus. Higher-education institutions need to have a set of baseline minimum security standards, a next-level set of higher standards and educational awareness material on how to protect all access.

Detect security issues adeptly and respond quickly.
Security personnel have to be able to monitor the entire campus—and its network. Successful detection requires advanced technology and human vigilance. And when an incident occurs, the school must respond quickly to limit its impact, whether it's an on-campus crime or a malware attack.

Recover quickly and thoroughly—and use incidents to strengthen security.
Life must go on after a security event, whether it's a dorm robbery or a cyberattack. Recovering quickly and completely means doing more than going back to the old ways. It means learning from every incident and using that knowledge to bolster security, whether on campus or online.

"It's important for colleges and universities to conduct their own SWOT (Strengths, Weaknesses, Opportunities and Threats) analysis right from the start."

—**Chief Gary D. Lewis, Jr,**
Director of Campus Safety and
Chief of Police at the University of Louisville



On-campus security solutions: Technology-driven and ever-expanding

Higher-ed security isn't all about reports of malware attacks, campus crime, and doom and gloom. There are significant new opportunities for boosting campus security and cybersecurity for institutions willing to embrace change and invest in technology. There's a financial upside as well. Though COVID-19 has negatively affected the finances of many higher ed institutions, smart technology can increase security while cutting costs via greater efficiency. During an era of financial pressure, a blended model helps these institutions do more with less by adopting smarter security solutions, both on campus and online.

Here we take a look at some of the innovative on-campus security solutions that colleges and universities are deploying.

Identify risks and vulnerabilities.

Awareness and monitoring technologies
In the past, knowing a campus meant people walking around—proctors, guards and other university personnel. Now those human eyes can be supplemented by more robust awareness technologies. For example, advanced video monitoring can provide near real-time awareness and remote monitoring that help security personnel know exactly what's going on. When something of interest occurs, security personnel receive proactive alerts and notifications that identify potential issues. And powerful analytics let schools identify threats and problematic areas on campus. As video moves beyond simple security cameras, colleges and universities will be able to be more proactive in identifying risks and vulnerabilities.

Protect students on campus.

Smart lighting on campus
Lighting is much more than decorative on college campuses. It's a key factor in helping to protect students. Smarter, brighter lighting can help increase safety on campus while reducing energy and maintenance costs. Advanced lighting solutions tap the ability of LED luminaires to be equipped with sensors that capture and transmit data in near real time. In short, campus lighting can become an early warning system, helping to protect students by spotting when lights are out, detecting motion and heat and much more.

Emergency phone solutions
Most students are probably familiar with centrally located emergency phones, which protect students by providing readily available emergency communication. Despite the widespread use of cellphones, emergency phones provide another layer of protection and communication. Next-generation emergency phone solutions have evolved from the red emergency boxes (usually mounted in highly visible places on campus) of the past. The latest solutions deliver reliable, completely wireless emergency communication capabilities, 24/7/365. Flashing strobes can assist responders when locating callers in trouble. Fueled by solar power and an internal battery, these systems can stay up and running even during grid failures.

Personal safety devices
Personal safety devices that communicate directly with campus police can serve as dedicated protection for students, faculty and other university personnel who find themselves in potentially dangerous situations—such as leaving campus buildings or parking garages late at night. Compact and simple to use, the latest personal safety devices are designed to be accessible at all times. At the push of a button, the device can send out duress alerts to campus police or anyone the user chooses.

On-campus security solutions: Technology-driven and ever-expanding

Detect potential incidents and respond quickly.

Real-time awareness and intelligent video
Real-time awareness and intelligent video also serve a key role in detection and response. Cameras capture high-quality video, which is analyzed to identify unusual or abnormal behavior. It helps improve safety on campus by detecting these anomalies when and where they occur—then sending proactive alerts and notifications to campus security. These next-generation video solutions help security personnel know when, what and where something of interest is happening, so they can respond quickly. The result? Reduced reaction times, increased clarity, greater insights into events—and safer campuses.

Drone security systems
Drone security systems are helping campus security respond more strategically and quickly to emergency situations. They go beyond the capabilities of fixed-site video cameras, allowing security personnel visibility into key areas when necessary. Advanced solution providers are helping universities integrate drones into their security plans.

Weapon detection systems
Weapon detection systems (also known as active shooter systems) can help campus security identify when and where shots are fired. Though these systems may seem like the domain of urban police forces, they can help prevent the kind of crimes that higher education institutions dread—hostage situations, active shooters and other armed attacks.

Reliable interoperable communications
Fast, connected communication is vital to a quick response. Campus security personnel need to coordinate their response seamlessly, enable rapid collaboration and make decisions in near real-time. Advanced, reliable interoperable communications and priority network access help first responders and other key personnel communicate during their response to all situations—from an isolated incident to a major emergency. More powerful, capable communication solutions use advanced network features to enable seamless, interoperable communication—and fast response.

Recover by taking action and making changes.

When a campus incident occurs, it's an opportunity to conduct analysis and make changes. "It's important for colleges and universities to conduct their own SWOT (Strengths, Weaknesses, Opportunities and Threats) analysis right from the start," says Chief Gary D. Lewis, Jr., director of Campus Safety, Chief of Police at the University of Louisville. "But in the aftermath of an incident, it's an opportunity to reassess and ask some hard questions. How did this happen? What are our vulnerabilities? Where are there gaps? Are we taking advantage of best practices in technology?"

Collaboration and communication
Answering these questions requires communication and collaboration among key stakeholders within the university. While institutions have formal processes for addressing and recovering from campus crime, collaborative communication solutions can foster new openness and communication. "It's important to break down silos within institutions," says Chief Lewis, "and create new best practices moving forward."

Online security solutions: Advanced cybersecurity to combat sophisticated threats

Cybersecurity presents some daunting challenges for higher education institutions, which may be at different stages in their digital transformation and security readiness. While some institutions have implemented extensive online security, layered defenses and user training, other institutions are less prepared—and more vulnerable. The general consensus is that there are more of the latter than the former.[14] While the COVID-19 pandemic intensified security challenges, it also inspired a serious re-evaluation of cybersecurity readiness, as higher education security leaders reassessed their strategies.[15]

Here are just some of the cybersecurity solutions available to higher-education institutions:

Identify the most probable cyberthreats.

Staying up to speed on cybersecurity threats is a major challenge for higher-education IT departments. That's why many are turning to managed and professional services from partners focused on the challenges of cybersecurity. This approach offers a range of benefits, foremost among them the ability to strengthen and extend the security of network operations and user security—on premises and in the cloud. The right partner can provide comprehensive security expertise on demand. It frees in-house IT professionals to turn their attention to foundational operations and initiatives, such as providing critical connectivity for students, staff and teachers. And scalable support provides higher-ed institutions with a cost-effective approach that keeps them flexible, responsive—and ready for the challenges ahead.

For example, cybersecurity assessments can help educational institutions focus on defending against the most likely and probable threats. These assessments help provide the valuable data that helps institutions decide where to focus their attention—and what security initiatives to pursue. After all, every institution is different, and it's important to understand the biggest threats for specific campuses. "To minimize risk exposure, security teams must fully understand the specific threats and vulnerabilities of their institutions," according to a recent EdTech article.

"Depending on various factors—the nature of academic programs, for example—some of these risks may differ among peer institutions."[16]

It's important to remember that online threats are constantly evolving, as hackers zero in on new areas of vulnerability—and sources of revenue. There are new (and increasingly sophisticated) methods for parting users from their sign-in credentials. New forms of ransomware and other threats (e.g., COVID-19 scams) appear—Emotet, Trickbot, Maze, Ryuk, Netwalker and others yet to be unidentified. And new cybercrime groups form and morph, with memorable names like Circus Spider and Mummy Spider.[17]

Ongoing risk monitoring is another area rich with managed and professional services, one that helps assess an institution's security. Monitoring insights can give IT teams the data they need to identify security gaps and evaluate where they need to focus, all leading to more informed decisions.

Online security solutions: Advanced cybersecurity to combat sophisticated threats

Protect your network and data.

The network and its data are an educational institution's crown jewels, demanding constant protection. The dilemma? The network, so critical and valuable, is also widely used—and often mis-used. Its openness, reliability and availability are critical to learning, research and all academic functions. So educational institutions have a dual challenge—protecting the network while ensuring seamless access to it by authorized users.

There are a range of managed solutions that focus on protecting the network. These services are designed to help institutions stay ahead of threats and protect the network. Network monitoring is a critical capability that complements risk/threat monitoring by focusing on the network. It helps keep applications up to date, properly configured and secure—often a weak point within higher-education institutions. And it can help detect potential threats before they happen, all while keeping security costs under control.

Detect network threats and respond effectively.

The longer network penetrations and other issues go undetected, the worse the damage. The bad news? The majority of cyberattacks go undetected.[18] According to the Mandiant Security Effectiveness Report 2020:[19]

9% of attacks generate alerts

26% of attacks are detected

33% of attacks are prevented

53% of attacks are missed completely

That said, there are different levels of threats, and threat assessment and managed services—such as network detection and response—that can help institutions identify and prioritize these threats. It's important for educational institutions to identify and prioritize risks, and to ward off future attacks before they become serious events.

Recover quickly so education continues uninterrupted.

A paralyzed network doesn't just stop communication; it brings education to a near standstill. Remote learning, research, administrative functions, financial operations—they all rely on network availability. Cyberattacks are often the cause of unplanned interruptions. Once they happen, it's important to respond and recover quickly. As an extreme example, a ransomware attack hit Düsseldorf University for several days in September, 2020. Though targeted at the university itself, the attack paralyzed the university clinic. Due to the network outage, a patient suffering from a life-threatening illness had to be turned away from the clinic and subsequently died—in what many are calling the first fatal cyberattack.[20]

Other recoveries are less dire, but also important since they can delay education, lose revenue and tarnish a university's reputation. Response retainers and similar managed services can help educational institutions get back up and running quickly, minimizing the damage by providing outside expertise during a cyber crisis.

Blended security: Verizon Is ready to help protect your campus and your network.

The security challenges faced by higher-ed institutions are significant, but so are the solutions that can help address them. Verizon serves as a trusted partner to thousands of universities and colleges, providing security innovations on campus and world-class cybersecurity online. We can make a blended security model a reality for your college or university—meeting its specific needs and building on its current strengths.

Learn more.

Contact us today to start making blended security part of your security plan.

verizon.com/business/contact-us

1 Ransomware Attack Forces North Carolina College to Cancel Classes," EdScoop, February 16, 2021.
Source: https://edscoop.com/ransomware-attack-central-piedmont-community-college/

2 "Indicators of School Crime and Safety." National Center for Education Statistics, U.S. Department of Education. (2020)
Source: https://nces.ed.gov/fastfacts/display.asp?id=804

3 "Campus crime update: Fall sees major crime upticks for University neighborhoods," The Minnesota Daily, December 5, 2020.
Source: https://mndaily.com/264343/news/campus-crime-update-fall-sees-major-crime-upticks-for-university-neighborhoods/

4 "2018 Education Cybersecurity Scorecard," SecurityScorecard cybersecurity ratings.
Source: https://securityscorecard.com/resources/2018-education-report

5 "What SolarWinds Hack Means for Campuses," Inside Higher Ed, January 6, 2021.
Source: https://www.insidehighered.com/news/2021/01/06/unraveling-solarwinds-hacks-fallout-higher-ed

6 "Less People = Less Crime: Campus Police Report Drop in Campus Crime for 2020," The Wichitan, February 1, 2021.

7 2020 Top 10 IT Issues: The Drive to Digital Transformation Begins, EDUCAUSE, January 27, 2020.
Source: https://www.educause.edu/research-and-publications/research/top-10-it-issues-technologies-and-trends/2020

8 "US Schools Have Lost 2.4 Million Records in Breaches since 2005," Jonathan Greig, TechRepublic. July 2, 2020.
Source: https://www.techrepublic.com/article/us-schools-have-lost-24-5-million-records-in-breaches-since-2005/

9 "Over Half of Universities Suffered Data Breach in Past Year," Phil Muncaster, Infosecurity. July 28, 2020.
Source: https://www.infosecurity-magazine.com/news/over-half-of-universities-suffered/

10 Verizon 2020 Data Breach Investigations Report, Educational Services.
Source: https://enterprise.verizon.com/resources/reports/dbir/2020/summary-of-findings/

11 "UCSF Pays Hackers $1.14M to Recover Encrypted Data," Daniel Wu, Palo Alto Daily News, July 1, 2020.
Source: https://www.govtech.com/security/UCSF-Pays-Hackers-1-14M-to-Recover-Encrypted-Data.html

12 Cyberextortion Threat Evolves," Lindsay McKenzie, Inside Higher Ed, June 11, 2020.

13 "Security Is Only As Strong as the Weakest Link," Infosecurity, November 21, 2019.
Source: https://www.infosecurity-magazine.com/opinions/strong-weakest-link/

14 Verizon 2020 Data Breach Investigations Report, Educational Services.
Source: https://enterprise.verizon.com/resources/reports/dbir/2020/summary-of-findings/

15 "Higher Ed's New Approach to Pandemic Cybersecurity," EdTech, September 16, 2020.
Source: https://edtechmagazine.com/higher/article/2020/09/higher-eds-new-approach-pandemic-cybersecurity

16 "Three Ways to Elevate Your College's Cybersecurity Defenses," Suchi Rudra, EdTech, January 13, 2021.
Source: https://edtechmagazine.com/higher/article/2021/01/3-ways-elevate-your-colleges-cybersecurity-defenses

17 "How Cyber Criminals Use Coronavirus Scams to Target Victims," Security Management, June 1, 2020.
Source: https://www.asisonline.org/security-management-magazine/articles/2020/06/how-cyber-criminals-use-coronavirus-scams-to-target-victims/

18 "Majority of Cyber Attacks Go Undetected," Security Boulevard, June 29, 2020
Source: https://securityboulevard.com/2020/06/majority-of-cyber-attacks-go-undetected/

19 Mandiant Security Effectiveness Report 2020
Source: https://www.fireeye.com/current-threats/annual-threat-report/security-effectiveness-report.html

20 "Was This the World's First Fatal Cyberattack? Bruce Sussman, SecureWorld, Sept 21, 2020.
Source: https://www.secureworldexpo.com/industry-news/fatal-cyberattack-killer-ransomware-attack

Verizon and higher-education cybersecurity

Verizon is a trusted advisor to higher education.

Verizon has many years of experience in higher education and offers a full portfolio of cybersecurity solutions, managed and professional services—as well as innovative on-campus security solutions.

Verizon offers strategic advantages to colleges and universities.
Verizon's experience monitoring and protecting its own networks from adversaries across the globe gives it a deep understanding of the types of threats that can impact colleges and universities.

Verizon means experience.
Verizon is one of the world's leading security companies, with 25+ years of experience.

Security is an ongoing, ever-evolving battle.
Verizon is on the frontlines, every day.

For more information:

- Explore Verizon's security offerings for higher education.
- Download the 2020 Verizon Data Breach Investigations Report (DBIR).
- Consult Smart-Safe Campus: A Planning Guide for Higher Education Leaders.
- Listen to EdScoop Radio's podcast, "Managed Services Key to Education Cybersecurity Post-COVID," featuring Verizon's Chris Novak and Shane Hallen, a strategic sales manager for service providers at Cisco Meraki.

On-campus security solutions from Verizon and our partners

- Video monitoring—Verizon Intelligent Video
- Emergency phone solutions—Blue Light Tower from CASE Emergency Systems
- Personal safety devices—Persa by Vestige
- Drone security systems—Skyward
- Weapon detection—ZeroEyes weapon detection
- Interoperable communications—Verizon Push to Talk Responder
- Collaborative communication—BlueJeans by Verizon

Verizon Managed and Professional Services for cybersecurity

- Cybersecurity Assessment
- Cyber Risk Monitoring
- DNS Safeguard
- DDoS Shield
- Network Security Monitoring
- Network Security Management
- Managed Detection and Response

verizon