

Digital  
security,  
everywhere  
you need it

FORTINET®

DIGITAL REPORT 2021







**FORTINET®**

**DIGITAL  
SECURITY,  
EVERYWHERE  
YOU NEED IT**







***Rick Peters***, CISO, explains why cybersecurity is a continuous journey and how Fortinet can help keep businesses secure in the post-COVID world

**F**rom an outsider perspective, one might imagine that cybersecurity has been a primary component of every company's strategy since the beginning of the digital era. And yet, recent headlines demonstrate how much progress is still needed across the board.

Founded in 2000 by CEO Ken Xie and headquartered in Sunnyvale, California, Fortinet has established a reputation as being a protector of small, medium and large-scale enterprises, and government institutions globally. Driven by a vision of the future in which the digital world is always safe and trustworthy, it has played an indispensable role in the evolution of cybersecurity with a suite of solutions that are among the industry's most popular. This comprehensive and complementary portfolio prioritises integration and automation to yield self-healing, faster, and more efficient operations across cloud, networks, and mobile environments. In short, Fortinet enables organisations to thrive.

Additionally, Fortinet espouses a philosophy that recontextualises cyber resilience as a journey, not a destination. As such, it recognises that IT and OT systems might change structurally over time but the need to keep them protected remains constant. Sustained protection of the cyber physical landscape and business innovation is achieved by integrating Fortinet's cutting-edge Security Fabric with the technology alliance ecosystem to match today's threat landscape. We spoke with Rick



**Rick Peters,**  
CISO





## Security-Driven Networking for a Hyperconnected World | Cybersecurity

WATCH NOW

Peters, Chief Information Security Officer, Operational Technology (OT) North America, to learn more.

Having spent almost four decades at the US National Security Agency (NSA) in a variety of managerial and executive roles, it is safe to say that Peters knows what constitutes strong cybersecurity system defences. During his long tenure, he was able to gain credentials, experience, and insight into what it takes to successfully launch a business in cyberspace. “I had the luxury of experiencing and executing missions from both the offensive and defensive sides. Post my IC career, I felt that whatever was next professionally needed to be a departure from working in the government, and private industry afforded such an opportunity.” It wasn’t long before Peters joined the Fortinet team in early 2018.

**“YOU HAVE TO  
ALIGN YOUR  
VALUES WITH THE  
CUSTOMER’S AND  
DETERMINE HOW  
THEY’RE TRYING  
TO SOLVE THEIR  
MOST IMPORTANT  
PROBLEMS”**

RICK PETERS  
CISO,  
FORTINET





## EXECUTIVE BIO

### RICK PETERS



TITLE: CISO

INDUSTRY: **COMPUTER &  
NETWORK SECURITY**

LOCATION: **UNITED STATES**

» Mr. Peters brings to the Fortinet Operational Technology Critical Infrastructure team more than 37 years of cybersecurity and global partnering experience working across foreign, domestic, and commercial industry sectors at the National Security Agency (NSA).

As Fortinet's Operational Technology North American CISO, he delivers cybersecurity defense solutions and insights for the OT/ICS/SCADA critical infrastructure environments. Prior to Fortinet, Rick led development of cyber capability across Endpoint, Infrastructure, and Industrial Control System technologies at the agency.

Previously, Rick also served as an executive leader supporting the Information Assurance Directorate at the NSA. Earlier in his career, he served in a broad range of leadership and Engineering roles including Chief of Staff for the NSA Cyber Task Force and a five-year forward liaison charged with directing integration of cyber and cryptologic solution for US Air Force Europe, Ramstein AFB, Germany.



# “I DISCOVERED THAT IT WAS A ‘SOLUTIONS FIRST’ ORIENTED ORGANISATION AND THAT GOT ME EXCITED”

RICK PETERS  
CISO,  
FORTINET

Sharing a mutual desire to expand OT cybersecurity, Peters spoke with Fortinet’s leadership and was impressed by what he found: “I discovered that it was a ‘solutions first’ oriented organisation and that got me excited. If you glance at Fortinet’s patent wall, you naturally realise it’s not just talking about innovation, it’s executing development to achieve it,” he recalls. At the centre of this is Fortinet’s Security Fabric- the industry’s highest-performing cybersecurity platform, powered by FortiOS, with a rich ecosystem. Conceived as a framework to enable both digital innovation and protection from cyber threats, this platform incorporates three key attributes:

- Broad visibility and protection across the entire attack surface
- Integrated and unified security that closes security gaps and reduces complexity
- Automated and context aware, it affords faster time to prevention and efficient operations

With security taking on increasing prominence within critical infrastructure for Energy and Utilities, Manufacturing, Transportation, and digitally connected building sectors, possessing expert knowledge and comprehension of the





sector's evolution is critical. "You can employ cutting-edge technology, but you also need to be committed to understanding the industrial environment. You are working with asset owners who have unique goals and a different perspective on what it means to protect the cyber-physical," says Peters. Furthermore, he identifies two other qualities that put Fortinet ahead of its competition: speed and a transparent, ecosystem-driven approach that mitigates latencies and data loss. At the heart of this is FortiOS, the foundation of the Security Fabric and what Peters considers to be a true "game changer." Delivering transparency, scalability, and sub-second response times, it employs

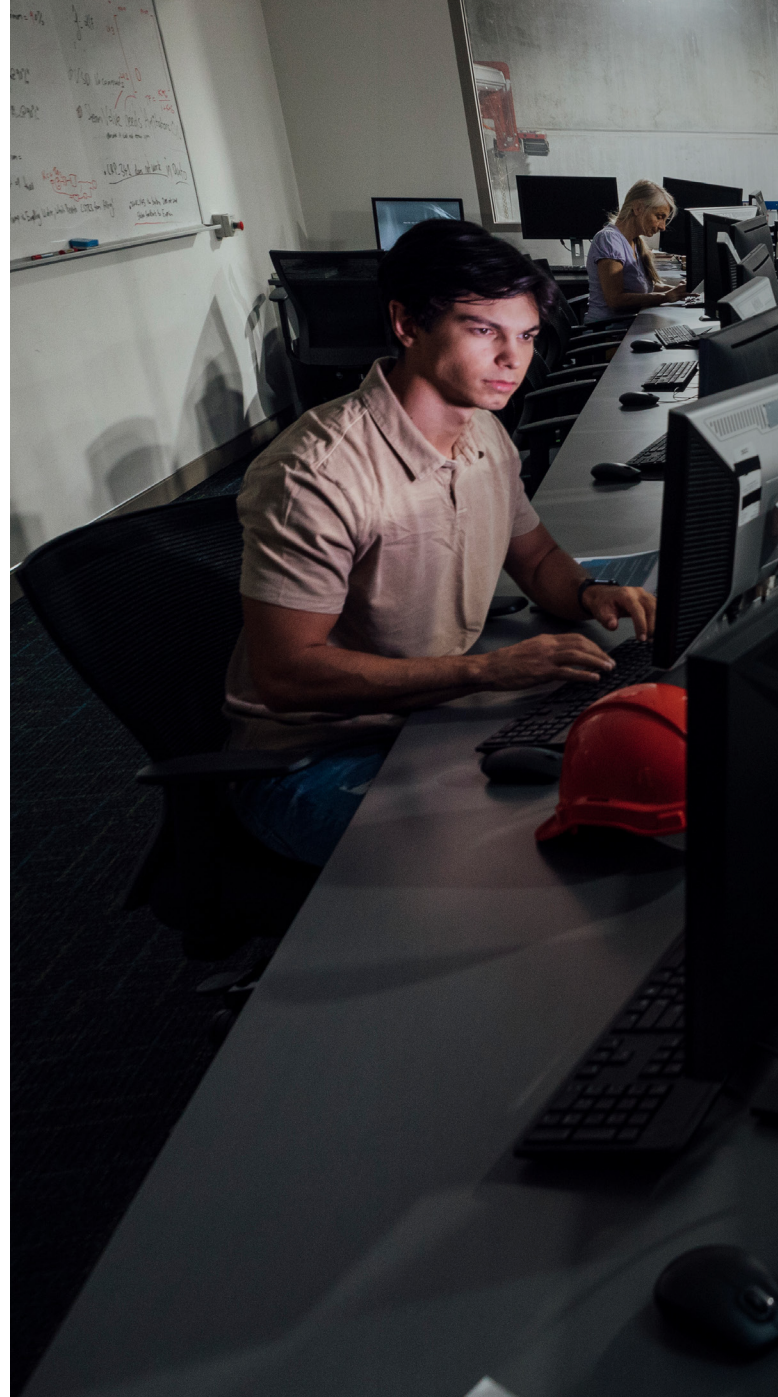
FortiGate technology, a "next-generation firewall," fully capable of accommodating the secure remote access requirements and highly adaptive cloud environments that have gained greater favour since the events of 2020.

In fact, the COVID-19 pandemic amplified an entirely new security environment challenge: circumstances made remote working a necessity to maintain business continuity, simultaneously expanding organisations' surface area for attack and instigating a shift away from on-premises business as the primary means to sustain operations. In this new paradigm, which is still far from reaching a state of equilibrium,

Fortinet is positioning itself as a guide for “new normal” security decision-making. “It’s all about building trust,” states Peters. “You have to align your values with the customer’s and determine how they’re trying to solve their most important problems.” In his view, there is no denying that data has become one of the most important assets of the 21st century - the near-ubiquity of Internet of Things (IoT) devices and the mounting viability of 5G are testaments to this, and as executives continue to collect ever-larger volumes of information to assist with operational optimisation. Maintaining a focus on enabling safe and continuous OT operations, Fortinet strives to identify and remediate threats in a way that inspires confidence and helps clients build robust security track records.

Fortinet aspires to “get out in front” of cyber threats at all times, a goal it achieves through endpoint detection and response and pre-/post-event analysis. The Fortinet Security Fabric enables the company to break down risks into manageable segments while still maintaining total visibility, therefore preventing customers from missing the big picture in the middle of an attack. “What we’re doing is flipping the script,” adds Peters. “If I were to sit down with a board today, I would probably try to convince them to behave as if they’ve already been compromised, because it’s highly likely that it will happen at some point in time. It could occur simply by employee error in accepting malware through an email. We’ve certainly heard many instances of that over the last couple of years.” Moving forward, he is confident that Fortinet will continue to enable even greater threat visibility wherever the customer needs it.

The company’s highly adaptive and proactive approach, which captures



granular elements of security without obscuring the whole, is a clear departure from cybersecurity’s highly reactive prior incarnations. Peters believes that new best-practice standards should coalesce on the idea of “zero-trust access” - “I think we have to insist on earning trust in 2021.” Several notable instances of ransomware attacks in the US confirm the formidable security challenges that modern businesses are facing. However, even here, Peters suggests a cultural solution that Fortinet can offer: stop thinking about the ransomware “payload” as the last event in a chain. “The attacker has probably undergone a period





## FORTINET - KEY STATS

- Stock symbol: FTNT (IPO October 2009)
  - 500,000+ customers
  - 6.8 million units shipped
- 776 patents issued; 211 pending
  - 8,615 employees
- US\$2.59bn = 2020 revenue
- US\$3.09bn = 2020 billings

**“I DISCOVERED THAT  
IT WAS A ‘SOLUTIONS  
FIRST’ ORIENTED  
ORGANISATION  
AND THAT GOT  
ME EXCITED”**

---

**RICK PETERS**  
CISO,  
FORTINET

of reconnaissance and figured out how to distribute their payload. In a distributed attack, like those witnessed in recent instances of supply chain exploitation, a payload is used to attack a broad range of targets and then exploit them based on opportunity and vulnerability.”

A multidimensional problem-solver, Fortinet believes in instilling a reliance on people, processes, and technology to secure IT and OT systems. “We’re advocating for the commitment of cybersecurity education as a means of improving situational awareness and realising the power of a well-informed employee as an asset instead of





2000  
Year  
founded

8,615  
Number  
of employees

\$2.59B  
FY2020  
Revenue



# “COMPLACENCY IS THE ENEMY IN THIS BUSINESS BECAUSE YOU’LL NEVER REACH THE END DESTINATION; CYBERSECURITY IS JUST A CONTINUOUS JOURNEY”

RICK PETERS


CISO,  
FORTINET

a liability.” It is the company’s belief that, through education and awareness of the role they can play, employees will naturally bolster cyber defences. “Of course, that’s not perfect,” clarifies Peters. “The human element is always going to offer a compelling reason to improve cybersecurity beyond present capabilities.” This takes the conversation not only back to the utility of “zero-trust access” but also behavioural-based endpoint security. “[The latter] raises the bar by recognising threats and learning from them. It gives you not just cyber resilience but a thorough comprehension of what’s going on. I think that’s really important: We never want to become complacent. Complacency is the enemy in this business because you’ll never reach the end destination; cybersecurity is just a continuous maturation.”

Looking ahead, Peters suggests that 2021 will symbolise a year of growth for the company, both financially and in the ongoing evolution of the Security Fabric. With the size of its initiatives in the North America, Europe, and Asia-Pacific regions doubling in the last 12 months alone, it’s clear that Fortinet has achieved a truly global appeal. Moreover, it will be capitalising on the power of partnerships to expand its problem-solving capabilities. “No one is solving [security] problems alone. We can’t be everywhere

- we’re not omnipresent - but I think our offering [via partnerships] allows us to be so much more agile and effective working with organisations and businesses of all sizes.”

However, commitment to the journey of cyber resilience is, has been, and will be Fortinet’s enduring focus. Peters explains, “Too often, leaders get trapped believing they can just commit a set amount of resources to a particular problem and then consider the issue to be resolved with a point solution. In today’s business world, whether you’re in IT or OT, that approach amounts to becoming complacent.”

Fortinet is combating this culture through cutting-edge technology and a determination to help others consider cybersecurity in a new way. This, Peters hopes, will grant customers a level of cyber resilience they can trust indefinitely, as Fortinet will share an equal dedication to their organisational objectives. “Our message is that resilience comes through persistence and the ability to continually grow and mature in the solution space. Let’s make sure we’re protecting that which is most important to our businesses so that we can remain sustainable and viable, not just this year but a decade from now.” 





---

899 Kifer Road  
Sunnyvale  
CA  
94086

T 408-235-7700 | [fortinet.com](https://fortinet.com)

POWERED BY:

